The Data Privacy/National Security Balancing Paradigm as Applied In The U.S.A. and Europe: Achieving an Acceptable Balance

Paul Raphael Murray, B.A. H.Dip in Ed. LL.B. LL.M Ph.D. (NUI)

Submitted for the Degree of Doctor in Philosophy

at

Trinity College, Dublin

School of Law

August 2017

Declaration and Online Access

I declare that this thesis has not been submitted as an exercise for a degree at this or any other university and it is entirely my own work.

I agree to deposit this thesis in the University's open access institutional repository or allow the library to do so on my behalf, subject to Irish Copyright Legislation and Trinity College Library conditions of use and acknowledgement.

Paul Raphael Murray

Acknowledgements

I would like to record my thanks to my Supervisor, Professor Neville Cox, School of Law, and Dean of Graduate Studies, Trinity College, Dublin, for his help and guidance.

Abstract

The Data Privacy/National Security Balancing Paradigm as Applied In The U.S.A. and Europe: Achieving an Acceptable Balance

Paul Raphael Murray

The overall research question addressed in this thesis is the data privacy/national security balancing paradigm, and the contrasting ways in which this operates in Europe and the U.S. Within this framework, the influences causing the balance to shift in one direction or another are examined: for example, the terrorist attacks on two U.S. cities in 2001 and in various countries in Europe in the opening decade of the new millennium, and the revelations by Edward Snowden in 2013 of the details of U.S. mass surveillance practices.

The thesis is divided into three main parts. The first part deals with European attitudes and practices in relation to the balancing paradigm. The second part deals with U.S. attitudes and practices on the same basis. It deals with the influence of the various branches of Government in determining this balance. In the third part, consideration is given to the contracts and similarities between the U.S. and Europe in relation to the balancing process, and in particular to the factors underlying the contrasts. The conclusion to the thesis gives details of the findings arrived at.

Table of Contents

Summary

1. Methodology

Having decided on a title for the thesis, I proceeded to conduct my bibliographical research. In conducting my bibliographical research, I first isolated the latest editions of books which provide broad, general surveys of the principles and practices governing my topic. These included D.P. Komers and J.E. Finn, *American Constitutional Law, Essays Texts and Materials*; Andreas Føllesdal, Brigit Peters, Geir Ulfstein, *Constituting Europe: The European Court of Human Rights in a National, European and Global Context*; Federico Fabbrini, *Fundamental Rights in Europe: Challenges and Transformations in Comparative Perspective;* Paul Craig and Gráinne de Búrca, *EU Law: Texts, Cases and Materials* (Sixth edn, Oxford University Press, 2011). A complete list of the latest editions of these and other books which reviewed aspects of my topic will be found in the Bibliography.

In the case of journal articles, I used Index Cards for compiling full details of authors' names, the full title of each article, the full title of each journal in which each article appeared and the date of publication. I found it useful to employ extra Index Cards to record significant material relating to my thesis topic, attaching these cards to the card giving the author/title details.

When I felt able to do so, I composed a table of contents to provide me with a plan as to the boundaries within which I must keep when writing the thesis. The table of contents, featuring a listing of the sub-sections in each chapter, would function as my guide to a working hypothesis, and serve to define, from the beginning, the limits of my thesis. It would give me a useful starting-point from which to work. From time to time, I was obliged to revise my hypothetical table of contents in the light of advice from my Supervisor, new insights, and second thoughts.

2. Filling the gap in the existing Literature on the subject dealt with in the thesis

Having studied all of the books, articles and other materials relevant to the subject-matter of this thesis, I have encountered none that deal with both European entities (Council of Europe and European Union) and the United States in a comparative perspective in the same detail that I have. All the works I have read in relation to my topic have concentrated on either the U.S. or Europe. The gap in the literature that I have tried to fill is the absence of a comprehensive treatment of the approaches taken by Europe on the one hand, and the U.S. on the other, to the necessary balancing process between data protection and national security. In filling this gap, as I have done, I believe that I am making an original contribution to research on a topical and developing area of law.

The differences of approach to the data privacy/national security balancing paradigm adopted by the U.S. and Europe are outlined early on in the thesis, and manifestations of these differences are featured throughout, culminating in a detailed treatment of them in Chapter Four. Furthermore, in the Overall Conclusion to the thesis, I consider the prospects of resolving these differences with a view to arriving at a principled balancing paradigm that might be acceptable on both sides of the Atlantic. Such a project would, as is suggested in the Overall Conclusion, be based on a frank assessment of issues in the domain of data privacy versus national security on which the U.S. and Europe are in conflict, in terms of Executive and legislative practice as well as jurisprudence. Account would also have to be taken of existing privacy/national security provisions common to both jurisdictions, commonalities deriving from recent U.S. Supreme Court privacy protective jurisprudence, and various pieces of recent legislation tending in the same direction.

3. Literature Review

(1) The European Approach to the National Security/Data Privacy balancing paradigm

The national security/data privacy balancing paradigm is treated extensively in the European literature in relation to the Council of Europe, the ECHR and the EU. Kokott and Sabotta emphasise that the ECHR is silent regarding a data protection provision, while Convention 108 does encompass a data protective function, but does not, in principle, fall under the jurisdiction of the ECtHR.[1] Bignami observes that the premise behind Convention 108 is the less personal data processing the better.[2]

Beddard comments that the ECHR represents a form of constitutional blueprint for a United Europe.[3] The impact of the case law of the ECtHR is evaluated by Merrills, who acknowledges the changes brought about in European domestic law because of verdicts given in Strasbourg.[4] Central to this, Helfer observes, is the access right to the ECtHR, which has made the ECHR a success in altering domestic legal provisions and challenging legal orders.[5]

Central to the research question is the concept of the 'Margin of Appreciation' as an adjudicative tool at the disposal of the ECtHR. Waldock contends that the margin of appreciation doctrine represents an important safeguard to promote the effective operation of the ECHR and allows governments to interfere with rights where such interference is necessary to promote security interests.[6] Gross

[1] Juliane Kokott and Christopher Sabotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and ECtHR' 3(4) (2013) *International Data Privacy Law* 223.
[2] Francesca Bignami, 'The Case for Tolerant Constitutional Patriotism: The Right to Privacy Before the European Courts' 41(2) (2008) *Cornell International Law Journal* 211, 222.
[3] Ralph Beddard, Human Rights and Europe (3rd edn, Cambridge University Press, 1993 5-6.
[4] J.G. Merrils, The development of International Law by the European Court of Human Rights, (2nd edn, Manchester University Press, 1993).
[5] Laurence R. Helfer, 'Towards a Theory of Effective Supranational Adjudication' 107 (1997) *The Yale Law Journal* 273, 294; Andreas Follesdal, Birgit Peters, Geir Ulfstein, (eds) *Constituting Europe. The European Court of Human Rights in a National, European and Global Context* (Cambridge University Press, 2013) 6.
[6] Humphrey Waldock, 'The Effectiveness of the system set up by the European Convention on Human Rights' 1 (1980) *International Human Rights Law Journal* 9.

and Ní Aoláin highlight the centrality of the doctrine in the jurisprudence of the European Court of Human Rights.[7]

Benvenisti cautions that the margin of appreciation doctrine could be used as a conceptual Trojan Horse in order to fragment the unity and harmony of established ECHR standards,[8] with Del Moral commenting that the doctrine has been a cause of concern to human rights lawyers and on occasions has been viewed as denying justice to individuals.[9] In this connection, Arai-Takahasi contends that the margin of appreciation can result in speedy adjudications being arrived at without evaluating the effect on privacy rights which could arise due to judicial economy.[10] Shany points to a resource gap in relation to the Court's operation.[11] Burke suggests that the interaction between the margin of appreciation doctrine and the Article 8(2) necessity in a democratic society requirement as posing an intricate question of balances.[12]

Morrisson argues that where the Court uses the margin of appreciation as a self-denying ordinance, limiting its own review of cases, it fails in its duty to address the findings of fact and law measured against the relevant ECHR provisions, in determining whether ECHR guarantees have been violated.[13] Kratochvíl observes that the consequences of applying the margin of appreciation doctrine are not possible to predict.[14] Brauch cautions that the margin of appreciation risks undermining the rule of law, two key elements of which are clarity and predictability.[15]

---

[7] Oren Gross and Fionnuala Ní Aoláin, 'From Discretion to Scrutiny: Revisiting the Application of the Margin of Appreciation Doctrine in the Context of Article 15 of the European Convention on Human Rights' 23(3) (2001) *Human Rights Quarterly* 625

[8] Eyal Benvenisti, 'Margin of Appreciation, Consensus and Universal Standards' 31 (1998-99) *New York University Journal of International Law and Practice* 843,844.

[9] ibid, 611-12.

[10] Yukata Arai-Takahasi, *The Margin of Appreciation Doctrine and the and the Principle of Proportionality in the Jurisprudence of the ECtHR* (Intersentia, Antwerp, 2002) 238-241.

[11] Yuval Shany, 'Towards s General Margin of Appreciation Doctrine in International Law?' 16(5) (2006) *European Journal of International Law* 907, 918.

[12] Karen C. Burke, 'Secret Surveillance and the European Convention on Human Rights' 33 (1981) *Stanford Law Review* 1113, 1133.

[13] Clovis C. Morrisson, 'Margin of Appreciation in European Human Rights Law' 6 (1973) *Human Rights Law Journal* 263.

[14] Jan Kratochvíl, 'The Inflation of the Margin of Appreciation by the European Court of Human Rights' 29 (3) (2001) *Netherlands Quarterly of Human Rights* 324, 325.

[15] Jeffrey A. Brauch, 'The Margin of Appreciation and the Jurisprudence of the European Court of Human Rights: Threat to the Rule of Law' 11 (2005) *Columbia Journal of European Law*, 125.

The influence of the ECHR is noted by Martinico, citing the requirement of judiciary in Germany and Italy to enforce the ECHR and to follow the jurisprudence of the ECtHR.[16] Conversely, Kay focuses on the resistance among citizens and governments of some Member States to be bound by bodies such as the ECtHR.[17]

The reliance of the EU Charter of Fundamental Rights on the provisions of the ECHR are evaluated by Craig and de Búrca, who observe that the ECtHR has in recent years made many references to, and actively accommodated, EU law and the jurisprudence of the CJEU, and has cited the EU Charter in many of its judgments.[18]

Luce Paris observes that many ECHR provisions are reproduced in the EU Charter of Fundamental Rights, some verbatim, and estimates that half of the Charter's substantive provisions can be found by reference to their equivalents in the ECHR or in ECtHR case law.[19] Craig and de Búrca observe the emerging trend in the approach of the CJEU which expresses a preference for recourse to the Charter as opposed to the ECHR, involving an increasingly more autonomous interpretation of the Charter without any reference to the ECHR.[20]

A key consideration for the future of judicial interpretation of the balancing paradigm in Europe centres on the prospect of the EU accession to the ECHR. This is assessed by Mjöll Arnardóttir and Buyse, who observe that should this come to fruition, the ECHR would exercise this function for all of Europe and the CJEU would not act as a parallel Human Rights Court, leaving the sphere

[16] See Giuseppe Martinico, 'Is the European Convention Going to be "Supreme"? A comparative constitutional overview of ECHR and EU law before national courts' 23(2) (2012) *European Journal of International Law* 401, 411.
[17] Richard S. Kay, 'The European Convention on Human Rights and the Authority of Law' 8(2) (1993) *Connecticut Journal of International Law* 217, 221. See also Peter Van Dijk and Godefridus, J.H van Hood, *Theory and Practice of the European Convention Human Rights* (Kluwer Law International, The Hague, The Netherlands, 1998), 616-45, whose authors suggested a tendency towards a growing resistance to the judgments of ECtHR.
[18] Paul Craig and Gráinne de Búrca, *EU Law: Texts, Cases and Materials* (Sixth edn, Oxford University Press, 2011) 426.
[19] Marie-Luce Paris, 'Paving the way: Adjustments of Systems and Mutual Influences Between the European Court of Human Rights and European Union Law before Accession.' 51(1) (2014) *The Irish Jurist* 1, 10.
[20] Paul Craig and Gráinne de Búrca, *EU Law: Texts, Cases and Materials* (Sixth edn, Oxford University Press, 2011) 427.

of human rights to the exclusive jurisdiction of the ECtHR.[21] Besson predicts that, based on continuing trends in relation to human rights, the EU has the capacity to become the predominant post-national human rights protection institution.[22]

Douglas-Scott contends that since the formal adoption of the EU Charter of Fundamental Rights by way of the ratified Lisbon Treaty in 2009, advantages are conferred on human rights litigants who, when applying to the ECtHR must have first exhausted all available domestic remedies, whereas applicants can seek a remedy from the CJEU through a preliminary reference from a domestic court.[23]

The enactment of the Data Retention Directive in 2006, was the most significant post-9/11 development in Europe affecting the national security/privacy rights paradigm. A critique of the Directive forms a substantial element of the research question. Some of those who held that privacy rights represented a fundamental principle of the EU complained that the Directive had betrayed this principle. McGarvey contends that it had given rise to questions being asked concerning the legitimacy of the EU by ignoring the salient principles of human rights by supplanting them in favour of the wishes of law enforcement agencies.[24] Maras contends that the Directive 'was passed with indecent haste'.[25]

The verdicts of the Constitutional Courts of Bulgaria, Romania, Germany, the Czech Republic, Slovakia and Slovenia are assessed, with Ní Loideáin highlighting a common judicial finding emerging, which centred on surveillance regimes, which emerged following the transposition of the

[21] Oddný Mjöll Arnardóttir and Antoine Buyse (eds.), *Shifting Centres of Gravity in Human Rights Protection: Rethinking Relations between the ECHR, EU and National Legal Orders* (Routledge, London and New York, 2016), p. 5.
[22] Samantha Besson. 'The European Union and Human Rights: Towards A Post-National Human Rights Institution' 6(2) (2006) *Human Rights Law Review* 323.
[23] Sionaidh Douglas-Scott, 'The European Union and Human Rights after the Treaty of Lisbon' 11(4) (2011) *Human Rights Law Review* 645, 657.
[24] Stephen McGarvey, 'The 2006 EC Data Retention Directive: A Systemic Failure' 10(1) (2011) *Hibernian Law Journal* 119, 136.
[25] Marie-Helen Maras, 'While the European Union was Sleeping, the Data Retention Directive was passed: The Political Consequences of Mandatory Retention' 6(2) (2011) *Hamburg Review of Social Sciences* 1,5.

Directive, giving rise to inadequate levels of oversight and security, falling short of the legality, necessity and proportionality requirements under Article 8 of the ECHR.[26]

The CJEU verdict in *Digital Rights Ireland* is assessed in detail. Ojanen argues that the CJEU judgment is one of the most significant ever given by the Court of Justice on fundamental rights.[27] Fabbrini describes the judgment as being the most advanced court pronouncement to data relating to privacy rights in the digital age.[28] In this connection, Ní Loideáin regards the Snowden revelations as having an influence on that landmark judgment.[29] Ojanen suggests that the *Digital Rights Ireland* judgment does not prohibit some form of mandatory data retention to combat serious crime and terrorism and that such a provision might not be incompatible with human rights.[30]

Granger and Irion suggest the *Digital Rights Ireland* judgment has moved the responsibility for human rights protection onto the EU legislator and that the prospect of EU accession to the ECHR in addition to the legal weight accorded to the EU Charter of Fundamental Rights were contributing factors.[31]

The verdicts in *Schrems* and *Google Spain* are addressed by a number of scholars, particularly in the context of the emerging and ongoing approach of the CJEU in its review of legislation governing the processing of personal data by public bodies, and as Ní Loideáin observes, in the context of the Snowden

[26] Nora Ní Loideáin, 'EU Law and Mass Internet Surveillance in the post-Snowden Era' 3(2) (2015) *Media and Communication Data* 53, 56.
[27] Tuomas Ojanen, 'Privacy is more than a seven-letter word: the Court of Justice of the European Union sets Constitutional limits on Mass Surveillance' 10(3) (2014) *European Constitutional Law Review* 528, 529.
[28] Federico Fabbrini, 'Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and surveillance in the United States' 28 (2015) *Harvard Human Rights Journal* 67-68.
[29] Nora Ní Loideáin, 'EU Law and Mass Internet Surveillance in the post-Snowden Era' 3(2) (2015) *Media and Communication Data* 53.
[30] Tuomas Ojanen, 'Privacy is more than a seven-letter word: the Court of Justice of the European Union sets Constitutional limits on Mass Surveillance' 10(3) (2014) *European Constitutional Law Review* 528,540. For the basis of Ojanen's contention, see in particular, Joined cases C-93/12, C-594/12 *Digital Rights Ireland and Seitlinger and Others*, at paragraph 42.
[31] Marie-Pierre Granger and Kristina Irion, 'The Court of Justice and the Data Retention Directive in Digital Rights Ireland; telling off the EU legislator and teaching a lesson in privacy and data protection' 39(6) (2014) *European Law Review* 835, 845.

revelations regarding mass communications data retention.[32] Rodotà observes that as the EU Charter of Fundamental Rights is legally binding, the balancing exercise in relation to national security/data privacy considerations must encompass the centrality of the provisions of the Charter.[33]

(2) United States approaches to and interpretations of the Data Privacy/National Security Balancing Paradigm pre and post-9/11

The thesis research question in relation to the United States is divided into two chapters, one dealing with the pre-9/11 era and the other dealing with the post-9/11 era.

As a starting point, the U.S. Constitution, the Patriot Act (2001) and the Freedom Act (2015) contribute *inter alia* to an understanding of the legislative background to the overall research question. The approach to the balancing paradigm in the pre-9/11 era is exhaustively analysed in the report of the Church Committee (1976), which outlines the activities and the remit of spy and intelligence agencies such as the FBI and the CIA and provides a significant account of the activities of the NSA and its secret activities. Bamford cites the Truman Memorandum, which was not publicised, as representing the 'birth certificate' of the NSA.[34]

The activities of the NSA and the availability of derogations afforded to it by Presidential Orders are evaluated by Schwartz, who observes that the NSA's ability to intercept the communications of U.S. citizens was not subject to constitutional restriction or oversight, thus running counter to the provisions of the Fourth Amendment.[35]

Yoo highlights the thinking which prevailed in the U.S. post-1945 among security-conscious administrators, who held that when serious threats to

[32] Nora Ní Loideáin, 'EU Law and Mass Internet Surveillance in the post-Snowden Era' 3(2) (2015) *Media and Communication Data* 53.
[33] See Stefano Rodotà, 'Data Protection as a Fundamental Right' in Serge Gutwith et al, (eds), *Reinventing Data Protection*? (Springer, New York, 2009) 77-82.
[34] James Bamford, *The Puzzle Palace: A Report on America's Most Secret Agency* (Penguin 1983). Cited in Robert N. Davis, 'Striking the Balance: National Security vs. Civil Liberties' *Brooklyn Journal of International Law* 29 (1) (2003-04) 182, fn 44.
[35] Paul M. Schwartz, 'Germany and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance' *Hastings Law Journal* 54 (2003) 764.

national security existed, conventional privacy rights, guaranteeing protection from unwarranted interference from surveillance agencies as enshrined in the Fourth Amendment could not inhibit the fight against such threats, even if this meant having recourse to unfettered presidential discretion' in matters of surveillance.[36]

The Recommendations of the Church Committee Report are analysed in an extensive literature. Bloom and Dunn observe, for example, that the NSA *Shamrock* operation had become illegal having violated the Fourth Amendment and the Communication Act of 1934 as soon as it began to target United States citizens and domestic terminals, which they attribute to the programme having 'expanded beyond its initial scope and initial justification'.[37]

One of the salient findings of the Church Committee was the undesirability of the secrecy afforded to agencies such as the NSA which was deemed to place constraints upon the liberty of Americans.[38] One of the reforms which emerged in the aftermath of the Church Committee was the promulgation of the Foreign Intelligence Surveillance Act, 1978 (FISA), which Rubenfeld observes was intended to create a legislative framework of judicial oversight while still enabling the Executive to promote intelligence gathering, but involving 'substantive procedural requirements'.[39] Birkenstock notes that the policy of the Executive in the pre-FISA era was evidenced in 1954 when the Attorney General issued a Directive to the FBI to engage in warrantless searches and seizures, if necessary by surreptitious means when the FBI deemed that such actions were necessary to uphold national security interests.[40]

---

[36] John Yoo, 'The Terrorist Surveillance Program and the Constitution' *Georgia Mason Law Review* 14 (2007) 565, 586-87. See also Jed Rubenfeld, 'The End of Privacy' *Stanford Law Review* 61 (2008) 101 and Joseph D. Mornin, 'NSA Metadata Collection and the Fourth Amendment' *Berkley Technology Law Journal* 29 (2006) 985.

[37] Robert Bloom and William J. Dunn, 'The Constitutional Infirmity of Warrantless NSA Surveillance: The Abuse of Presidential Power and the Injury to the Fourth Amendment' 15 (2006) *William and Mary Bill of Rights Journal* 147, 158.

[38] Church Committee Report, Book, 1, 9.

[39] Jed Rubenfeld, 'The End of Privacy: Presidential Power and the Fourth Amendment' 61 (2008) *Stanford Law Review* 101, 158.

[40] Gregory E. Birkenstock, 'The Foreign Intelligence Surveillance Act and Standards of Probable Cause: An Alternative Analysis' 80 (1992) *Georgetown Law Journal* 843, 846-49.

Brand, however, cites the Foreign Intelligence Surveillance Court (the FISC) as being the 'Achilles heel' of the FISA as it serves to preserve secrecy surrounding warrants issued by the FISC almost solely on the basis of information provided by the Executive, which Brand criticises for the absence of parties opposed to the granting of such warrants, the cross-examination of government witnesses and the submission of arguments opposing the granting of warrants.[41]

In a similar vein, Berman comments that the FISC procedure fails to scrutinise sufficiently any government justification for bulk data collection programmes, and that complex legal questions attaching to such programmes are determined by whichever presiding judge is tasked with adjudicating upon such questions at any given time, the decision of this judge on such matters representing the final determination.[42]

Sinah observes that, between 1978 and 2001, the U.S. government submitted 13,102 requests to the FISC to eavesdrop on Americans, with the FISC requiring modifications in relation to two of these requests, ultimately approving all of them.[43] Breglio contends that should more people become aware of how the FISC operates, this realisation would give rise to 'uproar' in relation to its 'seemingly undemocratic procedures'.[44]

Sievert, however, offers a contrary view of FISA and contends that by obligating the government to demonstrate probable cause before communications are intercepted, such an exacting standard, not mandated by the U.S. Constitution, has thwarted the collection of data necessary for

[41] Jeffrey S. Brand, 'Eavesdropping on our Founding Fathers: How a Return to the Republic's Core Democratic Values Can Help Us Resolve the Surveillance Crisis' 6 (2015) *Harvard National Security Journal* 1. ibid.
[42] See Emily Berman, 'The Two Faces of the Foreign Intelligence Surveillance Court' 91 (2016) *Indiana Law Journal* 1191, 1193.
[43] Alex G Sinah. 'NSA Surveillance Since 9/11 and the Human Right to Privacy' 59 (2013) *Loyola Law Review* 861, 874.
[44] Nola K. Breglio, 'Leaving FISA behind: The Need To return to Warrantless Surveillance' 113 (1) (2013) *Yale Law Journal* 179, at 190.

intelligence purposes and has 'already endangered the safety of U.S. citizens in numerous reported terrorist cases'.[45]

Yoo, however, condemns the proroguing of the Total Awareness Programme as representing a 'libertarian overreaction' and postulated that critics of similar programmes only served to limit government power while engaged in a 'tough war'.[46] Solove contends that the NSA's warrantless surveillance programme violated the FISA but the government felt able to justify the TSP as part of the fight against terrorism.[47]

In relation to the post-9/11 era in the United States there is extensive commentary on the deployment by the Bush Presidency of Executive Orders.[48] Rudalevige provides a comprehensive account of how this tool was relied upon to considerable effect during the post-9/11 epoch of the Bush Presidency.

Pfiffner analyses the approach of the Bush Presidency to measures adopted in the fight against terrorism and comments that this approach undermined the separation of powers principle as Bush claimed he had the authority to ignore elements of statutes of which he disapproved and which impinged upon his own prerogatives, in the process refusing to accept the legitimacy of Congress or the Courts in restricting his authority.[49]

---

[45] Ronald Sievert, 'The Foreign Intelligence Surveillance Act of 1978 Compared with the Law of Electronic Surveillance in Europe' (2016) 43(2) *American Journal of Criminal Law* 125, 128. See Also Ronald J. Sievert, 'Time to Rewrite the Ill-Conceived and Dangerous Foreign Intelligence Surveillance Act of 1978' 3(1) (2014) *National Security Law Journal* 47, 82-92.

[46] John Yoo, 'The Terrorist Surveillance Program and the Constitution' 14(3) (2007) *George Washington Law Review* 565, 580.

[47] Daniel J. Solove, *Nothing to Hide. The False Tradeoff between Privacy and Security* (Yale University Press, 2011) 82.

[48] Andrew Rudalevige, *The New Imperial Presidency. Renewing Presidential Power After Watergate*. (The University of Michigan Press, 2005)

[49] James P. Pfiffner, 'The Contemporary Presidency. Constraining Executive Power: George W. Bush and the Constitution' 31(1) (2008) *Presidential Studies Quarterly* 123, 140.

Balkin and Levison view the National Surveillance State as a means of identifying and resolving difficulties encountered by the Government by means of the collection of information and data,[50] while Solove contends that the 'war-powers argument,' enables the President to bypass the law.[51]

Schneier assesses whether the various measures and initiatives taken to combat acts of terror have in fact given rise to greater levels of security or the mere feeling of security, concluding that measures taken since 9/11 have needlessly deprived many people of liberty and invaded privacy in the process.[52]

Johnson comments that in the period from 1975 to 2008, members of Congress have exhibited varying levels of commitment in relation to intelligence supervision and distinguishes four kinds of response among those calling for greater levels of accountability.[53]

Zedner argues, in the context of the extension of data protection powers, that fundamental rights should never be sacrificed on the basis of consequentialist claims that security is enhanced.[54]

[50] Jack M. Balkin and Sandford Levinson, 'The Process of Constitutional Change: From Partisan Entrenchment to the National Surveillance State' 75(2) (2006) *Fordham Law Review* 489, 490; Jack M. Balkin, 'The Constitution in the National Surveillance State' 93(1) (2008) *Minnesota Law Review* 1 2.
[51] Daniel J. Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security* (Yale University Press, 2011) 82-3.
[52] Bruce Schneier, *Beyond Fear. Thinking Sensibly About Security in an Uncertain World* (Copernicus Books, New York, 2003) 38 and 249.
[53] Loch K. Johnson, 'Ostriches, Cheerleaders, Skeptics and Guardians: Role Selection by Congressional Intelligence Overseers' 28(1) (2008) *SAIS Review* 93, 98-101.
[54] Lucia Zedner, *Security: Key Ideas in Criminology* (Routledge, London, 2009) 136.

Etzioni highlights the hurried drafting and passage of the Patriot Act, which evoked opposition from civil liberties groups.[55] Gilbert emphasises an aspect of the Patriot Act, which makes obtaining search warrants easier for law enforcement agencies, the granting of such warrants by one federal Judge in relation to communications providers in multiple states, thus streamlining the search process.[56] Schneier contends that the Patriot Act was never intended to permit mass surveillance, based on the language used in the Act.[57]

Balkin cites the Foreign Intelligence Surveillance Amendments Act, 1978 as representing a further erosion of data privacy rights by retroactively legalising the warrantless surveillance programme and giving immunity to telecommunications companies which had participated in the secret NSA programme.[58] In this regard, Warren and Dirksen point out that President Obama's approach to the balancing of national security objectives with privacy rights was not dissimilar to that of his predecessor.[59]

The Snowden revelations regarding the NSA and the various bulk communications data retention programmes, most notably PRISM, are examined in detail by Greenwald,[60] Gellman and Poitras,[61] MacAskill[62] and Harding,[63] with the implications these have for the privacy rights of American and US citizens critiqued.

[55] Amitai Etzioni, 'Imperfections of Select New Technologies for Individual Rights and Public Safety,' 15(2) (2002) *Harvard Journal of Law and Technology* 258-290, 286 , fn 191.
[56] Francois Gilbert, 'Demystifying the United States Patriot Act' *Journal of Internet Law* 16(8) (2013) 1, 3-4.
[57] Bruce Schneier, *Data and Goliath: The Hidden Battle to Collect Your Data and Control Your World* (W.W Norton, New York and London 2015) 173.
[58] Jack M. Balkin, 'The Constitution in the National Surveillance State' 93 (2008) *Minnesota Law Review* 1, 2.
[59] Aiden Warren and Alaxendar Dirsken, 'Augmenting State Secrets: Obama's Information War' 9(1) (2014) *Yale Journal of International Affairs* 68-84, 68.
[60] Glenn Greenwald, 'NSA Collecting phone records of millions of Verizon Callers daily.' *The Guardian* June 6, 2013.
[61] Barton Gellman and Laura Poitras, 'U.S., British intelligence mining data from nine U.S. internet companies in broad secret programme' *Washington Post* June 6, 2013.
[62] Ewen MacAskill, 'Obama defends "system of checks and balances" around NSA surveillance' *The Guardian* 17 June 2013
[63] Luke Harding, *The Snowden Files* (Random House, 2014) 314.

Deflem and McDonough illustrate the changing attitudes of Americans to data retention post-9/11 up to 2011 and in the aftermath of the Snowden revelations, indicating that in 2013, 53% of Americans disapproved of Government surveillance programmes.[64] Owens illustrates that in the aftermath of measures taken post-9/11 by President Bush, his approval rating rose by 35 points to 87 per cent, the highest increase in American history.[65]

Forsyth assesses the USA Freedom Act, 2015 as an attempt it to balance national security objectives with privacy rights, noting the difficulty in even achieving this balance.[66] Berman notes the absence of a special advocate attaching to the Act's provisions.[67] Mondale, Stein and Fischer emphasise that the provision of an *amicus curiae*, pursuant to Section 401 of the Act does little but offer a token form of opposition during FISC proceedings and does not give rise to meaningful levels of oversight.[68] In this connection, Squitieri contends that the amicus provision in the Act amounts to little more than a diluted version of the absent special advocate.[69]

Reidenberg, with reference to recent jurisprudence dealing with interpretations of the Fourth Amendment, contends that lack of constitutional standards relating to data access, seems to endure.[70] Kerr, in the context of emerging and rapidly developing technologies, contends that such technological change is preferably regulated by way of legislative, as opposed to constitutional provisions.[71] Pell and Sogohian stress that for law to match the pace of developing surveillance technologies, a reliable procedure must be developed

[64] Mathiew Deflem and Shannon McDonough, 'The Fear of Counterterrorism: Surveillance and Civil Liberties since 9/11' 52(1) (2015) *Global Society* 70, 77.
[65] John E. Owens, 'Presidential Power and Congressional Acquiescence in the "War" on Terrorism: A New Constitutional Equilibrium?' 34(2) (2006) *Politics and Policy* 258, 259.
[66] Bart Forsyth, 'Banning Bulk: Passage of the USA Freedom Act and Ending Bulk Collection 72 (2015) *Washington and Lee Law Review* 1307, 1351.
[67] Emily Berman, 'Two Faces of the Foreign Intelligence Surveillance Court' 91(4) (2016) *Indiana Law Journal* 1191
[68] Walter R Mondale., Robert A. Stein and Caitlinrose Fisher, 'No Longer a Neutral Magistrate: The Foreign Intelligence Surveillance Court in the Wake of the War on Terror' 100(6) (2016) *Minnesota Law Review* 2251, 2296.
[69] Chad Squitieri, 'The Limits Of The Freedom Act's Amicus Curiae' 11(3) (2015) *Washington Journal Of Law, Technology and Arts* 197, 199.
[70] Joel R. Ridenberg, 'The Data Surveillance State in the United States and Europe' 49 (2014) *Lake Forrest Law Review* 583, 588.
[71] Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for* Caution' 102 (2004) *Michigan Law Review* 801, 805.

enabling Congress to be aware of the functions, capabilities and historical use of surveillance technologies.[72]

Kerr queries the adequacy of domestic US governance of Internet-related concerns and particularly how the existing Fourth Amendment doctrine can be applied outside US borders,[73] but does not entertain the promulgation of a new Fourth Amendment.[74]

(3) The EU and US Compared in their approaches to the National Security/Data Privacy Balancing Paradigm

Schwartz and Reidenberg establish that in the US privacy has been held to equate with the right to do what one wants without state interference, while privacy is not viewed as being a form of property, entailing the right not to be subjected to surveillance. On the other hand in Europe, both the Council of Europe and the European Union have been proactive in regulating the uses of personal data, something the U.S. authorities have refrained from doing.[75] Whitman contends that a European assertion to respect for a fundamental right to privacy is weak or absent in the cultural context of the US.[76]

[72] Stephanie K. Pell and Christopher Soghoian, 'A Lot more than a Pen Register and Less than a Wiretap: What the Stingray teaches us about How Congress should approach the Reform of Law Enforcement Surveillance Authorities' 16 (2016) *Yale Journal of Law and Technology* 134, 169.
[73] Orin S. Kerr, 'The Fourth Amendment and the Global Internet' 67 (2015) *Stanford Law Review* 285, 286.
[74] Orin S. Kerr, 'Do We Need A New Fourth Amendment' 107(6) (2009) *Michigan Law Review* 951,966.
[75] Paul M. Schwartz and Joel Reidenberg, 'Data Privacy Law: A Study of United States Data Protection' (Charlottesville, Virginia, Michie 1996): Julia .M Fromholz, 'The European Union Data Privacy Directive.' 15 (2000) *Berkeley Technology Law Journal* 461.
[76] James Q. Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' 113 (2004) *The Yale Law Journal* 1151, 1157.

Anderson argues that by reference to the ECHR and the EU Charter of Fundamental Rights, American law is perceived from a European standpoint to have failed.[77] Bender, in assessing which regime enjoys greater levels of privacy, refers to a 2006 study which finds that levels of privacy in the U.S. were somewhat higher in the US than in the EU.[78] Bender, when commenting on the situation in 2015 holds that it remains unclear whether the relative balance between the two regimes has changed materially.[79]

Bignami contrasts the ability of the President of America to issue a secret surveillance order to the NSA with the position in France and Germany, where proposals for government data mining, even on the pretext of national security requirements, would have to be reviewed by an independent regulator.[80]

Balkin observes that a vast amount of personal information is not protected by the Fourth Amendment,[81] while Alphran illustrates that US Courts have progressively eroded the force of the Fourth Amendment which is the basis of US personal data protection.[82] In this connection, Amsterdam comments that case law emerging from the US Supreme Court lacks clarity and consistency in relation to the interpretation of the Fourth Amendment, [83] while Wassterstrom and Seidman contend that some of the Court's decisions have been inconsistent and bizarre and have left the Fourth Amendment undefended.[84]

---

[77] See David A. Anderson, *The Failure of American Privacy Law, in* Protecting Privacy 139 (Basil S. Markesinis ed., 1999) 139.
[78] David Bender, 'E.U. or U.S. : which has more actual privacy? 21(1) (2015) *Computer Law and Security Review* 18.
[79] ibid, 19, fn 12.
[80] See Francesca Bignami, 'European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining,' 48 3(3) (2007) *Boston College Law Review* 609, 655.
[81] Jack M. Balkin, 'The Constitution in the National Surveillance State,' 93 (2008) *Minnesota Law Review* 1, 19.
[82] Derek M. Alphran, 'Changing Tides: A Lesser Expectation of Privacy in a Post-9/11 World' 13(1) (2009) *Richmond Journal and The Public Interest* 89, 120.
[83] Anthony G. Amsterdam, 'Perspectives on the Fourth Amendment' *Minnesota Law Review* 58 (1974) 4(3) 349-477, 349.
[84] Silas J Wasserstrom and Louis Michael Seidman, 'The Fourth Amendment as Constitutional Theory' 77 (1988) *Georgia Law Journal* 19, 29.

Normative Considerations

Solove contends that with regard to the balance between national security objectives and data privacy rights, it should not be assumed that the two concepts are mutually exclusive.[85] Davis observes that the protection of data rights must yield to the larger national interest.[86]

Zedner distinguishes the rights to privacy and national security from each other, arguing that they are separate and discrete social values and that neither should be traded against the other.[87] Raab cautions that there is no method of ascertaining whether parity exists between the two concepts being weighed in the balancing exercise and such a balance depends on subjective judgment.[88]

Bennett suggests that arriving at a balance could depend upon political negotiation, political consensus, or authoritative assertion.[89] Rengel contends that as human rights guarantors, states are obliged to balance the rights of an individual, including data privacy rights, against the general welfare of society.[90] Schauer comments that only arguments based on national security considerations possess the requisite normative force to justify the setting aside of fundamental rights,[91] with Kumm emphasising that only reasons that are proportional, under the circumstances, can properly be classified as compelling.[92]

Barak advocates the adoption of a principled balancing approach, involving a series of balancing tests, which involve measuring the importance of the rights

---

[85] This case is argued by Daniel J. Solove, *Northing to Hide: The false Tradeoff Between Privacy and National Security* (Yale University Press, 2001) 34.
[86] See generally, Robert N. Davis, 'Striking the Balance: National Security vs. Civil Liberties,' 29(1) (2003-04) *Brooklyn Journal of International Law* 178-238.
[87] See Lucia Zedner, *Security: Key Ideas in Criminology* (London, Routledge, 2009), 135-6.
[88] Charles D. Raab, 'From Balancing to Steering: New Directions for Data Protections' in Colin J. Bennett and Rebecca Grant (eds.) *Visions of Privacy for the Digital Age* (University of Toronto Press, 1999) 68-93, 69.
[89] Colin J Bennett and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (MIT Press, Cambridge Massachusetts, 2007) 13.
[90] Alexandra Rengel, *Privacy in the 21st Century* (Hotei Publishing, Leiden, 2014) 88.
[91] See Frederick Schauer, 'A Comment on the Structure of Rights,' (1993) 27 *Georgia Law Review* 415-34.
[92] See Mattias Kumm, 'Constitutional Rights as Principles. On the Structure and domain of Constitutional Justice. A review essay on A Theory of Constitutional Rights' 2(3) (2004) *International Journal of Constitutional Law* 574, 595.

in question and the nature of the impending restriction.[93] Aquilina, in this connection, suggests that the least privacy-invasive technologies should be used by governments. Additionally, he urges an emphasis on accountability, transparency, proportionality, fairness, purpose specification, informed consent, legality, purpose limitation and non-retention of data beyond a given timeframe, the right of access by the subject of surveillance to material concerning him or her, and the right of rectification where necessary.[94]

Chandler observes that where security and privacy rights are in competition, the human desire for security trumps data privacy.[95] Rivkin Jr, in the context of the Bush administration's response to the September 11 2001 attacks, comments that liberty and public safety are balanced differently during peacetime and times of war.[96] Alexy argues that the balancing exercise can be conducted in an effective manner and contends that arguments holding that balancing is inherently irrational and subjective are unjustified.[97]

Dworkin, an advocate of the proposition that it is not appropriate to seek to balance a human right such data privacy against national security, does accept that those asserting a claim that citizens have rights against a government, need not extend that argument to rule out instances where such a right can be abrogated, where the protection of others is at stake.[98]

[93] Ahraon Barak, 'Proportionality and Principled Balancing' 4(1) (2010) *Law and Ethics of Human Rights* 1
[94] Kevin Aquilina, 'Public security versus privacy in technology law: A balancing act?' 26(2) (2010) *Computer Law and Security Review* 130, 140-142.
[95] See Jennifer Chandler, 'Privacy Versus National Security: Clarifying the Trade-Off' in Ian Kerr, Valerie Stevens and Carole Lucock (eds)., *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (Oxford University Press, 2009) 131-138.
[96] David B. Rivkin Jr., 'Answering the Critics of the Legal Case for the War on Terror' 32(2) (2009) *Harvard Journal of Law and Public Policy* 485, 486.
[97] Alexy's approach to balancing is outlined in Robert Alexy, *A Theory of Constitutional Rights* (Oxford University Press, 2002).
[98] See Ronald Dworkin, *Taking Rights Seriously* (Harvard University Press, 1977) 191.

Overall Introduction

The geographical scope of the thesis as a whole is limited to the U.S.A. and Europe. In the context of a treatment of the privacy/security balance in the technological age, it would make little sense to deal with either Europe or the U.S.A. in isolation, if only because by far the greater number of content and service providers on which Europe relies are based in the U.S.A. There is the further important consideration that, especially since 11 September 2001, United States and European security agencies have been routinely engaged in in data sharing for retention purposes. In respect of data retention and data sharing, governments and security agencies on both sides of the Atlantic have common goals, based on common perceptions of the source of threats to their security. However, when understandings of privacy are in question, the situation is quite different. When one is considering the legal and cultural significance of privacy in a transatlantic context, one is confronted with two contrasting understandings of the concept. For that reason, the privacy/security balance in the U.S.A. and that in Europe are best treated separately and then contrasted.

The overall research question addressed in this thesis is the data privacy/national security balancing paradigm, and how this functions in Europe and the United States. At issue here are the limits on, and oversight of, the use of surveillance by government agencies for the collection and retention of telecommunications data in the interest of national security. The thesis is structured as follows. The first part, (Chapter One) is devoted to European attitudes and practices in relation to the balancing paradigm. This will involve a consideration of the part played in the determination of this balance by two European political systems: the Council of Europe and the European Union. This consideration will embrace an analysis of the influence of each of these systems on the other in the context of the data privacy/national security balance.

In the first section of Chapter One, the focus is on the Council of Europe, in particular on its landmark instrument of privacy law, the 1950 Convention for the Protection of Human Rights and Fundamental Freedoms (the ECHR), and

on the 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data, which provides the basis for the data privacy/national security paradigm with which the thesis as a whole is concerned. The jurisprudence of the Court of the Council of Europe, the ECtHR, will be scrutinised with a view to establishing the degree to which that court is prepared to restrict data privacy rights when it deems that a threat to national security is sufficiently serious to warrant such a restriction. A further significant issue examined is the influence of the principles enunciated by the ECHR on European legal systems. The chapter will also analyse what privacy means at national level: how various European State constitutional systems deal with the balance between an individual's right to privacy and the demands of national security. Consideration will be given to the fact that these constitutional systems display marked variations in their treatment of this balance, and to the consequent problems raised by the task of reconciling the single set of constitutional ideals at wider Council of Europe and EU level on the balance with diverse understandings at national level. At a judicial level, in the case of the ECtHR in particular, dealing with this problem involves the deployment of the doctrine of the Margin of Appreciation, which affords a degree of latitude to states in their observance of the principles laid down in the ECHR. The implications of the use of this doctrine will be analysed in the first part of Chapter One, which closes with a discussion of the ways in which the Council of Europe rights system influences the rights law of the European Union.

The second part of Chapter One deals with the European Union (EU) law on data privacy and on the restrictions that may be lawfully imposed on the data privacy rights of citizens when national security is deemed to be under threat. The EU is a federation of 27 European States. Some Member States of the Council of Europe are also members of the EU. One of these States, the United Kingdom, has voted by referendum to leave the EU. The EU has an Executive, a Legislature and a Judiciary. The European Commission acts as the Executive of the EU by implementing the policies decided by the European Council and the European Parliament. The 27 members of the Commission, one being nominated by each Member State, also make proposals as to what the policies they are implementing should be. The Council of the EU, known as the

Council of Ministers, is the main political institution of the EU, and is made up of one representative of each of the Member States. The council has the task of defining the overall political direction and priorities. Its membership comprises the heads of state or government of the Member States, along with the President of the Council and the President of the European Commission. The High Representative for Foreign Affairs and Security Policy of the EU also takes part in its proceedings. Legislative enactments such as Directives are officially described as being 'of the European parliament and of the Council,' which between them constitute the EU legislature. The Presidency of the Council is held in rotation by each Member State for a period of six months. This temporary measure is in place due to the failure to ratify the office of a full-time Presidency in the Constitutional Treaty. The judicial branch is the CJEU, the Court of Justice of the European Union.

The second section of Chapter One begins by dealing with the EU Primary and Secondary Law, the former embodied in the Lisbon Treaty on the European Union, the Treaty on the Functioning of the European Union, and the Charter of Fundamental Rights of the European Union. The Regulations, Directives are Decisions of the EU are commonly regarded as Secondary EU Law. The main legal EU instrument on data protection is Directive 95/46/EC. Others are 97/66/EC and Directive 2002/58/EC, which deal with the processing of personal data and the protection of privacy in the electronic communications sector. The implications for the data privacy/national security balance because of these instruments, and, above all, of the first EU Data Retention Directive, 2006/24/EC, are explored at length in the remainder of Chapter One.

Among the matters examined are the negative responses to the Data Retention Directive from a variety of sources: Member States of the EU, Constitutional Courts in these states, the European Data Protection Supervisor and the European Commission. The striking down of the Directive by the CJEU, the reasons for the Court's judgment and the implications of the judgment for the data privacy/national security balance, are considered at length, as are the consequences of the judgment for the increasing reputation of the CJEU as the primary European defender of data privacy rights.

The far-reaching implications of another major judgment delivered by the CJEU in 2015 in the case of *Schrems v Data Protection Commissioner*[1] are also examined. Schrems based his case on the claim that some or all of the data provided by him to Facebook were transferred from Facebook's Irish subsidiary to servers located in the United States and processed there. Schrems argued that in the light of revelations made by Edward Snowden concerning the privacy-invasive practices of U.S. intelligence services, the law and practice of the U.S. did not offer adequate protection against surveillance by public authorities of the data transferred there. The CJEU found in favour of Schrems, and went on to find that the Safe Harbour Agreement between the EU and the U.S. was supposed to prevent private companies and organisations in the U.S. or EU, which store data, from accidentally disclosing, or losing, personal information.

From the perspective of the data privacy/national security balance, the fundamental problem, as the CJEU pointed out, was that the national security, public interest and law enforcement objectives of the U.S. prevail over the Safe Harbour Agreement, which enabled interference with the data privacy rights of EU citizens, who had no administrative or judicial means of redress. The Schrems judgment implies that U.S. authorities cannot be trusted to respect the privacy rights of EU citizens where those data are transferred to the U.S. The discussion of the implications of the CJEU *Schrems* judgment dealing with future transfers of communications data from Europe to the U.S. looks forward to issues discussed in Chapters Two and Three and maintains a continuity with a central theme of the thesis: the contrast between the EU and the U.S. positions on the data privacy/national security balancing paradigm, and the prospect of reconciling these positions.

At this point in Chapter One, attention is focused on the contrast between the EU and U.S. positions on interferences with data privacy rights and how these rights should be balanced against national security interests.

The structure followed in Chapter Two, the first of two Chapters dealing with the United States, mirrors that followed in Chapter One. The relevant rights

[1] Case C-362/14, 6 October, 2015.

and their underpinning are first set out, followed by an examination of the ways in which these rights are infringed, or limited by the demands of national security. An exposition of the illegal infringement of privacy rights is followed by a discussion of the legislative response to such infringement, and an analysis of the measures introduced to curb the abuse by the Executive of the privacy rights of citizens, and of the effect of these measures on the adjustment of the data privacy/national security balance. The Chapter also deals with the problems associated with the carrying out of a balancing exercise involving rights which are qualitatively different and the philosophical issues underlying the data privacy/national security balancing paradigm.

Chapter Three deals with the Data Privacy/National Security Balance in the United States from September 11, 2001 to the present. A central theme explored in this chapter is the position adopted by the Bush Administration that at times when State security is in jeopardy, the President has the inherent power to determine what the law is when National Security issues are being addressed. The President, with the support of the legislature, assumed the authority to take whatever pre-emptive action he chose to deter and prevent acts of terrorism. The action he chose to take was to give secret orders to the National Security Agency (NSA) to engage in the mass collection of domestic phone calls and other telephony data of U.S. citizens. The NSA engaged in this process without seeking warrants or Court orders, thus violating the Foreign Intelligence Surveillance Act. Chapter Three underlines the differences between U.S. and European practices in the context of terrorist threats to national security. It also analyses the U.S. Administration's defence of its post-9/11 surveillance policies, and objections to these policies from scholarly sources. Normative arguments in defence of the erosion of privacy rights are also assessed, as a means of achieving a better understanding of U.S. surveillance policies post-9/11. Legislation such as the Patriot Act, which provided a number of mechanisms by which the Bush Administration could override previous legal controls on privacy-invasive methods of intelligence-gathering, is also examined.

The chapter, in dealing with the early attitude of the Obama Administration to data privacy/national security issues, stresses the continuity between the two

Administrations, and also later moves by the Obama Administration to moderate the privacy-invasive policies of the previous one. In this context, the Freedom Act introduced in Congress has a special significance, as have Obama's measures designed to reform the Foreign Intelligence Surveillance Court. The exposure by Edward Snowden in 2013 of the true nature and massive scope of U.S. and UK surveillance and its detrimental effects on data privacy rights is examined in detail, as is the international significance of Snowden's widely-publicised revelations. These revelations have moved the debate about U.S. surveillance practices from being a domestic U.S. issue to becoming an international one. The chapter discusses the reasons for finding NSA surveillance programmes failing to meet the standards set by the UN Convention on Civil and Political Rights. There is also some consideration of evidence suggesting that the surveillance programmes mandated by U.S. Administrations post-9/11 did little to protect the U.S. from security threats. The chapter further deals with the recent reconsideration by the U.S. Supreme Court of the constitutionality of mass data mining and long-term surveillance in the context of Fourth Amendment data privacy rights. In a number of cases, the Court moved to enhance privacy rights by remedying some previous deficiencies in the application of the Fourth Amendment doctrine.

These considerations come to a head in Chapter Four. Here, the emphasis is on the differences between the U.S. and Europe on the question of what privacy means and should mean, in attitudes to data privacy protection and its importance relative to other social goods such as National Security and freedom of speech. In the previous three chapters, aspects of these differences have been highlighted from time to time, particularly when U.S. privacy protection stands in marked contrast to that in Europe. Identifying these contrasts between the jurisdictions, in conjunction with existing privacy protection provisions common to both and the commonalities emerging from recent U.S. Supreme Court privacy-enhancing jurisprudence and various pieces of legislation tending in the same direction, is useful when one is trying to determine the feasibility of devising a principled data privacy/national security balancing paradigm which might find acceptance in both the U.S. and Europe. This topic is further explored in the overall conclusion to the thesis.

Chapter One

The Privacy/National Security Balance from a European Perspective

Introduction

The overall research question addressed in this chapter is how the European legal order, centrally as well as individually, looks at the interplay between privacy (specifically data privacy) and national security, as this is played out in the Council of Europe (COE) and European Union (EU) legal systems, as well as at Member State Constitutional, legislative, jurisprudential and political levels.

The chapter will first look at how the primary law of the COE, embodied in such instruments as the 1953 Convention for the Protection of Human Rights and Fundamental freedoms (the ECHR) and the 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention 108), provides the basis for the data privacy/national security balancing paradigm with which the thesis as a whole is concerned. For example, Article 8(2) of the ECHR lays down the conditions for legitimate restrictions which can be placed on privacy rights. The case law of the Court of the COE, the ECtHR, will be analysed with a view to establishing how that Court is prepared to restrict data privacy rights when it deems that a threat to national security is sufficiently severe to warrant such a restriction.

A parallel analysis will be applied to primary and secondary EU law as this relates to the data privacy/national security balance, and to how the Court of Justice deals with the balancing paradigm as this is outlined in the relevant primary law provisions of the Charter of Fundamental Rights of the EU (the CFR), the Lisbon Treaty on European Union (TEU), 2007 and the Treaty on the Functioning of the European Union, (TFEU), 2010. Among the relevant secondary EU law measures, two Directives will be subject to particular attention: Privacy Directive 95/46/EC, designed to give substance to the principle of the right to data privacy already enshrined in Convention 108 of the COE, and the European Data Retention Directive, 2006/24/EC, a politically-motivated response to terrorist activities in Europe and elsewhere.

The difficulties experienced throughout the EU arising from the implementation of this latter Directive and the consequent calls to have it annulled will be analysed, as will the ruling delivered by the Grand Chamber of the CJEU on 8 April 2014, which held that Directive 2006/24/EC was invalid *ab initio*.

Given that this ruling marks the point at which the highest Court in Europe is determining the data privacy/national security balance in the context of data protection, it has multiple implications for the central theme of this chapter and for the thesis as a whole. It thus warrants detailed consideration in the context of emerging trends, in particular the growing assertiveness of the CJEU as the primary defender of data protection rights in Europe, thus making a notable shift in the way European legal systems must interpret the data privacy/national security balance in the future, mandating as it has a significant enhancement of privacy protection.

The chapter will also deal with the intensification of this trend in the jurisprudence of the CJEU following the Grand Chamber judgment on the Data Retention Directive.[1] This judgment was followed by one which requires content providers such as Google to remove links emanating from search engines to types of information on individuals deemed to be outdated or incorrect. This in turn was followed by the Schrems case,[2] in which the CJEU invalidated the 'Safe Harbour' agreement between the EU and the U.S.A., drawn up in 2000, which allowed U.S. companies to transfer the personal data of Europeans to the U.S.A.[3]

Consideration of what those developments and other cognate ones mean for the data privacy/national security balance will be followed by an analysis of the extent to which the ECHR data privacy rights play into EU systems, and of

[1] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others*. Grand Chamber CJEU, 8 April 2014. The details of this ruling will be discussed.
[2] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* Judgment of 6 October 2015.
[3] 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML.> accessed 13 July 2016.

how the CJEU has traditionally looked to the ECHR and the jurisprudence of the ECtHR to establish new rights, especially in the area of data privacy, with consequences for the privacy/security balance. In this context another related issue will also be considered: the long-projected accession of the EU to the ECHR, which has been a regular feature of the EU integration debate for over three decades, the desirability or otherwise of such an accession, the obstacles facing it and the case-law arising from it.

The chapter will then analyse what privacy means at EU Member State (National) level, and how the various European state constitutional systems deal with the balance between the individual's right to data privacy and the demands of national security. In this context, consideration will be given to the fact that these constitutional systems display considerable variations in their treatment of this balance, and to problems raised by the task of reconciling the single set of European constitutional ideals at EU and COE level on the data privacy/national security balance with diverse understandings among Member States of how the private sphere many be sacrificed to other values such as State security. In this context a further complicating factor will also be considered: the tendency of the political establishments in some EU Member States to regard CJEU and ECtHR rulings and EU Directives as constituting unacceptable interferences with national sovereignty. In many cases, Governments in these Member States may be facing challenging political realities, including threats to national security, and in such circumstances may feel that the defence of privacy rights represents a troublesome technicality or an esoteric luxury imposed by unelected European courts. (ECtHR and CJEU).

How the ECtHR and the CJEU deal with this problem will be the subject of detailed analysis, which will involve some consideration of the deployment of the Margin of Appreciation Doctrine by the ECtHR and to a lesser extent by the CJEU, in the specific context of the data privacy/national security balance. This Doctrine deals with the latitude permitted to Member States in their observance of the principles laid down by the ECHR.[4]

[4] See Section One: The Council of Europe 4.0.

A wider issue addressed in this chapter, is the increasing disparity between the legal principles laid down by the European legal order in respect of the balance to be struck between data privacy and national security, and the widespread privacy-invasive practices informing contemporary European surveillance schemes. Since June 5, 2013, when the whistleblower Edward Snowden began to provide details of the near-universal mass data surveillance programmes of the U.S. Government, and corresponding U.K. programmes, the European Parliament instructed the Committee on Civil Liberties, Justice and Home Affairs (LIBE) to conduct an enquiry on how the programme revealed by Snowden affected the fundamental rights and freedoms of Europeans. The Centre for European Policy Studies, (CEPS) also conducted a study on the compatibility with EU law of the mass surveillance of personal data by EU Member States and examined data surveillance activities in five Member States: the UK., France, Germany, Sweden and The Netherlands. The detailed report by the CEPS revealed that intelligence agencies in those countries, with government connivance, had been engaged in large-scale surveillance activities, the mass collection of personal data, and the sharing of these data with their counterparts in other states. The LIBE enquiry reached similar conclusions.

The questions raised by this paradoxical situation, insofar as it impinges on the privacy/national security balance will be explored in this chapter, in particular whether the elaborate legal safeguards for the protection of personal data devised by the COE, the EU and the Member States may now be regarded as merely aspirational gestures, at odds with everyday reality, and giving rise to considerable implications for the actual privacy/national security balance.

Among the legal safeguards for data privacy emanating from the Data Protection Directive (95/46/EC), was the establishment in Member States of Data Protection Commissioners with responsibility for enforcing compliance with the provisions of Data Protection Acts on data controllers. Provision was also made for the appointment of a European Data Protection Supervisor by the European Parliament and Council for a five-year period.

The independence and role of the EU Member State Data Protection Authorities will be analysed, as will the role of the European Supervisory Authority headed by a European Data Protection Supervisor (EDPS). Recital 62 of the preamble to the 1995 Data Protection Directive states that 'the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data.' It is also essential to the maintenance of a legally appropriate privacy-security balance.

The analysis in this chapter of what EU law provides for in the case of Data protection Authorities, and of how these provisions are implemented, will focus on the phenomenon already noted in relation to the Snowden revelations: on the one hand a set of legal data protection provisions and on the other, the creation of major obstacles by state authorities and agencies preventing those entrusted with these powers (the Data Protection Authorities) from deploying them effectively. This situation will be dealt with as another aspect of the situation uncovered by the Snowden, LIBE and ECPS revelations of mass data surveillance, with massive consequences for the privacy/security balance.

In the context of achieving an acceptable data privacy/national security balance, difficulties are involved in carrying out a balancing exercise between rights such as data privacy and interests such as national security, which are qualitatively different. The conceptual question at issue here is whether a meaningful balancing exercise can be effectively carried out in weighing rights and interests. Responses to this question have been varied. At one extreme, there are those who have argued that although data privacy and national security are both social values, they are different values, and it is not reasonable to trade one against the other. A related view is that the idea of balancing human rights such as data privacy against national security is deeply misleading, because it assumes that we should decide which human rights to recognise through a kind of cost-benefit analysis. Those who advance such views tend to reject the idea that even in times of national emergency, when state security is under threat from terrorist activities, the interest of the greater good of society must prevail against an individual human right. On the other

hand, those who advocate the most extreme data retention measures, will argue that it becomes extremely difficult to preserve civil liberties if the survival of the state and its institutions is in jeopardy.

Although many commentators have raised the objection that the balancing process is both irrational and subjective, the legal scholar and philosopher, Robert Alexy, has argued that a balancing exercise in relation to the weighing of rights such as data and interests such as national security, can be carried out in an effective manner, and that the objection that balancing is inherently irrational and subjective is unjustified.[5] Other commentators who accepted the notion of a balancing paradigm when the relationship between a human right such as data privacy and societal interests such as national security is in question, have also devised principled balancing approaches. These include Barak, and Aquilina. It is also worthy of note that the principle of fair balancing has long been a feature of the jurisprudence of the European Court of Human Rights and the EU Court of Justice (CJEU).The work of Alexy and that of other commentators on the problems associated with the balancing rights and interests is reviewed in greater detail in Section 8.0 of Chapter Two of this thesis - 'Carrying out a balancing exercise involving rights which are qualitatively different.'

The chapter will conclude with consideration of the likely implications of the invalidation of the Data Retention Directive 2006/24/EC for Data Retention practices in EU Member States, and by extension for the data privacy/national security balance in Europe. Also considered will be the emergence of the CJEU as a primary defender of data privacy rights in Europe and the EU Charter of Fundamental Rights as the European equivalent of the United States Bill of Rights, again in the context of the data protection/national security balance.

[5] Alexy's approach to balancing is explained in *A Theory of Constitutional Rights* (Oxford University Press, 2002).

Section I: The Council of Europe

1.0 The Basis for the Data Privacy/National Security Balance

The primary law instrument of the Council of Europe, the European Convention on Human Rights (the ECHR), is an international agreement between the 47 Member States of the Council of Europe. All Member States are also Member States of the Council of Europe. All Member States of the European Union are also members of the Council of Europe, along with Russia, Turkey and Switzerland. The European Court of Human Rights (the ECtHR) is the final arbiter on the ECHR, which may be regarded as the first European Bill of Rights. The ECtHR hears submissions from individuals in Member States on alleged breaches by State authorities of rights guaranteed in the ECHR. Under Article 35 of the ECHR, the ECtHR may deal with such submissions only after all domestic remedies have been exhausted.

There is no provision for data protection *per se* in the ECHR. The second primary law instrument of the Council of Europe, the Data Protection Convention, or Convention 108, specifically addresses the protection of personal data. However, Convention 108 does not, in principle, fall under the jurisdiction of the ECtHR.[6] Even so, the ECtHR has interpreted Article 8 of the ECHR, which deals with the right to privacy, as also giving rise to a right of data protection.[7]

When the data privacy/national security balance is in question, the jurisprudence of the ECtHR is guided by the terms of Article 8 of the ECHR, and to a lesser extent by the provisions of Article 15. The latter Article deals with the right of Member States to take measures derogating from their obligations under the ECHR when faced with a national emergency.[8] The two parts of Article 8 provide the basis for the data privacy/national security

[6] Juliane Kokott and Christopher Sabotta, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and ECtHR' 3(4) (2013) *International Data Privacy Law* 223.

[7] For example, in *Amman v Switzerland* Application no. 27798/95, at para. 65; *Rotaru v Romania*, application no. 28341/95, at para. 143.

[8] Article 15 (1) of the Convention provides that 'In time of war or other public emergency threatening the life of nation, any High Contracting Party may take measures derogating from its obligations under this Convention to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with its other obligations under international law.

balancing paradigm employed by the ECtHR. Article 8(1) establishes a right whereby: 'Everyone has the right to respect for private and family life, his home and his correspondence.' Article 8(2) sets out a number of circumstances in which state authorities may interfere with the individual's right to data protection, for example, in pursuit of such legitimate aims as national security, public safety, economic well-being and prevention of crime.[9]

It is for the ECtHR, when adjudicating on complaints by individuals that their right to data privacy has been violated by state authorities, to strike a fair balance between the right in question and the goal pursued by the state, in this instance national security, taking account of the particular circumstances surrounding each case. This is a view endorsed by the ECtHR in its jurisprudence, with the provisions of the ECHR in mind:

> The Court agrees with the Commission that some compromise between the requirements for defending democratic society and individual rights is inherent in the system of the Convention. As the Preamble to the Convention states, 'Fundamental Freedoms … are best maintained on the one hand by an effective political democracy and on the other by a common understanding and observance of the Human Rights upon which [the Contracting States] depend'.[10]

2.0 The Influence of the ECHR on National Legal Systems

The European Court of Human Rights (ECtHR) has declared its principal text of the ECHR, the European Convention for the Protection of Human Rights and Fundamental Freedoms [11] a 'constitutional instrument of European public order.'[12] Two years before this declaration by the Court, Beddard characterised the Convention as 'a kind of constitutional document for a United Europe.' [13] Earlier, the ECtHR had established itself as the ultimate interpreter of the

[9] The full text of Article 8(2) reads: *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*.
[10] *Klass and Others v Federal Republic of Germany* (1979-1980), 2 EHRR 214, at 237, para 59.
[11] November 4, 1950 U.N.T.S. 222.
[12] *Loizidou v Turkey*, 310, ECtHR, Series A, at para. 27 (1995).
[13] Ralph Beddard, Human Rights and Europe (3rd edn, Cambridge University Press, 1993 5-6.

provisions of the ECHR [14] where the Court claimed that the ECtHR is 'empowered to give a final ruling' on whether a State's interference with a protected right is compatible with the ECHR. [15] A similar claim was advanced in *Muller v Switzerland*.[16] Merrills has remarked that '[t]he most dramatic impact of the Court's work is certainly to be found in the changes in domestic law and practice which have been introduced as a result of cases at Strasbourg.'[17]

In the context of the competing claims of data privacy and national security for legal protection, which is the central theme of this thesis, the ECHR and its Court perform two important functions. In Article 8 of its constitutional instrument it sets out a substantive guarantee protecting the right of individuals to data privacy, and through its Court it creates a complex enforcement mechanism permitting individuals and groups to file complaints against their national governments, alleging violation of the privacy rights guaranteed in Article 8. It is significant that although the treaty establishing the ECHR does not compel States party to it to recognise either the right of individuals to file such complaints, or the compulsory jurisdiction of the ECtHR, all states subscribing to the treaty and to membership of the ECHR have filed declarations accepting both obligations.[18] Article 46, headed 'Binding Force and Execution of Judgments' is of special relevance in this context: 'The High Contracting Parties undertake to abide by the final judgment of the Court in any case to which they are parties.' [19] The individual access right to the ECtHR has been crucial to the success of the ECHR in altering the domestic legal landscape, in challenging national legal orders and questioning the role of national constitutional provisions and national judiciaries.[20]

---

[14] *Barford v Denmark*, 149, ECtHR (Series A) para 12 (1989) .
[15] ibid, at para 28.
[16] 133 ECtHR (Series A) para 21 (1988).
[17] J.G. Merrils, The development of International Law by the European Court of Human Rights, (2nd edn, Manchester University Press, 1993).
[18] Council of Europe. Declarations Pursuant to articles 25 and 46 of the Convention for the Protection of Human Rights and Fundamental Freedoms, July 1, 1997.
[19] ibid.
[20] Laurence R. Helfer, 'Towards a Theory of Effective Supranational Adjudication' 107 (1997) *The Yale Law Journal* 273, 294; Andreas Follesdal, Birgit Peters, Geir Ulfstein, (eds) *Constituting Europe. The European Court of Human Rights in a National, European and Global Context* (Cambridge University Press, 2013) 6.

The approach of the ECHR to the enforcement of its provisions dealing with the right to privacy (including data privacy) afforded in Article 8(1) and the countervailing right of state authorities to interfere with this right in the interests of national security is influenced by the federalist framework within which it functions. Although by virtue of Article 46 ECHR, all of the state parties have undertaken to abide by the decisions of the ECtHR in any case to which they are parties,[21] the legal effect they give to the Court's judgment varies considerably, as does the status of the ECHR in the domestic law of Member States. In some states, the Convention is not a source of domestic law, while in between are countries in which it has the force of either Constitutional or statutory law.[22] In the light of this variation, the Court utilises a jurisprudential concept known as the 'margin of appreciation,' which refers to the latitude afforded to Member States in their observance of the Convention. Merrils refers to the margin of appreciation as

> [A] way of recognising that international protection of human rights and sovereign freedom of action are not contradictory but complementary. Where the one ends, the other begins. In helping the international judge to decide how and where the boundary is to be located, the concept of the margin of appreciation has a vital part to play.[23]

Sir Humphrey Waldock, past President of the ECtHR, described the margin of appreciation doctrine 'as one of the more important safeguards developed…. by the Court to reconcile the effective operation of the Convention with the sovereign powers and responsibilities of Governments in a democracy.' [24] In the context of the Court's practice of balancing data privacy rights guaranteed in Article 8(1) against the right of state governments to interfere with their

[21] Christoph Grabenwarter and Katharina Pabel, ' Fundamental Rights - The Charter and the ECHR' in Hermann-Josef Blanke and Stelio Mangiameli (eds.) *The Treaty on European Union (TEU). A Commentary* (Springer, 2013) 287-348, 287.
[22] Thomas A. O'Donnell, 'The Margin of Appreciation Doctrine: Standards in the Jurisprudence of the European Court of Human Rights' 4(4) (1982) *Human Rights Quarterly* 474, 475; Karen C. Burke, 'Secret Surveillance and the European Convention On Human Rights' 33 (1981) *Stanford Law Review* 1113, 1136.
[23] J.G. Merrils, *The Development of International Law by the European Court of Human Rights* (2nd edn), (Manchester University Press, 2003), 174-5.
[24] Humphrey Waldock, 'The Effectiveness of the system set up by the European Convention on Human Rights' 1 (1980) *International Human Rights Law Journal* 9.

rights if the interference is 'necessary in a democratic society in the interests of national security,' a right protected in Article 8(2). Waldock's reference to 'responsibilities of governments in a democracy'[25] embraces the 'interests of national security.'

Keller and Sweet focus on four interrelated questions as a first step to explain the impact of the ECHR on national legal systems. The first is whether a given national constitutional order adopts a monist or dualist posture with respect to supranational treaty law.[26] Secondly, what rank does the legal system assign to the Convention in the national hierarchy of norms? Thirdly, are the Convention guarantees directly binding on public authority, can they be pleaded before national courts and can judges enforce them against conflicting national norms, including statute. Finally, have the answers to these questions changed over time, and if so, through what procedures? [27]

From the perspective of balancing the right to data privacy against State or other interference with this right in the interest of public security, the Council of Europe, through its legal instruments, has consistently been heading in the direction of optimising the agency of data privacy rights, and limiting opportunities for undue interference with these by State agencies. Long before the ECHR interpreted the right to privacy to have broad application to any type of information concerning an individual, Member States of the Council of Europe negotiated a special set of rules relating to personal data. This is the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108), adopted in 1980, and opened for ratification in January 1981. The rules contained in the Convention apply to

[25] ibid.

[26] A dualist state looks on international law, or in the present context, supranational law, as being entirely separate from national law. It follows from this that unless a supranational agreement such as the ECHR is made part of national law by Parliament, it cannot be pleaded in a national court. A monist state does not distinguish between supranational and national law. Supranational law automatically becomes part of national law in a monist state. However, formal distinctions between systemic monism and systemic dualism have become less and less significant in determining the impact of the ECHR on national law.

[27] Helen Keller and Alec Stone Sweet, 'Assessing the Impact of the ECHR on National Legal Systems' 88 (2008) *Yale Law School* Paper 677, 682.

all those engaged in personal data processing: market actors, the media, government agencies and others.[28]

The data-protective measures embodied in the Convention provide that individuals must consent to the collection and use of their data or that a piece of government legislation must authorise the processing of these data, specifying the public reasons that necessitate personal data processing.[29] The quantity and type of personal data are also restricted: such data must be 'adequate, relevant and not excessive in relation to the purposes for which they are stored.'[30] The data stored in automated data files must also be protected against unauthorised access, alteration or dissemination.[31] The Convention further provides that individuals should have a right of access to their personal information, thus knowing what information about them is held by which institutions.[32] They are also entitled to correct any incorrect information and to demand that such information, and information retained for longer than necessary, be deleted. [33] In a general comment on Convention 108 provisions relating to data privacy, its protection and infringement, Bignami remarks that 'The basic theory behind these rules is the less personal data processing, the better.'[34]

A further manifestation of the ECHR's influence on the domestic law of Member States of the COE in reinforcing data privacy rights and inhibiting state and other interference with these, has been the action of the COE in supplementing the privacy provisions of Article 8 of the ECHR and Convention 108 with the 'Additional Protocol for the Protection of Individuals

[28] Article 3(1) of the Convention states that 'The Parties undertake to apply this Convention to automated personal files and automatic processing of personal data in the public and private sectors.' For commentary on Convention 108, see Colin J. Bennett and Charles D. Raab, *The Governance of Privacy Policy Instruments in Global Constitutional Perspective* (The MIT Press, 2006); Francesca Bignami, 'The Case for Tolerant Constitutional Patriotism: The Right to Privacy Before the European Courts' 41(2) (2008) *Cornell International Law Journal* 211, 220ff; Sylvia Kierkegaard, Nigel Waters, Graham Greenleaf, Lee A. Bygrave and Steve Saxby, '30 years on - The Review of the Council of Europe Data Protection Convention 108' 27(3) (2011) *Computer Law and Security Review* 223-231.

[29] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (Convention 108), Article 5(a).

[30] ibid, Article 5(c).

[31] ibid, Article 7.

[32] ibid, Article 8(a).

[33] ibid, Article 8(d).

[34] Francesca Bignami, 'The Case for Tolerant Constitutional Patriotism: The Right to Privacy Before the European Courts' 41(2) (2008) *Cornell International Law Journal* 211, 222.

with regard to the Automatic Processing of Personal data regarding supervisory authorities and transborder data flows.'[35] This Protocol directed each State party to the COE to provide one or more independent data protection authorities, exercising their functions in complete independence, on the basis that such authorities 'are an element of the effective protection of individuals with regard to the processing of personal data.' [36] The Protocol also added limitations on data exportation to non-Member States, thus meeting growing challenges to privacy protections resulting from transborder data flows. Article 2 provides that the Member States could provide for the transfer of personal data to non-Member States only if the non-Member State 'ensures an adequate level of protection for the intended data transfer.' The same Article suggests that safeguards for the privacy of transferred data to non-Member States 'can in particular result from contractual clauses' drawn up between the transmitting and receiving states.[37]

In their own detailed evaluation of the impact of the ECHR on eighteen national legal orders, Keller and Sweet conclude that national systems have become increasingly receptive to the influence of the ECHR and the case law of its Court. They point to two significant illustrations of this developing trend: 'judges once prohibited from engaging in judicial review of statute now do so routinely, with reference to European rights; and the dualist feature of many legal systems have given way to a sophisticated monism, when it comes to the Convention.'[38] Their survey of a wide variety of European legal orders shows that there is no necessary causal linkage between *ex ante* monism or dualism, on the one hand, and the reception by legal orders of the ECHR, on the other.[39]

What is of significance is whether and how the privacy provisions of the ECHR are incorporated by Member States. For example, in Belgium, a formally dualist state, the State's Courts, on their own initiative and without

[35] 'Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows' Strasbourg, 8.XI.2001 European Treaty Series -Series 181 Council of Europe, European Treaty Series. No. 181, Strasbourg, 8.XI,2001 <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680080626> accessed 26 July 2016.
[36] Article 1 of the Protocol and Preamble.
[37] Article 2 of the Protocol and Preamble.
[38] ibid, 677.
[39] ibid.

constitutional warrant, chose to confer supra-legislative status on ECHR rights and to apply them directly and so embrace monism with respect to ECHR law. In the 1990s both Sweden and Norway adopted Bills of Rights modelled on the ECHR. The Dutch Constitution provides for the supremacy of ECHR law over the Constitution itself, but does not provide for judicial review of statutes.[40] However, the Dutch Supreme Court has chosen to enforce the ECHR directly, in effect incorporating it as the *de facto* Bill of Rights. In the United Kingdom under the Human Rights Act (HRA) litigants may plead ECHR rights against any public authority, and Courts may enforce the ECHR against all but conflicting Parliamentary Statutes.[41] The Constitutional Courts in Germany and Italy have chosen to require the judiciary, as a matter of constitutional duty, to enforce the ECHR and to follow the jurisprudence of the ECtHR.[42]

In Germany, the ECHR originally enjoyed the same status as statute law, until the Federal Constitutional Court began to treat the ECHR as *lex specialias*. In 2004, the Court embraced the ECHR, and requires the judiciary to enforce convention rights even against statutes passed later in time. In 2007, the Italian Constitutional Court ruled that the ECHR enjoys higher status than domestic statutes. This means that in a case of conflict between Convention rights and a national statute passed after the 1995 law which incorporated the ECHR in Italian law, the ECHR will take precedence.[43] The Constitutional Court ruling means that in Italy, ECHR rights no longer have the status of ordinary law, but they are intermediate ('una norma interposta') between the Constitution and ordinary status. The Court also held that the exact meaning of the provisions of the ECHR may be ascertained only by the ECtHR. It followed from this that Italian human rights law must keep pace with ECHR rights as they evolve in

[40] Jurgen C.A. de Poorter, 'Constitutional Review in the Netherlands: A Joint Responsibility' 9(2) (2013) *Utrecht Law Review* 89.

[41] Section 3 Human Rights Act (1998) reads: '(1) So far as it is possible to do so, primary legislation and subordinate legislation must be read and given effect in a way which is compatible with the Convention rights. (2) This section - (a) applies to primary legislation and subordinate legislation whenever enacted; (b) does not affect the validity, continuing operation or enforcement of any incompatible primary legislation; and(c) does not affect the validity, continuing operation or enforcement of any incompatible subordinate legislation if (disregarding any possibility of revocation) primary legislation prevents removal of the incompatibility.'

[42] See Giuseppe Martinico, 'Is the European Convention Going to be "Supreme"? A comparative constitutional overview of ECHR and EU law before national courts' 23(2) (2012) *European Journal of International Law* 401, 411.

[43] Giuseppe Martinico and Oreste Pollicino, 'Report on Italy' in Giuseppe Martinico and Oreste Pollicino (eds)*The National Judicial Treatment of the ECHR and EU Laws: A Comparative Perspective* (Europa Law Publishing, 2010), 285.

the jurisprudence of the ECtHR. The main thrust of the clarification by the Italian Constitutional Court is that Italian national law must be interpreted in the light of ECHR norms.[44]

The Spanish Constitutional Court has consistently worked to enforce the ECHR as a quasi-constitutional body of law, and will strike down any statutes that violate the Convention as unconstitutional, interprets Spanish constitutional rights in the light of the ECHR, and has ordered the ordinary courts to conform their judgments to the case-law of the ECtHR as a matter of constitutional obligation.[45] For a number of state authorities, the ECHR is a foreign, alien law, having little force in the democratic order. These include Russia, Slovakia and the Ukraine.[46] The judgment of the Grand Chamber ECtHR on 4 December 2015 in the case of *Zakharov v Russia* throws light on the attitude of Russian authorities to the data privacy/security balance, as this is understood by the ECtHR.[47]

The current Spanish Constitution, passed in 1978, specifically addresses the right to data privacy in a manner which recalls the provision in Article 8 (1) ECHR of a right to data privacy and in Article 8 (2) outlining the conditions for legal limitation of that right. Article 18.3 of the Spanish Constitution establishes that 'the secretary of communication, particularly via postal, telegraph and telephone services, shall be guaranteed unless a court decision is made to the contrary.' [48] In a similar way, Article 18.4 establishes that 'the law shall limit the use of computerised information in order to guarantee the honour and privacy of all citizens and their families and the full exercise of their rights.'[49]

The limitations on access by intelligence agencies to electronic mail or other communication services in place, by these two data protective Constitutional

[44] The judgments of the Italian Constitutional Court (nos. 348 and 349/2007 are available at: <www.corteconstituzionale.it> Accessed 29 August, 2016.
[45] ibid, 684-86.
[46] ibid, 684-85.
[47] For a detailed discussion of this case see the next section, 3.0 'The Jurisprudence of the ECtHR and the Data Privacy/National Security Balance.'
[48] *Spanish Yearbook Of International Law* Volume IV, 1995-1996, (Martinus Nijhoff Publishers, Netherlands, 2001), 410.
[49] Privacy Online. OECD Guidance On Policy And Practice (OECD, 2003) 82.

Articles, at a time when acts of terrorism constituted an ongoing threat, had a part to play in the failure of the authorities to anticipate, or prevent, the Madrid bombings of 11 March 2004. This episode in turn brought the issue of telecommunications data to the forefront of the EU's legislative agenda and ultimately resulted in the promulgation of the Data Retention Directive in 2006, changing the existing balance between data privacy rights and national security demands in favour of the latter. The Madrid bombers had relied on telecommunications in their execution of the attacks in two ways, namely that the attacks had been co-ordinated by mobile phone and the bombers had obtained vital information on the Internet for their preparation for the attacks.[50] By contrast, as Blakeney remarks, the Spanish intelligence agencies 'had only limited access to data, such as telephone data, which would have been helpful to their investigations in establishing complete records on the communications, contacts, interests, business dealings, transactions and movements of certain individuals.'[51]

In the Baltic countries, the ECHR is deemed a source for the construction of national - including constitutional law.[52] The ECHR was cited by the Constitutional Courts of Estonia, Latvia and Lithuania before their accession to the EU.[53] In Estonia, Latvia and Lithuania, the Constitutional Courts expressly agreed to be bound by the ECtHR's case law, even when it interprets their own Constitutions.[54] The Supreme Courts of the Nordic Countries have acknowledged the special role of the ECHR, and have taken measures to avoid constitutional conflicts between national and supranational laws, like those of the ECHR.[55] While recognising the priority of its own constitution over both EU and ECHR law, the Bulgarian Supreme Court has acknowledged that the

[50] 'Tube wi-fi internet plan progresses despite security fears,' BBC News (25 March, 2011) available at: <http://www.bbc.com/news/uk-england-london-12856289> accessed 16 July, 2016.
[51] Simone Blakeney, 'The Data Retention Directive: combating terrorism or invading privacy' 13(5) (2007) *Computer and Telecommunications Law Review* 153.
[52] See Irmantas Jarukaitis, 'Report on Estonia, Latvia and Lithuania,' in G Martinico and O. Pollicino (eds.), *The National Judicial Treatment of the ECHR and EU Laws; A Comparative Constitutional Perspective* (Groningen Europa Law Publishing, 2010) 167-204, 202.
[53] See Giuseppe Martinico, 'Two Worlds (Still) Apart? ECHR and EU Law before National Judges,' in Vasiliki Kosta, Nikos Skoutaris and Vassilis Tzevekos (eds.), *The EU Accession To The ECHR* (Hart, Oxford And Portland, Oregon, 2004) 141 to 158, 148, fn 41.
[54] Giuseppe Martinico, 'Is the European Convention Going to Be "Supreme"? A Comparative-Constitutional Overview of ECHR and EU Law before National Courts' 23(2) (2012) *European Journal of International Law* 401-424, 412.
[55] ibid.

Bulgarian Constitution is to be interpreted as far as possible, in the light of ECHR law.[56] In the context of the data privacy/national security balance, the influence of the ECHR and the jurisprudence of the ECtHR on national, constitutional and jurisprudential systems has naturally tended to be uniformly benign from the standpoint of the data privacy aspect of the balance, given the primary role of the ECHR as an upholder and defender of human rights.

In February 1953, Ireland was the first member state of the Council of Europe to recognise the compulsory jurisdiction of the European Court of Human Rights (the ECtHR). However, fifty years after this token of recognition, Ireland was the only state out of the forty-four member states of the Council of Europe which had yet to incorporate the ECHR into its domestic law. Finally, on June 30, 2003, the Irish legislature passed the European Convention on Human Rights Act, in the process avoiding the use of the term 'incorporation.' The stated purpose of this Act was 'to enable further effect, subject to the Constitution, to certain provisions of the Convention.' [57] The effect of the passage of the ECHR Act was to allow the ECHR to be cited in Irish Courts as part of Irish law, but subject to the extent to which the ECHR is not in conflict with the Irish Constitution. Thus, the Constitution remains the paramount source of law in the Irish State, and the ECHR may not be used as a basis to declare Irish laws invalid.

International treaties such as the ECHR are not directly effective in Irish law from the perspective of the Irish legal system. The reason for this is that Article 29.6 of the Irish Constitution provides that: 'No international agreement shall be part of the domestic law of the State save as may be determined by the Oireachtas.' The extent to which the ECHR is to have domestic application has been expressed in the ECHR Act, 2003, as described above. The effect of the 2003 Act was clarified in a 2009 judgment of the Irish Supreme Court, when the Chief Justice, pointing out that Ireland was a dualist state, declared that the ECHR Act of 2003 did not allow for autonomous claims based purely on the

[56] ibid, 416.
[57] See Suzanne Egan, 'The European Convention on Human Rights Act 2003: A Missed Opportunity for Domestic Human Rights Litigation,' 25(1) (2003) *Dublin University Law Journal* 230.

Convention.[58] Thus, the Supreme Court disavowed the possibility of moulding Irish law in accordance with provisions of the ECHR.

In the Irish Courts, there was an initial resistance to the invocation of ECtHR jurisprudence in cases involving privacy as an informational right, controlling the collection and use of personal data. For a considerable period stretching to the 1990s, the Courts, instead of invoking ECtHR decisions when dealing with data privacy violations, preferred to address these issues solely on the basis of domestic law and the relevant provisions of the Irish Constitution, with little or no analysis of Article 8 of the ECHR. For example in *White v Morris*, the comment of Finnegan J that Article 8, ECHR did not add anything to the Irish Constitutional right to privacy,[59] indicated a judicial preference in data privacy cases to reach a decision on purely domestic grounds where possible.[60] In several important cases, such as the judgment in *Gray v Minister for Justice*,[61] which concerned Gárda leaking of information, there is no reference to the ECHR. In others, Article 8 ECHR is mentioned, but only to be dismissed as irrelevant.[62]

It is surprising that in cases involving the leaking of private information by members of the Gárda Síochána, such as *Gray v Minister for Justice*, there was no advertence to the ECHR. This is especially so since Article 3 of the Irish ECHR Act of 2003 states that: '[e]very organ of the state shall perform its functions in a manner compatible with the State's obligations under the Convention [ECHR] provisions.' Since it is beyond doubt that An Gárda Síochána is an organ of the State, and if covert surveillance is subject to the provisions of the ECHR, then Gárdaí must act in a manner compatible with its construction under ECtHR jurisprudence, and the Courts should take this into account when dealing with cases concerning the leaking of private information by an organ of the State.

[58] *McD v L* (2010) 2 I.R. 199, at 255. This judgment has proved to be controversial. See, for example, the comment of de Londras at footnote 5 infra.
[59] [2007] IEHC 107.
[60] See T.J. McIntyre, 'Implementing Information Privacy Rights in Ireland' in Suzanne Egan, ed. *International Human Rights Perspectives from Ireland* (Dublin, Bloomsbury, 2015) 271-287.
[61] [2007] IEHC 52.
[62] T.J. McIntyre, 'Implementing Information Privacy Rights in Ireland' in Suzanne Egan, ed. *International Human Rights Perspectives from Ireland* (Dublin, Bloomsbury, 2015) 271-287.

The resistance of the Irish Courts, and of Irish litigators to having recourse to the provisions of the ECHR and the jurisprudence of the ECtHR is understandable in the light of the fact that Ireland is a dualist state with a well-established system of constitutional justice in which litigants are much more likely to plead domestic constitutional law than the provisions of the ECHR before national judges. Furthermore, national judges, especially those sitting on Constitutional Courts, will, as Keller and Sweet point out, have a weaker interest in developing ECHR rights: 'they may even be jealous of their positions, and resist recognising the primacy of Convention rights when these come into tension with constitutional rights.' [63]

From the mid to late 1990s onwards, there has been some moderation of the previous concerns that the use of ECHR norms would undermine the dualist nature of the Irish legal system. In a more recent assessment, de Búrca suggests that the Irish Courts overall, now regard the ECHR as a hierarchically superior set of standards to trump the Irish Constitution, but as 'an additional resource for enhancing or strengthening certain rights, bringing other neglected or missing protections into Irish cases, in forming the interpretation of the Constitution and, in some cases, pointing out the incompatibilities of domestic legislation.' [64] It has been suggested that the abatement of judicial hostility towards the ECHR has its origin, in part at least, in the increased awareness of the ECHR in Irish legal circles, thus implying that a lack of knowledge and familiarity may have been a reason for the earlier lack of impact of the ECHR.[65] Another explanation for the greater receptivity of the ECHR over time may have been an increasing creativity on the part of the Irish judiciary in the interpretation of constitutional rights, in contrast to the earlier view that the ECHR would be of limited effectiveness because of the existence of an entrenched Constitution in Ireland, capable of affording adequate standards of human rights protection.

[63] Helen Keller and Alec Stone Sweet, *A Europe of Rights. The Impact of the ECHR On National Legal Systems'* (Oxford University Press, 2008) 20.
[64] Gráinne de Búrca, 'The Domestic Impact of the EU Charter of Fundamental Rights' 49(1) (2013) *The Irish Jurist* 49, 57.
[65] Suzanne Egan, 'The European Convention on Human Rights Act, 2003: A missed opportunity for Domestic Human Rights Litigation 25 (2003) *Dublin University Law Journal* 230.

The Criminal Justice (Surveillance) Act, 2009, which deals with the rights issues presented by state surveillance, has introduced several new provisions into Irish surveillance law. These provisions draw their inspiration from two main sources. In part they reflect the Irish Constitutional guarantee of the inviolability of the dwelling and in part ECtHR jurisprudence under Article 8 ECHR. For the first time there is a requirement (in section 5 of the Act) of judicial authorisation before surveillance can be carried out, and there is also a provision for modification after the event of those affected by the surveillance. This latter provision provides an important safeguard against the improper use of surveillance mechanisms and reflects a key element of ECtHR jurisprudence.[66]

The 2009 Act has facilitated one successful challenge to the admissibility of surveillance evidence. In *Sunny Idah v DPP*,[67] recordings of face-to-face meetings between the appellant and undercover Gárdaí were found to be inadmissible where such recordings had not been authorised in accordance with the 2009 Act. It is significant that the case relied on ECtHR jurisprudence[68] in determining the extent of the right to privacy in the context of covert surveillance.

In the context of using the ECHR in the Irish Courts, de Londras points out that the Irish ECHR Act of 2003 does not make ECtHR jurisprudence binding, what it does instead is to say that in all cases, 'judicial notice of such decisions should be taken, and that when interpreting and applying the provisions of the Convention, due account must be taken of the principles laid down in such [ECtHR] decisions.' [69] This means, de Londras argues, that when interpreting the content of Irish law and the requirements of the ECHR, Irish Courts are to be guided by the principles laid down in ECtHR jurisprudence.[70] In the light of this, de Londras concludes that 'the most disappointing aspect of the Supreme

[66] T.J. McIntyre, 'Implementing Information Privacy Rights in Ireland' in Suzanne Egan, ed. *International Human Rights Perspectives from Ireland* (Dublin, Bloomsbury, 2015) 271-287.
[67] [2014] IECCA, 3.
[68] *Lüdi v Switzerland*, Application no. 12433/86, judgment of 15 June 1992.
[69] Fiona de Londras, 'Using The ECHR In Irish Courts: More Whisper Than Bang?' *Using the ECHR: Where are we Now?* (PILA Seminar, 13 May, 2013). available at: <https://www.ucd.ie/t4cms/pilaechrseminar130511fdelondras.pdf> Accessed 28 June, 2017, 1, 9.
[70] ibid.

Court's decision in *McD v L* is its failure to acknowledge and fully embrace the court's proper role under the ECHR Act 2003.' [71]

3.0 The Jurisprudence of the ECtHR and the Data Privacy/National Security Balance

(a) Clarification by the ECtHR of the Provisions of Article 8 ECHR

From a legal perspective, the balancing of data privacy against national security is provided for in abstracto by the legislative framework outlined in Article 8 of the ECHR. The balancing of the two values takes concrete form during the judicial process when the ECtHR derives a balancing paradigm from the provisions of Article 8. [72] An analysis of the case law of the ECtHR will facilitate the extrapolation of the principles the Court applies in its interpretation of the meaning to be attached to the unarticulated precepts and categories outlined in the exiguous and vague language of Article 8.

One of the two concepts involved in the balancing process, data privacy, is not mentioned in Article 8 of the ECHR. However, within the Council of Europe framework, explicit recognition is accorded to the protection of personal data as a fundamental right in the 1981 Convention for the protection of individuals with regard Automatic Processing of Personal Data.[73] The case law of the Court illustrates how it brings necessary clarity and substance to the terminology of Article 8(2), in addition to developing a considerable corpus of law with relevance to the determination of the privacy/security balance.

Taking the clarification of terminology first, the Court provided a detailed interpretation of the requirement under Article 8(2) of the ECHR that any interference by a public authority with the right protected under Article 8(1)

---

[71] ibid, 10.

[72] Right to respect for private and family life: (1). Everyone has the right to respect for his private and family life, his home and his correspondence (2) There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

[73] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg Council of Europe 28.I.1981 European Treaty Series 108 <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37> accessed 13 August 2016.

must be 'in accordance with the law.' [74] The Court declared that this argument will be met only where three conditions are satisfied. First, the impugned measure must have some basis in domestic law, which includes judge-made or unwritten law, as well as statutes.[75] Second, the domestic law in question must be compatible with the rule of law, and be accessible to the person concerned. Third, the person affected must be able to foresee the consequences of the domestic law for him.[76] This clarification requires further elaboration by the Court. This involves the meaning of two terms: 'the Rule of Law' and 'foreseeability.' In order to be compatible with the rule of law, the domestic law 'must meet quality requirements: it must be accessible to the person concerned and foreseeable as to its effects.'[77] In the special context of secret surveillance such as the interception of communications, it is essential that the domestic law must be sufficiently clear to give citizens 'an adequate indication as to the circumstances in which, and the conditions on which, public authorities are empowered to resort to any such measures.'[78] The Court adopted minimum safeguards to be set out in domestic law in order to avoid abuses of power when secret measures of surveillance are in question. These measures should include an indication of the nature of the offences which may give rise to an interception order; a definition of the categories of people liable to have their telephones tapped, and a limit on the duration of telephone tapping.[79] As to the requirements concerning the law's foreseeability, the Court pointed that foresee ability in the special context of secret surveillance measures, such as the interception of communications, the requirement of foreseeability 'cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly.' [80]

On the question whether interference was 'necessary in a democratic society' in pursuit of a legitimate aim, the doctrine of the Court is that powers to instruct secret surveillance of citizens are tolerated under article 8 only to the extent

[74] *Rotaru v Romania*, No. 28341/95, at para 48.
[75] See, e.g. *Sunday Times v United Kingdom* (1979), 2 E.H.R.R. 245, at para 47; *Malone v United Kingdom* (1984) 7 E.H.R.R. 14, para 66.
[76] *Rotaru v Romania*, No. 28341/95, at para 52.
[77] *Sergerstedt-Wilberg v Sweden* 44 E.H.R.R., 2, at para 76 (2007)
[78] *Roman Zakharov v Russia*, No. 47143/06, 4 December 2015, at para 229.
[79] ibid, at para 231.
[80] *Weber and Savaria v Germany* Application No. 54934/00, at para 93.

that they are 'strictly necessary for safeguarding democratic institutions.' [81] This connects with the defence of national security. In practice, this means that when surveillance is being deployed in the interest of national security, there must be 'adequate and effective guarantees against abuse' [82] by State authorities of surveillance powers. Assessment of such abuses depend on the nature, scope and duration of the possible surveillance measures, the grounds required for ordering them, the authorities competent to authorise, carry out and supervise them and the kind of remedy provided by national law to the persons to whom surveillance has been applied.[83] The case law provides a further elaboration of 'necessary in a democratic society': that there must be a pressing social need for the interference' [84]

The Court, again in the context of the need for secret surveillance to be compatible with the rule of law, is particularly concerned that national law must provide a measure of legal protection against arbitrary interference by public authorities with the privacy rights protected by Article 8(1), especially where the power of the Executive is exercised in secret, 'the risks of arbitrariness are evident.' [85] Furthermore, since the implementation in practice of measures of secret surveillance 'is not open to scrutiny by the individuals concerned or the public at large,' [86] it would be contrary to the rule of law for the legal discretion granted to the Executive to be expressed 'in terms of an unfettered power.' [87] This would unduly tilt the privacy/security balance in favour of the latter interest. For this reason, the law must indicate the scope of any legal discretion conferred on state authorities, and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference.[88]

[81] *Kennedy v The United Kingdom*, No. 26839 05, 10 May 2010, at para 153.
[82] *Klass and others v Federal Republic of Germany* 1979-80, 2. E.H.R.R. 214, 6 September 1978, at paras 49 and 50.
[83] at para 55.
[84] *Sunday Times v The United Kingdom* 2 E.H.R.R. 14, para 59 (1979).
[85] *Huvig v France*, 24 April 1990, § 26, Series A no. 176-B, at pp. 54-55, § 29;
[86] *Iordachi and Others v Moldova* Application no. 25198/02 Fourth Section 10 February 2009, at para 94.
[87] ibid.
[88] *Segerstedt-Wilberg v Sweden*, at para 76. See also *Malone v United Kingdom* (A/82) 1985, 7 E.H.R.R 14 at paras 67-8, and *Rotaru v Romania* at para 58.

The 'pressing social need for the interference' is linked to another concept, proportionality, which is central to the Court's determination of the legitimacy of a given instance of state interference with the privacy right protected by Article 8(1). In the case-law of the Court, the establishment of this pressing social need will depend, inter alia, on whether the interference with the right was proportionate. Proportionality is not mentioned in Article 8, but has been specifically recognised in ECtHR case law.[89] '[B]ut broadly speaking, the principle of proportionality means that there must be a reasonable relationship between a particular objective to be achieved and the means used to achieve that objective' (national security) and the means used to achieve this objective (interference with the right to data privacy).[90]

The emphasis thus far has been on the essential objective of Article 8, which is to protect citizens against arbitrary interference by public authorities. This is among the negative obligations imposed by the Article not simply to compel the state to abstain from such interference. The case-law of the ECtHR also suggests that the Courts consider that States have positive obligations on the basis of the provision in Article 8(1) of the ECHR that 'Everyone has the right to respect for his private and family life, his home and his correspondence' and the State's positive obligation to respect and defend these values are inherent in this provision. [91] The Court deems it an interference with private life when state agencies install a listening device in a person's home,[92] or intercept telephone calls made to or from a person's home. [93] 'Telephone conversations are covered by the notions of 'private life' and 'correspondence.' The Court has also held that Member States are not only responsible for interceptions they carry out themselves, but in some circumstances for those carried out by individuals on behalf of police forces.[94] A recurring feature of ECtHR case law is that the mere existence of state legislation permitting the interception of

[89] For example, *Leander v Sweden* (1987) 9, E.H.R.R. 433, at para 58*; Hansyside v United Kingdom* (1976) 1, E.H.R.R. 737, at para 49.
[90] See Nicole A. Moreham, 'The Right to Respect for Private life in the European Convention on Human Rights: a re-examination' 1 (2008) *European Human Rights Law Review* 44, 47, fn 16.
[91] *Van Kück v Germany* (2003) 37, E.H.R.R. 51, at para 70 and *McGinley and Egan v United Kingdom* (1998) 27 E.H.R.R. 1 at para 98.
[92] *Lewis v United Kingdom* (2004) 39 E.H.R.R. 9, at para 18, *Lewiston v United Kingdom* (2003), 37 E.H.R.R. 31, at para 20.
[93] *Malone v United Kingdom* (1984) 7, E.H.R.R. 14 at para 64.
[94] *M.M. v Netherlands* (2004) 39 E.H.R.R., 414, at para 19.

communications can interfere with applicants' private lives even if the legislation is not actually used against them.[95] This case involved legislation authorising the opening and inspection of mail, reading of telegraphic messages and monitoring and recording of telephone conversations. The Court found that this legislation interfered with the applicants' private lives even though the applicants' conversations and mail had not been intercepted: 'in the mere existence of the legislation itself, there is involved, for all those to whom the legislation could be applied, a menace of surveillance.' [96] In the *Rotaru v Romania* (2000) and the *Malone v United Kingdom* (1984) judgments, the fact that each applicant was a member of a class of persons against whom measures of postal and telephone interception were liable to be employed, was sufficient to establish a breach of article 8(1) ECHR.

(b) The Approach of the ECtHR to the Balancing of data privacy against National Security

In the course of its jurisprudence, the ECtHR invokes the stated purpose of the ECHR: 'to secure in the territory of each party for every individual…..respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him.' [97] It also invoked the ECHR definition of personal data, as 'any information relating to an identified or identifiable individual.' [98] These references of the Court were made in a case where information about the applicant stored on a cord was found to constitute an interference with private life, even though the card did not contain any sensitive information and may not even have been consulted by State authorities.[99]

The scope of this section is limited to cases in which surveillance measures undertaken in the interest of national security and the prevention of terrorism are an interference with the applicant's right to data privacy. These commonly

[95] *Klass and Others v Federal Republic of Germany* (1978) 2 E.H.R.R. 214 at para 41.
[96] ibid.
[97] *Amann v Switzerland*, No. 27798/95, paras 65-67, ECtHR, 2000-11.
[98] ibid.
[99] A similar kind of judgment was arrived at in a similar kind of case: *P.G. and J.H. v The United Kingdom*, 44787/98 Judgment 25 September 2001, at para 57. Here the Court held that 'The installation of listening devices and the recording of the applicants' conversations were not unlawful in the sense of being contrary to domestic criminal law: the unlawfulness related exclusively to the absence of statutory authority for the interference with the right to private life and correspondence.' The applicants were awarded damages and costs.

include cases regarding protection against the interception of communications,[100] various kinds of surveillance [101] and the storage of personal data by public authorities.[102]

ECtHR cases involving the use of the data privacy/national security balancing paradigm follow a standard pattern, but the Court allows for a deviation from this when it considers that a particularly State, whose surveillance practices are impugned by an applicant, has been the victim of terrorist activity constituting a serious threat to its security. This deviation is commonly known as the margin of appreciation. The Court explains the *raison d'être* of such latitude when it states that '[p]owers of secret surveillance of citizens, characterising as they did the police state, were tolerable under the Convention only insofar as strictly necessary for safeguarding democratic institutions.'[103] The latitude accorded to the states by the ECtHR when national security is under threat by terrorist activity, resulting in an interference by state authorities with the right of citizens to data privacy is influenced by the existence among the states constituting the membership of the Council of Europe of 'Societies and individuals with different histories, different and, almost certainly, different basic social or political ethics about the values that underline many of the Convention Rights.'[104] Kay also cites the natural resistance among citizens and governments of Member States when important domestic policies [on human rights and national security] are being regulated from outside [by bodies such

[100] *Malone v United Kingdom*, no. 8691/79, 1984 and *Copland v United Kingdom* No. 62617/00, (2007)

[101] *Klass and Others v The Federal Republic of Germany*, No. 5029/71 (1878); Uzun v Germany No. 25623/05 (2010). See Jennifer Chandler, 'Privacy Versus National Security: Clarifying the Trade-Off,' in Ian Kerr, Carole Lucock and Valerie Stevens, (eds.) *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (Oxford University Press, 2009), 131-138: 'The danger with permanently permitting the needs of national security to trump competing values [as happens in *Klass*] is that important questions may not be adequately considered.' See also Aharon Barak, 'Proportionality and Principled Balancing' 4(1) (2010) *Law and Ethics of Human Rights* 1, 7-12; Ronald Dworkin: 'It is absurd to calculate human rights according to a cost-benefit analysis…. one cannot apply a cost-benefit analysis to a human right' (*The Guardian* 24 May, 2006); Helen Nissenbaum, 'Privacy as Contextual Integrity' (2004) 79(1) *Washington Law Review* 101: 'Privacy may sometimes be at odds with other values such as security…when these values clash…we need to pursue trade-offs and balance,' 151.

[102] *Leander v Sweden* No. 9248/81 (1987) and *Marper v United Kingdom*, No. 30562, (2008).

[103] *Klass and Others v Federal Republic of Germany* (1979-80) 2 E.H.R.R. 214, at para 42.

[104] David Seymore, 'The Extension of the European Convention on Human Rights to Central and Eastern Europe: Prospects and Risks' 8 (1993) *Connecticut Journal of International Law* 243, 245-7.

as the ECtHR] as the decision-makers are perceived as increasingly 'foreign.'[105] However, although the ECtHR routinely finds that states party to the ECHR have defaulted on their legal obligations under the Convention, these judgments, dealing with difficult and contested issues touching on state sovereignty, are also routinely honoured by the respondent states. These states pay whatever compensation is ordered by the Court and adjust their laws and practices to conform to the Court's findings.[106] An illustration of the resistance of Member States to ordinances of international bodies to which they subscribe, ordinances which were in conflict with settled domestic constitutional provisions, has been the widespread opposition of EU citizens as well as human rights and civil liberties groups to the Data Retention Directive of 2006.

(c) The ECtHR and Methodological Challenges

The methodological challenges confronting the ECtHR when dealing with the lawfulness of the limitation of a fundamental right such as data privacy emerge in the course of its implementation of the data privacy/national security paradigm. Under the terms of Article 35, ECHR, the Court may deal with a complaint brought forward by an applicant only after all domestic remedies have been exhausted. In interpreting the accommodation clause in Part 2 of Article 8, the Court applies a five-stage test. It first tries to ascertain whether the State authority interfered with the right to data privacy set out in Part 1 of Article 8. If it is satisfied that such an interference has occurred, it proceeds to the next stage: if not it dismisses the applicant's case. The second stage involves a consideration of whether the interference is in accordance with the law: whether it had a legal basis in domestic law and was compatible with the rule of law. The latter phrase has a special significance based on the well-established case law of the Court: the law governing the state interference with the privacy right must meet 'quality requirements,' be accessible to the person

[105] Richard S. Kay, 'The European Convention on Human Rights and the Authority of Law' 8(2) (1993) *Connecticut Journal of International Law* 217, 221. See also Peter Van Dijk and Godefridus J.H van Hood, *Theory and Practice of the European Convention Human Rights* (Kluwer Law International, The Hague, The Netherlands, 1998), 616-45, whose authors suggested a tendency towards a growing resistance to the judgments of ECtHR.

[106] Mark W. Janis and Richard S. Kay, *European Human Rights Law* (University of Connecticut Law School Foundation, 1990), xlii-XLV.

subjected to the interference and foreseeable as to its effects.[107] In the special context of secret measures of surveillance, such as state interception of communications, the Court deems it essential that the domestic law governing the interception must be sufficiently clear to give citizens an adequate indication of the circumstances in which, and the conditions on which State authorities are empowered to undertake interception measures. The third stage involves ascertaining whether the interference pursues one or more of the legitimate aims mentioned in Article 8(2), national security being one of these. The fourth stage involves an examination of whether the interference was necessary in a democratic society in pursuit of a legitimate aim. From the perspective of a legal examination, the public interest of security as one of the legitimate aims does not need further justification when it or certain aspects of it, such as state security, are named in the relevant limitation clause in Article 8(2). In this context, the Court, in its case law has made a significant and far-reaching acknowledgement that

> [W]hen balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his private life, the national authorities enjoy a certain margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security.[108]

The Zakharov verdict also enshrined that this margin 'is subject to European supervision embracing both legislation and decisions applying to it,' and warned of the dangers of too ready and easy a deployment of this judge-made law:

> In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the guise of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse.[109]

[107] For the ECtHR case law on this, see *Rotaru v Romania*, Grand Chamber, No. 28341/95, at para 52, ECtHR, 2000-v and *Marper v The United Kingdom* [Grand Chamber] nos. 30562/04 and 30566/04 (2008).
[108] *Roman Sakharov v Russia*, Application No. 47143/06 [Grand Chamber] 4 December 2015, at para 232.
[109] ibid, at para 232.

However, the case law of the ECtHR, as will be suggested below,[110] gives the impression that the Court, in many cases, is liable to accept governments' claims in relation to their pursuit of legitimate aims, almost as a matter of course. The fifth and final stage of the process covers the proportionality of the state infringement to its purposes. Here, the Court must decide whether the State interference with a fundamental right such as privacy was proportionate in a democratic society, or whether there was a pressing need for it. It is important to note that the proportionality test is the real area of judicial discretion, requiring the Court to balance two values: the aim of the limitation and the limited fundamental right. The earlier tests in the adjudicatory process involved arguments based on ascertainable facts. The proportionality test involves the court in adjudicating on normative issues, deciding whether, in a particular case, if there is a proper relation between the benefit gained by the realisation of a State's aim through interference with a right, and the harm caused to those entitled to benefit from the enjoyment of that right. The protection of data privacy rights against the interests of State security is thus at the discretion of the Court as it weighs them in a normative balance. In a case involving the use of surveillance for security purposes,[111] the ECtHR provided a summary of the methodology involved in its assessment of the concepts of necessity, proportionality and the Margin of Appreciation.

The notion of security implies that the interference corresponds to a pressing social need and, in particular, that it is proportionate to the legitimate aim pursued.[112] However, the Court recognises that the national authorities enjoy a Margin of Appreciation, the scope of which will depend not only on the nature of the legitimate aim pursued, but also on the particular nature of the interference involved. In the instant case, the interest of the respondent State in

[110] See section dealing with the Margin of Appreciation.
[111] *Leander v Sweden*, No. 9248/81, 26 March 1987, at para 58. In this case, The Applicant, a Swedish national, had applied for a post relating to high-level Swedish policy-making. As part of an assessment as to the suitability of candidates for the post, recourse was had to secret police files containing information regarding the Applicant's private life. A request by the Applicant to have access to these files was refused. The Applicant initiated proceedings on the basis that a violation of his right to private life, as enshrined in Article 8 ECHR had been violated. The ECHR did not find in favour of the Applicant, inter alia on the basis that although a breach of Article 8(1) ECHR had occurred, the breach was justified by virtue of the legitimate aim of Article 8(2) ECHR to uphold national security.
[112] ibid.

protecting its national security must be balanced against the seriousness of the interference with the applicant's right to respect for his private life.[113]

In this case, the Court found that the storing and release of information relating to Leander's private life, coupled with a refusal to allow the applicant to refute it amounted to an interference with his right to private life as guaranteed by Article 8 (1) ECHR.[114] However, the Court also found that the interference was justified, that it had a valid basis in domestic law, that the law in question was accessible to the applicant and that the relevant Swedish law satisfied the requirement of foreseeability.[115] In balancing the State's interest in protecting national security against interference with the applicant's right to respect for his private life, the Court accepted that the State enjoyed 'a wide margin of appreciation.' [116] Having regard to the wide margin of appreciation available to it, the respondent State was entitled to consider that in this particular case, the interests of national security prevailed over Leander's individual interests, so that there was no breach of Article 8 ECHR.[117]

The case law of the ECtHR on the secret surveillance of communications reveals a recognition by the Court that secret surveillance has features that call for a variety of approaches, depending on the circumstances surrounding each case. Two lines of case-law help to illustrate this. One is exemplified in the case of *Esbester v the United Kingdom* [118] the other in *Klass and others v The Federal Republic of Germany*. [119] In neither case did the applicant have any concrete proof that he had been subject to surveillance. In each case, the Court had to decide, as a first step in the judicial process, whether the claim made by each applicant, that the very existence of a system of secret surveillance, as distinct from its use in respect to either of them, violated their privacy rights under article 8. In *Esbester*, where the hearing was before the European Commission of Human Rights, the *Malone* [120] case was cited in support of the well-established principle in ECHR case law, that an applicant can claim to be

[113] ibid, at paras 58-9.
[114] ibid, at para 48.
[115] ibid, at para 51.
[116] ibid, at para 67.
[117] ibid.
[118] (1994), 18. E.H.R.R. CD72.
[119] Application No. 5029/71 6 September 1978.
[120] *Malone v United Kingdom* (1985) 7, E.H.R.R. 14.

a victim of a violation of Article 8 'by reason of the "very existence" of surveillance practices, apart from 'any concrete measure of the implementation taken against him.'[121] However, in *Ebester*, the Commission pointed out that the case law stated in *Malone* 'cannot be interpreted so broadly as to encompass every person in the United Kingdom who fears that the Secret Surveillance may have compiled information about him.' However, 'since an applicant cannot be expected to prove that such information has been retained, it is sufficient that there is a *reasonable likelihood* that the Security Service has compiled and retained information about the applicant's private life.'[122] Esbester was deemed to have passed this test.

In *Klass*, by contrast, the applicant was not required to pass the 'reasonable likelihood test.' Instead, it was held that 'in the mere existence of the legislation,' [123] there was involved for all those to whom 'it could be applied,'[124] what was described as 'a menace of surveillance' which 'necessarily strikes at freedom of communication between users of the postal and telecommunications services, and thereby constituted 'an interference by a public authority' with the right to respect for private and family life and correspondence, protected by Article 8(1).[125] The application was consequently deemed admissible. In a comment on what she calls the 'potentially conflicting decisions' in *Klass* and *Esbester*, Woods suggests that the ECtHR in *Kennedy v The United Kingdom* [126] 'took the opportunity to try and resolve these.' [127] The Court in *Kennedy* held that an applicant can challenge surveillance legislation on two grounds: (a) that secret surveillance measures were applied to him, or that, at the material time, he was *potentially at risk* of being subjected to such measures [128] and (b) that the remedies against abuse provided by domestic law are inadequate.[129] In cases where there are no effective measures against abuse

[121] ibid, at para 86.
[122] *Esbester v the United Kingdom* (1994), 18. E.H.R.R. CD72.
[123] *Klass and Others v Federal Republic of Germany* (1979-80) 2 E.H.R.R. 214, at para 41.
[124] ibid.
[125] ibid.
[126] Application No. 26859/05 (2010).
[127] Lorna Woods, 'Zakharov v Russia: Mass Surveillance and the European Court of Human Rights' *EU Law Analysis* 16 December 2015 <http://eulawanalysis.blogspot.ie/2015/12/zakharov-v-russia-mass-surveillance-and.html> accessed 21 January 2016.
[128] *Kennedy v The United Kingdom* Application No. 26859/05 (2010), at para 128.
[129] *Klass and Others v Federal Republic of Germany* (1978) 2 E.H.R.R. 214 at para 41.

of the applicant's rights, then 'the menace of secret surveillance' argument put forward by the Court in *Klass* could be applied.

In *Kennedy* the Court adduced 'special reasons' [130] justifying its departure, in cases concerning secret surveillance measures, from its general approach which denies individuals the opportunity to challenge a law *in abstracto,*[131] in other words to challenge a secret surveillance law even when an applicant has had no proof that he or she had been a target of such surveillance. The principal reason adduced by the Court for permitting this departure was 'to ensure that the secrecy of surveillance measures did not result in their being unchallengeable and outside the supervision of the national judicial authorities' as well as of the ECtHR.[132] Where there is no possibility at domestic level of challenging the alleged application of secret surveillance measures, 'widespread suspicion and concern among the general public that secret surveillance powers are being abused cannot be said to be unjustified. In such cases, even where the actual risk of surveillance is low, there is greater need for scrutiny by this Court.' [133]

The emphasis here on the need for state legislation to provide strong safeguards against the risk of abuse of the privacy rights of citizens by law enforcement authorities when secret surveillance is in question is reaffirmed in the more recent case of *Zakharov v Russia,*[134] in which the applicant claimed that Russian laws governing interception did not provide adequate and effective safeguards against abuse. It is significant that the Court in *Zakharov* relies heavily and consistently on the principles it enunciated in *Kennedy* on the need to avoid the abuse of secret surveillance powers by State authorities:

> The *Kennedy* approach therefore provides the Court with the requisite degree of flexibility to deal with a variety of situations which might arise in the context of secret surveillance, taking into account the particularities of the legal systems in the member States, namely the available remedies, as well as the different personal situations of applicants.[135]

[130] *Kennedy v The United Kingdom* Application No. 26859/05 (2010), at para 124.
[131] ibid.
[132] ibid.
[133] ibid.
[134] Application no. 47143/06 (2015).
[135] *Zakharov v Russia* Application no. 47143/06 (2015), at para 172.

Zakharov, a campaigner for media freedom and the rights of journalists, sought to challenge a Russian system of secret surveillance which required mobile operators to intercept mobile telephone communications. Attempts to challenge this practice were unsuccessful at national level, and the matter was brought before the ECtHR. Zakharov argued that the laws governing the monitoring infringed his right to respect for private life guaranteed by Article 8(1) ECHR, that elements of these laws were not accessible [136] and that there were no effective remedies available under Russian law,[137] relying on Article 13 of the ECHR, which provided for such a right.[138] He also submitted that although Russian domestic law required prior judicial authorisation for interceptions, the authorisation procedure did not provide for sufficient safeguards against abuse.[139]

A notable feature of the Court's analysis in this case is its thoroughness in investigating every relevant provision of Russian surveillance law. Not only did it look at these provisions on their face, but, more importantly, how they were applied in practice. In undertaking its review, the court examined:

> [T]he accessibility of the domestic law, the scope and duration of the secret surveillance measures, the procedures to be followed for storing, accessing, examining, using, communicating and destroying the intercepted data, the authorisation procedures, the arrangements for supervising the implementation of secret surveillance measures, any notification mechanisms and the remedies provided for by national law.[140]

It found a wide range of defects in the Russian regulatory framework. Among the most significant of these were the breadth of discretion granted to the executive when dealing with national security;[141] that the emergency procedure provided for in Russian law, which enables interception without judicial

[136] ibid, at para 180.
[137] ibid, at para 217.
[138] Article 13 reads 'Everyone whose rights and freedoms as set forth in the convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.'
[139] *Zakharov v Russia* Application no. 47143/06 (2015) at para 191.
[140] ibid, at para 238.
[141] ibid, at para 248.

authorisation, does not provide sufficient safeguards against abuse;[142] that the secret services had direct remote access to the databases and networks of communications service providers, thus enabling them to circumvent even the existing legal safeguards, because they were not required to serve a judicial order to service providers before collecting data;[143] that judicial involvement was limited solely to the authorisation stage, with the courts having no continuous supervisory function; [144] that the government was unable to provide the Court with any examples of effective prosecutorial oversight [145] and that judicial remedies in Russia were generally ineffective, particularly in the light of the total absence of any notification requirement with regard to the interception subject, without any meaningful ability of retrospective challenges to surveillance measures.[146]

In the light of these shortcomings in the legal framework, the Court was not persuaded by the Government's assertion that all interceptions in Russia are performed lawfully on the basis of proper judicial authorisation. Instead, it found evidence of arbitrary and abusive surveillance practices, due to inadequate safeguards against abuse provided for by law.[147] Overall, the Court found that Russian law does not meet the 'quality of law' requirement and is incapable of keeping the interference with privacy rights to what is 'necessary in a democratic society.' [148] The detail and rigour of the Court's analysis is in marked contrast to the Court's relatively casual analysis in *Klass*[149] regarding West German surveillance practices.

In *Zakharov*[150] the ECtHR adopted the broad approach to the standing of the applicant that it had already taken in *Klass* [151] *Esbester* [152] and *Kennedy*.[153] This is a two-strand approach: (1) If an applicant claims that he has been subjected to surveillance, he merely has to furnish conclusive proof, which,

[142] ibid, at para 266.
[143] ibid, at paras 268-271.
[144] ibid, at para 274.
[145] ibid, at para 284.
[146] ibid, at para 300.
[147] ibid, at paras 168 and 169.
[148] ibid, at para 304.
[149] *Klass and Others v Federal Republic of Germany* (1979-80) 2 E.H.R.R. 214.
[150] *Zakharov v Russia* Application no. 47143/06 (2015).
[151] *Klass and Others v Federal Republic of Germany* (1979-80) 2 E.H.R.R. 214
[152] *Esbester v the United Kingdom* (1994), 18. E.H.R.R. CD72.
[153] *Kennedy v The United Kingdom* Application No. 26859/05 (2010).

given the nature of secret surveillance, would be difficult, if not impossible to obtain; (2) Applicants can challenge the surveillance regulatory framework *in abstracto*, without alleging that they have been spied upon. This abstract review standard, defended by the Court in *Kennedy* [154] seems likely to be a feature of future ECtHR cases involving secret surveillance.

An early indication that this may be the case is the judgment in *Szabó and Vissy v Hungary*.[155] The circumstances leading to the application were similar to those surrounding *Klass*, *Kennedy* and *Zakharov*. In January 2011, the Hungarian Government established an Anti-Terrorism Task Force. Under the governing legislation, The National Security Act, the task force engaged in secret house searches, surveillance recording, opening of letters and parcels and recording of electronic and computerised communications.[156] Ministerial approval for these activities was not subject to judicial review, the domestic law did not indicate the circumstances under which surveillance could be ordered, and there was no provision for deletion of seized data and information.[157] In June 2012, two Hungarian nationals, Mate Szabo and Beatrix Vissy, resident in Budapest, filed a Constitutional complaint, arguing that the sweeping prerogatives of secret intelligence gathering for national security purposes breached their right to privacy.[158] Most of their complaints were dismissed by the Hungarian Constitutional Court.[159]

Szabó and Vissy brought an application before the ECtHR, relying on Article 8 of the ECHR. They did not claim to have been subjected to surveillance, but argued that they could be subjected to disproportionately intrusive measures because the Hungarian surveillance regime was open to abuse for want of judicial oversight. The ECtHR continued to take the expansive view of the applicants' standing manifested in a number of previous cases of this kind, holding that:

[154] ibid, at para 124.
[155] *Szabó and Vissy v Hungary* Application no. 37138/14 (12 January 2016).
[156] ibid, at para 8 and 9.
[157] ibid, at para 13.
[158] ibid, at para 14.
[159] ibid, at para 15.

> [I]n recognition of the particular features of secret surveillance measures and the importance of ensuring effective control and supervision of them, the Court has accepted that, under certain circumstances, an individual may claim to be a victim on account of the mere existence of legislation permitting secret surveillance, even if he cannot point to any concrete measures specifically affecting him.[160]

The traditional approach of the ECtHR had been to hear cases *in abstracto* only in exceptional circumstances. This approach was articulated in *Kennedy* as recently as 2010.[161] However, the Court felt the need to come to terms, especially when dealing with secret surveillance cases, with the development of sophisticated technologies which provided state security agencies with the means to alter the traditional data privacy/national security balance in favour of national security interests. The response of the ECtHR, as a human rights court, has been to convert what had been the exception - hearing about secret surveillance cases *in abstracto* - into the norm, by making it easier for those who feel threatened by mass surveillance measures, as distinct from being subject to them, to have their cases heard *in abstracto*.

In *Szabó and Vissy v Hungary*,[162] the Court found that there had been a violation of the applicants' right to respect for private and family life, agreeing with the applicants' submission that they could be subjected to intrusive measures without the availability of adequate remedies at national level, and guarantees against the abuse of these measures. The key to the Court's understanding of the balance to be struck between the protection of privacy rights and the protection of national security through secret surveillance measures is found in the following:

[160] ibid, at para 33.
[161] 'The Court has consistently held in its case-law that its task is not normally to review the relevant law and practice *in abstracto*, but to determine whether the manner in which they were applied to, or affected, the applicant gave rise to a violation of the Convention..' *Kennedy v The United Kingdom* Application No. 26859/05 (2010), at para 119.
[162] *Szabó and Vissy v Hungary* Application No. 37138/14. 12 January 2016. (2016) 63 E.H.R.R. 3.

> When balancing the interest of the respondent State in protecting its national security through secret surveillance measures against the seriousness of the interference with an applicant's right to respect for his or her private life, the national authorities enjoy a certain margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security. However, this margin is subject to European supervision embracing both legislation and decisions applying it. In view of the risk that a system of secret surveillance set up to protect national security may undermine or even destroy democracy under the cloak of defending it, the Court must be satisfied that there are adequate and effective guarantees against abuse.[163]

The Court found that the Hungarian legislation under the National Security Act did not satisfy the 'adequate and effective guarantees against abuse' required.[164]

4.0 Shortcomings in the Jurisprudence of the ECtHR - The Application of the Margin of Appreciation

The margin of appreciation has been defined as

> [T]he breadth of deference the Strasbourg organs will allow to national legislative, executive and judicial bodies before they will disallow a national derogation from the [the European Convention for the Protection of Human Rights and Fundamental Freedoms], or before they will find a restriction of a substantive convention right incompatible with a State Party's obligations under the Convention.[165]

A simpler definition describes the margin of appreciation as referring to the latitude allowed to Member States in their observance of the principles enunciated in the ECHR. As the concept has developed in the jurisprudence of the ECtHR, it implies a room for manoeuvre given to national authorities in assessing the degree to which ECHR principles should be applied, taking into account local values, traditions, laws and practices.

[163] ibid, at para 57.
[164] ibid.
[165] Howard Charles Yourow, 'The margin of appreciation doctrine in the dynamics of European human rights jurisprudence' 3 (1987) *Connecticut Journal of International Law* 111, 118.

There is a sense in which the routine application of the margin of appreciation by the ECtHR is best explained and understood in the light of the original understanding shared by the contracting parties that the ECHR would be supplementary to national constitutional systems in the role they would play in protecting fundamental rights such as those guaranteed in the Articles of the ECHR.[166] The treaty establishing the ECHR did not envisage the replacement of national laws nor did it have the aim of bringing about absolute uniformity of national rules. Instead, the Convention simply established a standard for the protection of rights which it guarantees, while leaving states free to go beyond this standard and to select the legal ways and means of protecting these rights.[167] When the treaty establishing the ECHR, was being drawn up, the concept of national sovereignty was foremost in the minds of the drafters. It was envisaged that 'the ECHR as an international treaty could serve as the lowest common denominator among diverse member states,' [168] a human rights floor rather than a ceiling.

The introduction of the margin of appreciation into the jurisprudence of the ECtHR, as several commentators have pointed out, had a pragmatic basis. Arai-Takahashi observes that the ECtHR judges 'have been aware that the treatment of their judgment and decisions has to rely ultimately on the good faith and co-operation of the contracting states.'[169] Waldock has argued that:

> [T]he doctrine of the margin of appreciation is one of the more important safeguards developed by the……Court to reconcile the effective operation of the Convention with the sovereign powers and responsibilities of governments in a democracy.[170]

[166] Herbert Petzold, 'The Convention and the Principle of Subsidiarity,' in *The European System For The Protection Of Human Rights* (Martinus Nijhoff, Dordrecht, 1993) 41.
[167] Article 60 of the ECHR states that nothing in the Convention shall be construed as limited or derogating from any human rights guarantees in the laws of the Convention States.
[168] See Yutaka Arai Takahashi, 'The Margin of Appreciation doctrine: a theoretical analysis of Strasbourg's Variable Geometry,' in Andreas Follesdal, Birgit Peters and Geir Ulf stein (eds.), *Constituting Europe: The European Court of Human Rights in a National, European and Global Context* (Cambridge University Press, 2013) 63.
[169] ibid.
[170] Humphrey Waldock, 'The Effectiveness of the system set up by the European Convention on Human Rights' 1 (1980) *Human Rights Law Journal* 1, 9.

Macdonald has emphasised that the process of bringing about a Europe-wide system of human rights protection and a 'uniform standard' of human rights must be 'gradual' because 'the entire legal framework rests on the fragile foundations of the consent of the Contracting parties.' [171] It is in this context that the deployment of the margin of appreciation is seen by its advocates as performing a useful function. As Macdonald puts it:

> '[I]t gives the flexibility needed to avoid damaging confrontations between the Court and the Contracting States over their respective spheres of authority and enables the Court to balance the Sovereignty of Contracting Parties with their obligations under the Convention.[172]

The margin of appreciation was first resorted to in the context of the derogation clause in Article 15 of the ECHR, which allowed Member States to derogate from human rights provisions of the ECHR if confronted with a public emergency posing a significant threat to state security. In the very early cases dealing with Article 15 derogation applications, one of these being the *Cyprus case*, the United Kingdom authorities were permitted to exercise 'a certain measure of discretion' in evaluating the proportionality of a derogating measure in relation to a serious state of unrest in the British colony of Cyprus. [173] It was not too long before the term 'measure of discretion' mutated into that of 'margin of appreciation.' This happened in the *Lawless* case where the ECtHR granted the Irish Government 'a certain discretion - a certain margin of appreciation' in assessing the existence of a public emergency.[174] The margin of appreciation formula was finally entrenched and its scope further enlarged in *Ireland v United Kingdom*, where the Court proposed a sliding scale on which the range of the application would vary. National authorities dealing with emergency situations were given a 'wide margin of appreciation in assessing the existence or otherwise of an emergency, and the range and scope of the derogating measures necessary to deal with it.[175]

---

[171] R. St. J. Macdonald, 'The Margin of Appreciation,' in R. St. J. Macdonald, F. Natcher and H. Petzold (eds.) *The European System for the Protection of Human Rights* (Dortrecht London: Martinus Nijhoff, 1993), 123.
[172] ibid.
[173] *Greece v United Kingdom* (Application No 176/56 (1958-9), 174, at 176.
[174] *Lawless v Ireland* (Appeal No 5319/57 (1960-61), at para 82.
[175] *Ireland v United Kingdom* (Application No. 5310/71, (1978), at para 207.

Until the late nineteen-seventies, the Court's application of the margin of appreciation tended to be largely *ad hoc* and experimental. With the passage of time it has been expanded, extending its range from Article 15 derogation cases to cases involving substantive human rights issues, personal freedom rights, including private rights. This evolution in the use of the concept is illustrated in the growing volume of cases involving the limitation clauses under Article 8-11 ECHR, in which data privacy/national security balancing issues loomed large. It is in the process of balancing the individual rights of citizens (data privacy being a major one) and public interest claims, that the application of a margin of appreciation is most prominent, and most controversial. The extensive use of the concept in attempting to rationalise the relationship between the rights of individuals (for instance data privacy), and collective interests (such as national security) has been subjected to much hostile comment. One commentator has claimed that the term 'margin of appreciation' might be rendered redundant if the concept of a fair balance were deployed more consistently and coherently in the *modus operandi* of the ECtHR.[176] Far from being re-entered redundant in the practice of the ECtHR, however, it has been acknowledged by one of its judges that 'the margin of appreciation is at the heart of virtually all major cases that come before the Court, whether the judgments refer to it explicitly or not.'[177] By 2001, Gross and Ní Aoláin were able to claim that 'the margin of appreciation doctrine has come to occupy a central position in jurisprudence of the European Court of Human Rights.' [178]

The margin of appreciation may be regarded by the Court as a useful tool to define the relations between the domestic authorities and the ECHR [179] and thus served a useful practical purpose. However, its critics tend to see it as furtively introducing subjective and relativist standards into treaty provisions of human rights treaties and formal sources of international law. The political risk involved here is that the introduction of such standards into case law

[176] See Alasdair. Mowbray, 'A Study of the Principle of Fair Balance in the Jurisprudence of the European Court of Human Rights' 10(2) (2010) *Human Rights Law Review* 289.
[177] RJ Macdonald, 'The Margin of Appreciation in the Jurisprudence of the European Court of Human Rights', in Anon (ed), *International Law at the Time of its Codification, Essays in Honour of Judge Roberto Ago* (Giuffrè, Milan 1987) 187-208, 192.
[178] Oren Gross and Fionnuala Ní Aoláin, 'From Discretion to Scrutiny: Revisiting the Application of the Margin of Appreciation Doctrine in the Context of Article 15 of the European Convention on Human Rights' 23(3) (2001) *Human Rights Quarterly* 625.
[179] *A and Others v United Kingdom* No. 3455/05, Grand Chamber 2009, at para 184.

would run counter to the 'universalizing project' of human rights. The margin of appreciation might be deployed as a conceptual 'Trojan horse' for the purpose of fragmenting the unity and harmony of established ECHR standards.[180] Some critics of the concept are even more scathing than this, emphasising the negative effects of the margin of appreciation on the substantive protection of human rights brought about by undue deference to the concerns of states over individuals, the protection of whose rights is the main concern of the European Convention on Human Rights. Lord Lester of Herne Hill, Q.C., himself a Judge, has claimed that:

> The concept of the "margin of appreciation" has become as slippery and elusive as an eel. Again and again the Court now appears to use the margin of appreciation as a substitute for coherent legal analysis of the issues at stake… The danger of continuing to use the standardless doctrine of the margin of appreciation is that…. it will become the source of a pernicious "variable geometry" of human rights, eroding the *acquis* of existing jurisprudence and giving undue deference to local conditions, traditions and practices.[181]

A similar, if even more radical, assessment of the use of the margin of appreciation in cases involving human rights was advanced by Judge De Meyer in a partly dissenting judgment:

> But where human rights are concerned, there is no room for a margin of appreciation which would enable the states to decide what is acceptable and what is not.
>
> On that subject the boundary not to be overstepped must be as clear and precise as possible. It is for the Court, not each state individually, to decide that issue, and the Court's views must apply to everyone within the jurisdiction of each state.

[180] Eyal Benvenisti, 'Margin of Appreciation, Consensus and Universal Standards' 31 (1998-99) *New York University Journal of International Law and Practice* 843,844.
[181] Lord Lester of Herne Hill, Q.C., Universality Versus Subsidiarity: A Reply. *European Human Rights Law Review* 1 (1998) 73, 75-75, citing Lord Lester of Herne Hill, Q.C., General Report Proceedings of the 8th International Colloquy On The European Convention On Human Rights (1995) 227, 236-37.

> The empty phrases concerning the State's margin of appreciation—repeated in the Court's judgments for too long already—are unnecessary circumlocutions, serving only to indicate abstrusely that the states may do anything the Court does not consider incompatible with human rights.
>
> Such terminology, as wrong in principle as it is pointless in practice, should be abandoned without delay.[182]

Del Moral observes that '[t]he Trojan Horse-like character of the Strasbourg's judge-made margin-of-appreciation doctrine' which has become a component of human rights protection in Europe, has long since bothered human rights lawyers.'[183] Del Moral further comments:

> Cases of reliance on this review doctrine have been generally criticised as denials of justice for individuals, abdications by the Court of its duty of adjudication in difficult or sensitive issues or as a judicial diluting technique of the strict conditions laid down in the European Convention on Human Rights.[184]

A feature of numerous ECtHR cases is the lax application of the margin of appreciation by the Court. Examples include cases in which the ECtHR has to decide whether a particular interference with an ECHR right is justified. In addressing that question, the Court often invokes the margin of appreciation without drawing on a substantive theory of rights as a justification for the conclusions it reaches. In other cases, the margin of appreciation concept may be invoked for dismissing an applicant's claim that his rights have been violated, and for declining to undertake a substantive review of the decision of national authorities as to whether there had been a violation. In many instances, the concept has been used by the Court as a substitute for careful and painstaking reasoning based on coherent interpretative principles. The case law on the balancing of the right to data privacy against the interests of national security, features many unsubstantiated generalisations when the Court is

[182] *Z v Finland* (Application No. 22009/93) (1998) 25 E.H.R.R. 371 at paras 415 to 417.
[183] Ignacio de la Rasilla del Moral, 'The Increasingly Marginal Appreciation of the Margin-of-Appreciation Doctrine' 6(7) (2006) *German Law Journal* 611.
[184] ibid, 611-12.

assessing the existence of one or more of the legitimate aims of a state intervention underpinned by the State's enjoyment of a wide margin of appreciation. In cases like this, when security-related purposes are deemed by the Court to have justified the limitation on privacy rights, the Court often tends to avoid reasoned argumentation on how and why the state intervention to the detriment of privacy serves the identified legitimate aim. Instead, the wording used by the Court indicates a desire on its part to dispense with argumentation and concede to the Government in question, as if its agenda is to dispose with cases as quickly as possible. Some commentators have suggested that the tendency of the Court to use the margin of appreciation to reach speedy decisions in the absence of a substantive review of the justification for State interference with protected privacy rights, may be explained by considerations of 'judicial economy.'[185] Greer highlights the contention of some commentators that:

> Determining if an application is, or is not, manifestly ill-founded requires the exercise of judgment and the interpretation of conduct, facts, and norms; it is, therefore, inescapably discretionary. Some commentators maintain that many complaints are rejected on this basis simply because the Court does not have the resources to consider them properly.[186]

Shany points to a 'resource gap'[187] in the Court's capacity to collect evidence on other empirical data, so that 'a utilitarian rationale bolsters the Strasbourg judges' decision to endorse the 'fact-finding' and ascertainment of a state of emergency by the national authorities.[188] It is noted that '[i]n September 2008 the pending applications totalled 100,000. Each month around 2,300 new applications are filed, whereas the Court can only handle an average of 1,500 a month.' [189]

---

[185] Yukata Arai-Takahasi, *The Margin of Appreciation Doctrine and the and the Principle of Proportionality in the Jurisprudence of the ECtHR* (Intersentia, Antwerp, 2002), 238-241.
[186] Steven Greer, 'What's Wrong with the European Convention on Human Rights?' 30(3) (2008) *Human Rights Quarterly* 680, 686.
[187] Yuval Shany, 'Towards s General Margin of Appreciation Doctrine in International Law?' 16(5) (2006) *European Journal of International Law* 907, 918.
[188] ibid, 919.
[189] Advisory Report on the Application of Protocol No. 14 to the European Convention on Human Rights and Fundamental Freedoms,' cited in *Netherlands International Law Review* 56(1) (2009) 71-92,75.

The lax application of the margin of appreciation may be seen in its readiness to accept the word of state authorities that security-related purposes justified their limitation of the privacy rights of their citizens. In cases where the State does not affirm the existence of a legitimate aim for its limitation of privacy rights and the applicant contests the existence of such an aim, the ECtHR is prepared to further the State's case without undertaking a review of privacy:

> While the applicant contested the existence of a legitimate aim, the government did not expressly refer to any legitimate aim in this case. The Court, for its part, is ready to accept that the impugned measure pursued the legitimate aims of safeguarding national security and preventing disorder.[190]

Readiness to accept the State's case on trust is exemplified in the consistent employment of phrases such as 'the Court finds it established' [191] or 'the Court is prepared to accept' what the Government tells it.[192] The lack of a reverse statement by the applicant may be sufficient for the Court to affirm the establishment of a legitimate aim: 'The applicant did not appear to deny that the impugned restrictions were imposed in pursuit of legitimate aims.' [193] Even the probability or possibility of the establishment of a legitimate aim may prove sufficient, in the eyes of the Court, to lead it to conclude that there was, in fact, such a legitimate aim: the intervention [by the State] 'could have been in the interests' of the relevant purposes, or alternatively, 'the Court therefore concludes that the interference pursued a legitimate aim.' [194] The proposition that 'if something could have been, therefore it was, is not legitimate, whatever may be said of the aim pursued by the Belgian Government.

When one tries to discern what conclusion may be drawn from this about the *modus operandi* of the ECtHR in cases involving the balancing of data privacy rights against the demands of national security, and also involving the extension of a generous margin of appreciation to the State, the unmistakable

[190] *Cubature v Moldova*, No. 27138/04, (2010), at para 55.
[191] *Nada v Switzerland* (Application no. 10593/08) 12 September 2012, at para 174.
[192] *Liu v Russia* No. 29157/09, (2011) at para 80.
[193] *Nada v Switzerland* (Application no. 10593/08) 12 September 2012, at para 174.
[194] *Mubilanzila Maycka and Kaniki Mitunga v Belgium* (Application no. 13178/03) 12 October 2006, at para 79.

impression is that in the Court's views, the power to decide on the legitimacy of the security-based restriction on privacy falls within the competence of the State, such competence not being impinged on by the privacy-based provisions of the ECHR and not subject to reconsiderations by the ECtHR. This would help to explain why the ECtHR has seldom found a violation of ECtHR rights by reference to the legitimate aim standard. The same might be said of cases in which the purpose of state interference is not motivated by security concerns.[195] It would also account for the perfunctory dispatch of the claims made by applicants that they have been victims of state interference with their privacy rights in the interest of State security, in the context of a generous margin of appreciation.

The interaction between the margin of appreciation doctrine and the requirement of 'necessity in a democratic society' stipulated in Article 8(2) ECHR, as Burke observes, 'poses an intricate question of balances.'[196] While application of a margin of appreciation, especially a wide margin, tends to favour Member States, the requirement of necessity means that the balance must not be tipped too far against individual States.[197] As the ultimate interpreter of the ECHR, the ECtHR, it seems reasonable to argue, should not defer uncritically to the national governments' determinations of necessity, but should undertake an independent examination of the relevant facts and the reasons the State advances for derogating from Convention guarantees. Jacobs remarks that an objective test must be applied to determine whether restrictive measures are necessary, the question to be answered 'is not, did the authorities think they had sufficient reason, but did they have sufficient reason in fact.'[198] However, the judicial techniques employed by the ECtHR under the margin of appreciation doctrine, as Burke observes, 'tend to inhibit precisely this kind of inquiry.' [199] There is much to be said for the view that the Court has tended to use the margin of appreciation as 'a self-denying ordinance' against its own

[195] Pieter van Dijk et al (eds.), *Theory and Practice of the European Convention on Human Rights* (Intersentia, 2006), 340.
[196] Karen C. Burke, 'Secret Surveillance and the European Convention on Human Rights' 33 (1981) *Stanford Law Review* 1113, 1133.
[197] Rosalyn Higgins, 'Derogations under Human Rights Treaties' 48(1) (1976) *British Yearbook of International Law* 281, 313.
[198] Francis Jacobs, *The European Convention on Human Rights* (Oxford, 1975) 19.
[199] Karen C. Burke, 'Secret Surveillance and the European Convention on Human Rights' 33 (1981) *Stanford Law Review* 1113. 1133.

review of all the evidence before it. In cases where the Court is acting in this spirit, it is failing in its duty to address the findings of fact and law against the relevant provisions of the ECHR in order to ascertain whether ECHR guarantees have been violated.[200]

In some more recent cases, the ECtHR has been noticeably more vigilant in ascertaining the facts surrounding an alleged violation of the ECHR by carrying out a thorough investigation of the formal legal process available in the Member States affording substantive protection for individual privacy rights, and adequate safeguards against the abuse of these rights when secret surveillance is carried out by the State in question. Such an investigation was carried out by the Court in *Roman Zakharov v Russia* [201] By contrast, in the case of *Klass and Others v The Federal Republic of Germany* [202] where the ECtHR accorded a wide margin of appreciation to the State against a background of terrorist threats to its security. The applicants, five German lawyers, challenged German legislation which permits the State authorities to open and inspect mail and listen to telephone conversations in order to protect against 'imminent dangers' threatening 'the existence and security of the State.' The applicants claimed that the legislation infringed Article 8 ECHR (right to respect for correspondence). They further challenged the law because it did not require a court order to authorise wire-tapping and did not require post-surveillance notification to those who had been surveilled in every case.[203] The essence of the applicants' position was that individuals throughout Germany might never know they were objects of surveillance and might, as a result, never know they were under surveillance, and might never seek judicial recourse because the authorisation and implementation of wiretaps remained secret.

The Court acknowledged that surveillance procedures must provide 'adequate and effective safeguards against abuse,' based on a relative assessment of particular circumstances.[204] The Court also cautioned that governments ought

[200] Clovis C. Morrisson, 'Margin of Appreciation in European Human Rights Law' 6 (1973) *Human Rights Law Journal* 263.
[201] *Zakharov v Russia* Application no. 47143/06 (2015).
[202] *Klass and Others v Federal Republic of Germany* (1979-1980) 2 EHRR 214.
[203] ibid, at para 10.
[204] ibid, at para 50.

not to implement whatever measures they considered appropriate, but also stated, by way of qualification, that Member States enjoy a 'margin of appreciation,' adding that 'it is surely not for the Court to substitute for the assessment of the national authorities any other assessment of what might be the best policy in this field.' [205] In this way, the Court is using the margin of appreciation as a means to allow the State authorizing breaches of privacy rights, in a national security context, to decide on the legitimacy or otherwise of what it is doing. At the same time, the Court is prescinding from its duty to test the State action in the light of ECHR standards. The Court also demonstrated its willingness to accommodate the State authorities by authorising them to enforce measures for the supervision of surveillance at below the optimum level. Having asserted that 'it is in principle desirable to entrust supervisory control to a judge,' on the ground that the judiciary offers the best guarantee of independence and impartiality, the Court found that by 'having regard to the nature of the supervisory and other safeguards provided' in the domestic West German law complained of, the Court found that the absence of judicial control does not exceed the limits of what may be deemed necessary in a democratic society.' [206] However, applying the doctrine of the margin of appreciation to the German surveillance law, the Court concluded that the German system remained within the margin because it provided an adequate substitute for judicial control in the form of parliamentary supervision. The Court found in favour of the German State.

As Burke points out, the *Klass* Court 'might have reached a very different conclusion if it had examined the intelligence law's *actual* operation.' In effect, she argues, the Court 'approved a surveillance system whose formal procedural safeguards are vitiated by its lack of substantive protection for individual privacy rights.'[207] The actual operation of German intelligence laws was far less rigorous than even the Court had envisaged. The supervision of surveillance was entrusted to an extra-judicial Advisory Commission which did

[205] ibid, at para 49.
[206] ibid, at paras 55-6.
[207] Karen C. Burke, 'Secret Surveillance and the European Convention On Human Rights' 33 (1981) *Stanford Law Review* 1134-1135.

not follow judicial procedures, its deliberations being secret. Advisory parties were not heard, and there was considerable scope for political influence.[208]

The application by the ECtHR of the margin of appreciation doctrine in the context of the derogation regime under Article 15 in situations of entrenched emergency, reveals some of the deleterious consequences for the substantive protection of privacy rights and the integrity of oversight by an international court that can follow from the misplaced judicial self-restraint characteristic of the ECtHR in derogation cases. In almost all of these, the Court has extended and widened the margin of appreciation, progressively eroding its ability to exercise an efficient system of supervision of the activities undertaken by State agencies in circumstances of alleged threats to national security. The practice of the ECtHR in dealing with Article 15 derogation cases should be tested against the conditions laid down in Article 15(1) of the ECHR governing the right of Member States to derogate from individual rights that are otherwise protected under the Convention. If a State derogation is to conform to the terms of the derogation clause, it has to satisfy two primary conditions: 'the existence of a war or other public emergency threatening the life of the nation,' and the state 'may take measures derogating from its original obligations' under the ECHR [ie derogating from otherwise protected rights] to the extent strictly required by the exigencies of the situation, provided that such measures are not inconsistent with its obligations under international law.' Thus, there are limits to what the state may do in derogation cases. However, Article 15 (1) offers no guidance on the part to be played by the ECtHR in the investigation of the alleged national emergency, or in determining whether the measures taken by the State are proportionate and not inconsistent with its international law obligations.

The ECtHR has never regarded the margin of appreciation, however wide its scope, as conferring an unlimited discretion on the derogating Government. For example, the Court acknowledged its own supervisory responsibilities in *Ireland v United Kingdom*:

[208] R.B. Kamlah, 'The Invasion of privacy by Electronic Listening devices in the United States and Germany,' International Symposium on Comparative Law (University of Ottawa Press, 1970) 161, 191.

> [T]he States do not enjoy an unlimited power in this respect. The Court, which, with the Commission, is responsible for ensuring the observance of the States' engagements (Art. 19), is empowered to rule on whether the States have gone beyond the 'extent strictly required by the exigencies' of the crisis. The domestic margin of appreciation is thus accompanied by a European supervision.[209]

The right of the ECtHR to act in a supervisory capacity in derogation cases is consistently asserted in its case-law. In the *Lawless* case, the Court declared itself competent to exercise its supervisory function in reviewing the national emergency claims of State authorities in Article 15 cases and the proportionality of their response. Nevertheless what matters in terms of the data privacy/national balance is the extent to which the ECtHR is prepared to exercise the supervisory function it lays claim to. In Article 15 derogation cases the robust exercise of this function would do much to ensure that alleged public emergencies 'do not become a pretext [for] unwarranted deviations from the [privacy] guarantees provided by the European Convention.' [210] In effect, the active agreement of the ECtHR with its invigilatory task and its strict scrutiny of state measures in derogation situations, would do much to obviate the danger of state erosion and sometimes abrogation of privacy rights and impede state parties from engaging in uncontrolled interference with the privacy rights guaranteed in Article 8(1), The ECtHR itself in its case law has assumed the task of taking on an active invigilatory role in Article 15 cases, declaring that in exercising its supervision, 'the Court must give appropriate weight to such relevant factors as the nature of the rights affected by the derogation, the circumstances leading to, and the duration of, the emergency situation.' [211]

For these strong assertions by the Court to have value, they must be borne out in its *modus operandi*. However, a notable feature of its case law when an Article 15 derogation is involved, is the contrast it reveals between what it

[209] The Republic of *Ireland v The United Kingdom* Series A, No. 25 18 January 1978 (1979-80) 2 E.H.R.R. 25, at para 207.
[210] Oren Gross and Fionnuala Ní Aoláin, 'From Discretion to Scrutiny: Revisiting the Application of the Margin of Appreciation Doctrine in the Context of Article 15 of the European Convention on Human Rights' 23(3) (2001) *Human Rights Quarterly* 625, 635.
[211] *Brannigan and McBride v United Kingdom*, Series A, No. 258-B Application Nos. 14553-14554/89 26 May 1993 (1994) 17 E.H.R.R. 539, 570 at para 43.

proclaims it must do and what it does.[212] The Court's approach in *Aksoy v Turkey* [213] is a typical instance of this contrast. The Court repeats its standard reference to its well-established holding that the wide domestic margin of appreciation in derogation cases should be accompanied by ECtHR supervision, and provides details on the scope of this, citing as precedent its holding in *Branigan and McBride v The United Kingdom*.[214] Two paragraphs later, the Court peremptorily disposes of the existence of a prolonged public emergency allegedly threatening the life of the Turkish nation and the privacy rights issues arising therefrom in a single sentence: The Court considers, in the light of all the material before it, that the particular extent and impact of PKK terrorist activity in South East Turkey has undoubtedly created, in the region concerned, a "public emergency threatening the life of the nation."[215] There is no evidence in this case of any attempt on the part of the Court to review the nature of the threat with reference to the measures taken by the Turkish State to deal with it. It is not incoherent to argue, as Gross and Ní Aoláin do, that there is a strong case for strict scrutiny of a derogating Government's arguments, and for invoking the narrowest possible margin of appreciation when an entrenched emergency is at issue, and that 'there should be an inverse connection between the scope of the margin of appreciation allowed to a derogating government in a particular case and the length of the emergency situation.'[216]

The generous use of the margin of appreciation, particularly the manner in which the Court applies it, defies coherent explanation. This is because, as Greer points out, 'no simple formula can describe how it works,' and it has a 'caustic, uneven and largely unpredictable nature.'[217] It is not clear from the

[212] Article 15 ECHR affords contracting states the ability to derogate from their obligations to uphold rights and freedoms enshrined in the Convention on Human Rights. Such derogations obtain only in exceptional circumstances, in a limited and supervised manner. The conditions necessary for a valid derogation to be permissible are enshrined in Article 15(1): (1) In times of war or other public emergency where the life of a nation is under threat; (2) Measures taken in response to instances of war or public emergency, must not exceed what is strictly necessary as required by the exigencies of the situation and (3) That any measures taken cannot be inconsistent with other obligations attaching to a State under international law.

[213] *Aksoy v Turkey* Application No. 21987/93 18 December 1996 (1997) 23 E.H.R.R. 553.

[214] ibid. See paras 77, 80, 180 and 181.

[215] *Aksoy v Turkey* Application No. 21987/93 18 December 1996 (1997) 23 E.H.R.R. 553 587, at para 70.

[216] Oren Gross and Fionnuala Ní Aoláin, 'From Discretion to Scrutiny: Revisiting the Application of the Margin of Appreciation Doctrine in the Context of Article 15 of the European Convention on Human Rights' 23(3) (2001) *Human Rights Quarterly* 625, 647.

[217] Steven Greer, 'The Margin of Appreciation Interpretation and Discretion under the European Convention on Human Rights' (Council of Europe, 2000), 1,5.

practice of the ECtHR when the margin of appreciation should be used or what its limits or contours are. Furthermore, it is not possible to predict with any degree of precision what the consequences of invoking it might be.[218] The confusion, vagueness, uncertainty and unpredictability associated with the Court's deployment of the margin of appreciation is a function of its common practice of referring to 'a certain margin of appreciation' without indicating its width. For example, a study of the 108 references to the margin in the first half of 2009, indicated that the width of the margin, whether wide or narrow, was specified in only 24 cases, while the remaining ones mention 'a certain margin of appreciation' or 'a margin of appreciation' without an adjective. The use of vague locutions such as these is unhelpful, in addition to being a source of confusion. The case of *Sanoma Uitgevers B.V.* v *The Netherlands* [219] illustrates this point. In this case, the Third Section of the ECtHR, having allotted 'a certain margin of appreciation'[220] to the State party, went on to assert that it must ascertain 'whether the measure' taken by the State was "proportionate to the legitimate aims pursued" [221] The Court carried out its own proportionality analysis without adverting explicitly to the margin of appreciation with the result that the 'certain margin of appreciation' [222] allocated by the Court does nothing to clarify the rationale behind the Court's analysis. The case was decided by four to three. The dissenting judges commented on 'the most careful scrutiny' that the Court should have exercised.[223] It appears that the disagreement among the judges concerned the appropriate breadth of the margin of appreciation. This, however, is not reflected in the judgment, which means that the Court's reasoning lacks transparency.

Brauch considers that the margin of appreciation threatens to undermine the rule of law, two key elements of which are clarity and predictability.[224] Fuller has argued that consistency in decision-making based on rules of law is

[218] Jan Kratochvíl, 'The Inflation of the Margin of Appreciation by the European Court of Human Rights' 29 (3) (2001) *Netherlands Quarterly of Human Rights* 324, 325.
[219] 31 March 2009, Application No. 38224/03.
[220] ibid, at para 54(a).
[221] ibid, at para 54(c).
[222] ibid, at para 54(a)
[223] Dissenting opinion of Judges Power, Gyulumyan and Ziemele.
[224] Jeffrey A. Brauch, 'The Margin of Appreciation and the Jurisprudence of the European Court of Human Rights: Threat to the Rule of Law' 11 (2005) *Columbia Journal of European Law*, 125.

fundamental to any legal system.[225] It is also the case that the rule of law together with foreseeability as to the effects of domestic law are long-established principles if ECtHR jurisprudence in cases dealing with the privacy-security balance. In such cases, involving recourse by the Court to Article 8(2) and, to a lesser extent Article 15 ECHR, the standard formula of the Court is that 'in accordance with the law' means 'in accordance with the rule of law,' which is expressly mentioned in the Preamble to the ECHR, and 'inherent in the object and purpose of Article 8.'[226] The Court makes it clear in its case law that conforming to the rule of law means meeting 'quality requirements,' one of which is that it must be 'foreseeable as to its effects' on the persons affected. The Court has also held that

> In matters affecting fundamental rights it would be contrary to the rule of law, one of the basic principles of a democratic society enshrined in the Convention, for a legal discretion granted to the executive to be expressed in terms of unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question, to give the individual adequate protection against arbitrary interference.[227]

How does the *modus operandi* of the ECHR comport with the Court's own judicial principles necessitating a rule of law-based decision-making process ensuring clarity and foreseeability? How does the Court's use of the margin of appreciation in privacy/security cases match clarity and predictability requirements which Brauch associates with the rule of law, or the requirements of consistency in decision-making based on rules of law outlined by Fuller? There can be little doubt that the ECHR, in many cases, is inconsistent in its use of the margin of appreciation, as has been shown in examples discussed. This inconsistency arises from the fact that there are no set rules governing the use of the margin, with the result that many of the judgments of the Court lack the support of a coherent, rule-based and principled decision-making process, in the absence of which judgments can appear quite arbitrary. This, as

[225] Lon L. Fuller, *The Morality of Law* (Yale University Press, New Haven 1969) 34-41.
[226] *Kennedy v The United Kingdom* at para 151. See also footnotes 51 to 57 supra.
[227] *Liu v Russia*, no. 42086/05, 6 December 2007, at para 56.

Kratochvíl observes, 'helps to build a judicial environment akin to a legal realist paradise where judges can decide cases on whatever preference they have.'[228] The lack of clarity and predictability when the margin of appreciation is involved also undermines the principle of legal certainty and the principle that legal uncertainty is incompatible with a fundamental right, deemed important by the ECtHR itself. A recent reiteration of these principles is found in *Zolotukhin v Russia* [229] The key paragraph in this judgment reads:

> The Court considers that the existence of a variety of approaches to ascertaining whether the offence for which an applicant has been prosecuted is indeed the same as the one of which he or she was already finally convicted or acquitted engenders legal uncertainty incompatible with a fundamental right, namely the right not to be prosecuted twice for the same offence. It is against this background that the Court is now called upon to provide a harmonised interpretation of the notion of the "same offence"—the *idem* element of the *non bis in idem* principle—for the purposes of art.4 of Protocol No.7. While it is in the interests of legal certainty, foreseeability and equality before the law that the Court should not depart, without good reason, from precedents laid down in previous cases, a failure by the Court to maintain a dynamic and evolutive approach would risk rendering it a bar to reform or improvement. [230]

Were this kind of reasoning to be adopted in conjunction with a more nuanced, rule-based, far less diffuse and automatic application of the margin of appreciation, its use might serve a purpose, especially if criteria could be devised setting out clearly the circumstances in which it could be used. What is difficult to defend is the overuse of the practice of applying a wide margin of

[228] Jan Kratochvíl, 'The Inflation of the Margin of Appreciation by the European Court of Human Rights' 29 (3) (2001) *Netherlands Quarterly of Human Rights* 352.
[229] Application No.14939/0310 February 2009 (2012) 54 E.H.R.R. 16.
[230] *Zolotukhin v Russia* Application No.14939/0310 February 2009 (2012) 54 E.H.R.R. 16, at para 78. The Applicant, a Russian citizen, brought his girlfriend onto a Russia military base while drunk. During his arrest, he threatened the arresting officer. At an administrative hearing the following day, the Applicant was found guilty. He was subsequently prosecuted and was bought before a Russian Criminal Court, which referred the case to the ECtHR and sought clarification regarding what constitutes the same offence as captured by article 4 of the seventh additional protocol attaching to the ECHR. The Court held that two parallel proceedings in train at the same time, which are grounded upon the same facts, should be held to concern the same offence as captured by the ECHR and that where two proceedings are in being in such circumstances, this constitutes a breach of article 4 of seventh additional protocol.

appreciation to the degree that it effectively extends to Member States virtually unlimited discretion to restrict the human rights enumerated in Articles 8-11 ECHR.[231] It is not surprising, in the light of widespread dissatisfaction with some of the practices of the ECtHR, including the quality and comprehensibility of the reasoning in its judgments, that discussions have been taking place on the reform of the ECHR system, including the ECtHR. In 2009, the President of the ECtHR suggested the setting up of a conference of State parties to discuss the problems facing the Court and its future. In response, the Swiss Government organised a conference in Interlaken. The first outcome of this Conference was the Interlaken Declaration, which committed the parties to an action plan. Mowbray observes that one of the initiatives involves '[t]he supervision of the execution of judgments by the Committee of Ministers should be made more 'efficient and transparent' by, *inter alia*, according greater priority to cases disclosing significant structural problems.[232] The declaration stressed the importance of ensuring 'the clarity and consistency of the Court's case law.' [233] The process inaugurated in 2009 is not likely to conclude until the end of 2019.[234]

5.0 The ECtHR and the CJEU Nexus: Mutual Influence

The European right to privacy, in its various forms, emanates from two overlapping systems: the Council of Europe and the European Union. From the perspective of the human right to privacy, and by extension the right to data privacy, the Council of Europe was first in the field, with the European Convention for the Protection of Human Rights and Fundamental Freedoms [235] and the European Court of Human Rights. However, the importance of fundamental rights has long also been a preoccupation of the European Union, as is clear from the Joint Declaration of the European Parliament, Council and Commission concerning the protection of fundamental rights and the ECHR

[231] See Cora S. Feingold, 'The Doctrine of Margin of Appreciation and the European Convention of Human Rights' 53 (1978) *Notre Dame Law Review* 90-106.
[232] Alaistair Mowbray 'The Interlaken Declaration - The Beginning of a New Era for the European Court of Human Rights?' 10(3) (2010) *Human Rights Law Review* 519, 526.
[233] High Level Conference on the Future of the European Court of Human Rights. Interlaken Declaration 19 February 2010. <http://www.echr.coe.int/documents/2010_interlaken_finaldeclaration_eng.pdf> accessed 21 October 2016.
[234] Iain Cameron, 'The Court and the Member States: Procedural Aspects,' in Andreas Føllesdal, Birgit Peters, Geir Ulfstein, (eds) *Constituting Europe. The European Court of Human Rights in a National, European and Global Context* (Cambridge University Press, 2013), 44.
[235] November 4 1950, 213, U.NT.S., 222.

issued on 5 April, 1977.[236] The reference in this Declaration to the Council of Europe Convention adumbrates what was to become a central feature of European Union rights law: the human rights protected by the EU legal order, including the right to the protection of personal data, were to a considerable extent transposed into the primary law of the EU and mediated in the jurisprudence of the EU Court of Justice (the CJEU). This has been emphasised in the case law of the CJEU:

> It must also be stated that fundamental rights form an integral part of the general principles of law whose observance the Court ensures. For that purpose, the Court draws inspiration from the constitutional traditions common to the Member States and from the guidelines supplied by international instruments for the protection of human rights on which the Member States have collaborated or to which they are signatories. In that regard, the ECHR has special significance…. [237]

What would prove to be the most significant instrument of primary legislation enacted by the EU was its own version of a Bill of Rights: the Charter of Fundamental Rights.[238] The right to privacy provisions are strongly influenced by those contained in the ECHR - one of the two Articles in the Charter dealing with privacy, the first, Article 7, copies the equivalent provision in the ECHR, word for word: 'Everyone has the right to respect for his or her private and family life, home and communications.' The second Charter provision dealing with privacy, Article 8, addresses itself to threats of privacy protection, specifically the protection of personal data by developments in electronic technology and the world wide web. Article 8(1) provides that 'everyone has the right to the protection of personal data concerning him or her.,' while Article 8(2) declares that such data must be 'processed fairly for specified purposes and on the basis of the consent of the person concerned, or some

[236] Official Journal of the European Communities (OJEC). 27.04.1977, No C 103. [s.l.] Article 1 of this Declaration reads: 'The European Parliament, Council and Commission stress the prime importance they attach to the protection of fundamental rights, as derived in particular from the Constitutions of Member States and the European Convention for the Protection of Human Rights and Fundamental Freedoms.'

[237] Case C-305/05, *Ordre des barreaux francophones and germanophone & Others v Conseildes Ministres* (ECJ, Grand Chamber) (26 June 2007), at para 29.

[238] Charter of Fundamental Rights of the European Union, December 7 2000, 2000 O.J. C 364, 1, 8.

other legitimate basis laid down by law.' Furthermore 'everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. Article 8(3) makes provision for the establishment of an independent authority to ensure compliance with the rules set out in Articles 8(1) and 8(2). The provisions for personal data protection measures in Article 8 of the EU Charter mirror those provided for in the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of January 28, 1981.[239]

The requirement of independent data protection authorities to oversee compliance with data-protection rules had been part of data protection schemes for almost three decades before the introduction of the EU Charter of Fundamental Rights. The influence of Convention 108 of the Council of Europe is also clear in the first EU Data Protection Directive.[240] The EU Data Protection Directive builds on Convention 108 of the Council of Europe in a variety of ways. The Directive begins with a restatement of the Convention's case provisions on lawfulness, specific purposes, necessity, accuracy and limited data retention.[241] Like the Convention, the Directive recognises certain categories of personal information that should receive special protection, [242] gives individuals a right of access to their personal information [243] and imposes a duty to adopt security measures to protect personal data.[244] Article 29 of the Directive provides for the establishment of the 'Article 29 Working Party' a supervisory body mandated to ensure compliance with the provisions of Directive 95/46/EC by the Member States.

The EU Charter of Fundamental Rights signifies its dependence on ECHR rights provisions. Article 52(3) of the Charter requires that the meaning and scope of Charter rights which correspond to ECHR rights are to be the same as those laid down by the ECHR. In a variety of cases, the CJEU has looked to the relevant ECtHR case-law for guidance on the interpretation of Charter

[239] Convention 108, EUR.TS No. 108.
[240] European Parliament and Council Directive 95/46. On the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995, O.J. (L 281) EC.
[241] ibid, Article 6.
[242] ibid, Article 8.
[243] ibid, Article 12.
[244] ibid, Article 17.

Articles.[245] As Craig and de Búrca observe, the ECtHR has in recent years made many references to, and actively accommodated, EU law and the jurisprudence of the CJEU, and has cited the EU Charter in many of its judgments.[246] The proportionality principle, a key element of the ECtHR data privacy/national security balancing paradigm, appears throughout the Data Protection Directive (95/46/EC). Government actors and private individuals who seek to collect and process personal information must demonstrate that their operations satisfy the proportionality principle- that the burden imposed on the right to personal data protection is proportionate to the aim being pursued through their data-processing operation.[247]

The Articles of the Treaty of Lisbon, which took formal effect in 2009 as the controlling instrument of EU Primary Law, amending the Treaty of The European Union and the Treaty Establishing the European Community, had two significant consequences following from two provisions of Article 6 of the Lisbon Treaty. The first, Article 6(1), recognised the EU Charter of Fundamental Rights (2000) as having the same value as the EU Treaties, thus making it an integral part of EU primary law and giving it binding legal force. The second, Article 6(2) declared that the EU 'shall accede to the European Convention for the Protection of Human Rights and Fundamental Freedoms, adding the rider that 'such accession shall not affect the Union's competences as defined in the Treaties.' Article 6(3) provided that the fundamental rights guaranteed by the ECHR, 'and as they result from the constitutional traditions common to Member States, shall constitute general principles of EU law: Article 6(3) is significant, since the EU Charter embodies elements both from the constitutional traditions common to the Member States and human rights, especially the privacy rights, guaranteed by the ECHR. In the formulation of the Charter, the influence of the ECHR has been paramount.[248] The drafters of the Charter used the ECHR as a model. This is clear from the Preamble to the Charter, which 'reaffirms …. the rights as they result, in particular, from …..the European Convention on Human Rights and Fundamental Freedoms and the

[245] Paul Craig and Gráinne de Búrca, *EU Law: Texts, Cases and Materials* (Sixth edn, Oxford University Press, 2011), 386, fn 30.
[246] ibid, 426.
[247] Article 7(f).
[248] See generally Steven Peers and Angela Ward, *The European Union and Fundamental Rights* (Oxford, Hart, 2004).

case law of ……..the European Court of Human Rights.' Furthermore, numerous provisions of the ECHR are reproduced in the Charter, some of them word for word. Paris has calculated that '[a]pproximately half of the substantive provisions of the Charter find their equivalent in the ECHR….or the case law of the ECtHR.[249]

In the context of the symbiotic relationship between the CJEU and the ECtHR and specifically in the context of the influence of the EU Charter on the jurisprudence of the ECtHR, it is worth noting that the ECtHR referred to the Charter at a very early stage, even before the CJEU did.[250] In the meantime, the ECtHR has made multiple references to the Charter since its adoption in 2002, 'giving the impression that the model [the ECtHR] has been overtaken by the copy [the Charter].'[251] The absorption of much existing ECHR human rights law by the Charter might suggest that the actual model, by overtaking the copy is part of a longer-term project by EU agencies to facilitate the emergence of the CJEU as the major European Human Rights Court. There is evidence in the jurisprudence of the CJEU, especially since the Charter became part of primary EU law in 2009, that the CJEU, instead of deferring to the extent that it had to the law and jurisprudence of the ECHR, becoming reluctant to embrace the project decreed in Article 6(2) of the Lisbon Treaty that the EU should accede to the ECHR, was striving for greater autonomy as a specifically EU Court. Accession by the EU to the ECtHR would mean that individuals whose ECHR rights had been breached by acts of the EU will be able to seek redress before the ECtHR. In other words, EU legal acts would be liable to be subjected to external review under the ECHR system.

[249] Marie-Luce Paris, 'Paving the way: Adjustments of Systems and Mutual Influences Between the European Court of Human Rights and European Union Law before Accession.' 51(1) (2014) *The Irish Jurist* 1,10.

[250] *Christine Goodwin v The United Kingdom* [Grand Chamber], Application Number 28957/95, 2002, at paras 58 and 100.

[251] Marie Luce Paris, 'Paving the way: Adjustments of Systems and Mutual Influences Between the European Court of Human Rights and European Union Law before Accession' 51(1) (2014) *The Irish Jurist* 11. See Articles 1,3,8, 11(2) and 22-26 of the Charter. In Article 19(2), the Charter 'Codifies' for example, the ECtHR case law arising from the cases of *Ahmed v Austria* (Application No 25964 (1986) and *Soering V United Kingdom* (1989), Series A, No. 161.

A 2012 study by the European Parliament of the Fundamental Rights case law of the CJEU and the ECtHR [252] indicated that 'the CJEU sometimes manifestly expressed the preference for the Charter over [the ECHR], without entering into conflict with the ECHR.' [253] Craig and de Búrca draw attention to a tendency on the part of the CJEU towards increasing reliance on the Charter and towards more autonomous interpretation of the Charter without reference to the ECHR.[254] De Búrca reports on the results of an analysis of the available cases in which the CJEU referred to the Charter from the time it gained binding effect in 2009 until the end of 2012. The statistics indicate that the frequency of citations of the CJEU to the ECHR had declined, and that 'whereas the CJEU used to cite the ECHR significantly more than the EU Charter in cases involving human rights claims, the reverse is now the case.' [255] More importantly, 'the CJEU does not cite or draw in any significant way on the relevant jurisprudence of other courts - including the European Court of Human Rights - when interpreting provisions of the Charter.'[256]

The prospect of accession of the EU to the ECHR had been a live subject of debate since the 1970s, as part of a vision for an integrated Europe-wide system of human rights protection in which the ECtHR, with its expertise and stature as a human rights Court, would exercise this function for all of Europe and the CJEU would not act as a parallel Human Rights Courts, leaving the sphere of human rights to the exclusive jurisdiction of the ECtHR.[257] Among the perceived advantages of the accession scheme, according to the European Commission which endorsed it, were that it would help to develop a common culture of fundamental rights in the EU, reinforce the credibility of the EU's

[252] Pompeu Fabra, Alejandro Saiz Arnalz and Aida Torres Pérez, 'Main Trends in the Recent Case Law of the EU Court of Justice and the European Court of Human Rights In the Fields of Fundamental Rights.' (April 2012) *European Parliament Civil Liberties, Justice And Home Affairs* <http://www.statewatch.org/news/2012/may/ep-study-ecj-echr.pdf> accessed 2 January 2017.
[253] Paul Craig and Gráinne de Búrca, *EU Law: Texts, Cases and Materials* (Sixth edn, Oxford University Press, 2011) 427.
[254] ibid.
[255] Grainne de Búrca 'After the EU Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator?' (2013) 20(2) *Maastricht Journal of European and Comparative Law* (2013) 168, 175.
[256] ibid, 175-76.
[257] Oddný Mjöll Arnardóttir and Antoine Buyse (eds.), *Shifting Centres of Gravity in Human Rights Protection: Rethinking Relations between the ECHR, EU and National Legal Orders* (Routledge, London and New York, 2016), p. 5. See also Paul Craig and Gráinne de Búrca, *EU Law: Texts, Cases and Materials* (Sixth edn, Oxford University Press, 2011) 419-420.

human rights system, place the weight of the EU behind the ECHR system, and ensure the harmonious development of the Courts.[258]

Following the passage of the Lisbon Treaty in 2009, Article 6(2) of which imposed a legal obligation to accede to the ECHR, political negotiations resulted in a Draft Agreement on Accession which took three years to complete. However, the CJEU, in its December 2014 Opinion on the Draft Agreement, decided that it was incompatible with the EU Treaties.[259] The main significance of Opinion 2/13 is that it reflects the determination of the CJEU to protect the independence of the EU legal architecture, the autonomy and exclusivity of its own jurisdiction, and its concern to avoid being part of any process that would legally bind EU legal norms too closely to those of the ECHR and, above all, to the rulings of the ECtHR. Along with the growing tendency of the CJEU to rely on the EU Charter as the primary source of EU law in conjunction with diminishing advertence to the ECHR in its case law, and the fact that the jurisprudence of the CJEU reveals a growing proportion of cases dealing with human rights issues, all suggest a common purpose: to defend and promote the autonomy of law. As Halberstam observes, the tone of Opinion 2/13, which is binding on EU Member States and the EU institutions, suggests that '[w]ary of its overburdened sibling [the ECtHR], the CJEU seems intent on guarding its privileged judicial position in Europe.' [260] Opinion 2/13 is not the final assertion by the CJEU of its role as final arbiter on the EU Charter and on human rights adjudication in an autonomous EU legal system. Its engagement with the Digital Rights case, [261] marks another phase in its growing dominance as a defender of human rights in Europe.

---

[258] 'European Commission acts to bolster the EU's system of protecting fundamental rights' European Commission Press Release IP /10/291 of March 2010 <http://europa.eu/rapid/press-release_IP-10-291_en.htm?locale=en> accessed 28 October 2016.

[259] Opinion Pursuant to Article 218 (11) TFEU, C-2/13. December 18 2014 <http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d5498e825298f346e99568a78451b88b99.e34KaxiLc3eQc40LaxqMbN4Pa3mSe0?text=&docid=160882&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=432736> accessed 7 September 2016.

[260] Daniel Halberstam, 'It's the Autonomy Stupid! A Modest Defence of Opinion 2/13 on EU Accession to the ECHR, and the Way Forward.' (2015) 16(1) *German Law Journal* 106.

[261] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others*. Grand Chamber CJEU, 8 April 2014.

Section II: The European Union

European Union law on data privacy, and on the restrictions that may lawfully be imposed on the data privacy rights of citizens, is divisible into two categories, primary and secondary. Primary EU law is embodied in two treaties, namely the Lisbon Treaty on the European Union (TEU) [262] and the Treaty on the Functioning of the European Union (TFEU).[263] A third primary law instrument is the Charter of Fundamental Rights of the European Union (CFR), which became legally binding as primary law with the coming into force of the Lisbon Treaty on 1 December 2009.[264] In the treatment of the protection of personal data as an autonomous right, the CFR differs from other international human rights documents, which do not specifically mention a right to data protection, but tend to treat data protection as an extension of the right to privacy.[265] Post 2009, the CFR played a decisive role in the jurisprudence of the Court of Justice of the European Union (the CJEU). On 8 April 2014, the Grand Chamber, the highest Court of the CJEU, declared the Data Retention Directive (2006/24/EC) invalid, thus determining the data privacy/security balance in the context of data protection.

The Regulations, Directives and Decisions of the EU are commonly referred to as secondary EU law. In this category, the principal legal instrument on data protection is Directive 95/46/EC of the European Parliament and Council on the protection of individuals with regard to the processing of personal data, and on the free movement of such data.[266] This Directive is designed to give substance to the principle of the right to data privacy already enshrined in Convention 108 of the Council of Europe. Since all 15 Member States of the EC at the time were contracting parties to Convention 108, this obviated the possibility of contradictory provisions in the Convention and the EC Privacy Directive.

---

[262] OJ 2007, C-306(1).
[263] OJ 2010, C-83/47.
[264] See Article 6(1) of the TEU: 'The Union recognises the rights, freedoms and principles set out in the Charter of Fundamental Rights on 12 December 2007, which shall have the same legal values as the Treaties.'
[265] Data Protection in the European Union: the Role of Data Protection Authorities: Strengthening the Fundamental Rights Architecture in the EU.' European Union Agency for Fundamental Rights (2010). See also Maria Tzanou, 'Is Data Protection the Same as Privacy? 17(3) (2013) *Journal of Internet Law* 20, 25-6.
[266] OJL 281, 23 November 1995.

EU Directive 95/46/EC gives explicit recognition to data privacy as a fundamental right. However, in this as in other privacy rights instruments, whether Council of Europe or European Union, the right to data privacy is not absolute. Interferences with this right are legitimate under certain conditions. The conditions for the legal processing of personal data are set out in Article 7 of the Directive. This embodies a number of principles, such as the purpose specification principle: that the processing and use of data must be for specified, explicit and legitimate purposes, and the fairness principle: that all processing must be lawful and fair to the data subject. When one of the legitimate purposes is national security, the security/data privacy balancing exercise comes into play in cases coming before the Courts. The Court of Justice of the EU (CJEU) has jurisdiction to determine whether a Member State has fulfilled its obligations under Directive 95/46/EC, and to give preliminary rulings concerning the interpretation of the Directive in order to ensure its effective and uniform application in the Member States.

The Data Protection Directive, 95/46/EC, set up a Working Party on the Protection of individuals 'with regard to the Processing of Personal Data,' commonly referred to as the Article 29 Working Party.[267] The Working Party was composed of a representative of the supervisory authority designated by each Member State, and of a representative of the authority or authorities established for the European Community institutions and bodies and of representatives of the European Commission. The Working Party was given advisory status and the power to act independently. Its remit was to consider items placed on its agenda by its chairman, or at the request of a representative of the supervisory authorities of individual states or of the European Commission.

Other significant secondary instruments covering data protection which set out the conditions for balancing data privacy rights against competing rights and values are Directive 97/66/EC of the European Parliament and of the Council;[268] Regulation EC No. 45/2000 of the European Parliament and Council of 18 December 2000 on the protection of individuals with regard to

[267] The title derives from the fact that the Working Party was established under Article 29 of the Directive.
[268] Official Journal, L 024, 30 January 1998, 001-008.

the processing of personal data by the Community institutions and bodies, and on the free movement of data; Directive 2002/58/EC of July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. Provisions in the instruments mentioned above deal with the extent to which governments may retain personal data. Directive 97/66/EC dealt with the processing of personal data and the protection of privacy in the telecommunications sector. The Directive provides that:

> Traffic data relating to subscribers and users processed to establish calls and stored by the provider of a public telecommunications network and/or publicly available telecommunications service must be erased or made anonymous upon termination of the call.[269]

Directive 2002/58/EC stands apart from previous secondary EC instruments which had laid down the conditions under which a balance between data privacy rights and the demands of national security might be achieved. Article 15 of this Directive altered the balance between data privacy rights and the right of state authorities by restricting those rights in the interests of national security. To bring this change of balance about, the Council (the 15 Governments) and the Parliament repealed Directive 97/66/EC.[270] More importantly, Directive 2002/58/EC permitted Member States to pass laws requiring communications providers to retain data for a so-called, but unspecified, 'Limitation period.' This arrangement was implemented in Article 15 of the Directive, which gave directions for the amendment of certain provisions of Directive 95/46/EC. Article 15 acknowledges that States may adopt legislative measures to restrict the scope of privacy rights and obligations, 'where such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State Security).'

[269] Article 6(1) Official Journal, L 024, 30 January 1998, p. 001-008.
[270] Directive 2002/58/EC Of The European Parliament And Of The Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, 37), Article 19: 'Directive 97/66/EC is hereby repealed from the date referred to in Article 17(1).' viz. October 31, 2003).

This change to the privacy/security balance made by Directive 2002/58/EC was strongly opposed by the Article 29 Working Party.[271] The Chairman of the Working Party, Stefano Rodatà, wrote to the Parliament, the Commission and the Council, calling on them to resist the proposed limitations on privacy rights. The members of the working party were adamant that no changes should be made to existing provisions of Directive 95/46/EC guaranteeing confidentiality of communications (Article 5), or to provisions covering limited processing of traffic data (Article 6). Rodotà found it unacceptable that the scope of initial data processing should be widened in order to increase the amount of data available for furthering security and law enforcement objectives. In the light of what was to follow - a major data retention Directive- Rodatà made the prescient comment that changes made to Directive 95/46/EC such as these made in Article 15 of Directive 2002/58/EC, 'changes that are directly related to fundamental human rights, would turn the exception into a new rule.'[272] He foresaw a time when 'systematic and preventative storage of EU citizens' communications and related traffic data would undermine the fundamental right to privacy, data protection, freedom of expression, liberty and presumption of innocence,' as well as the end of a 'democratic' information society.[273] Rodatà also observed that:

> The Charter of Fundamental Rights of the European Union recognises all these fundamental rights and freedoms and requires that any limitations on the exercise thereof must respect the essence of those rights and freedoms. Moreover, the Charter takes a clear position on the tendency of protection for those rights that are also guaranteed by the European Convention on Human Rights as it states that Union law may provide more extensive protection. A lower level of protection would be legally and politically unacceptable.[274]

On 25 November, 2009, Directive 2002/58/EC was amended. The amendments gave rise to *inter alia*, an obligation that providers of electronic

[271] The letter sent by Stefano Rodotà Chairman of the Article 29 Working Party of June 7, 2001, when the proposal to introduce the Directive was being considered, is available at: <http://www.statewatch.org/news/2001/jun/07Rodota.pdf> accessed 3 September, 2016.
[272] ibid.
[273] ibid.
[274] ibid.

communications services or networks to notify data breaches to national data protection authorities and their customers,[275] and introduced more stringent rules dealing with the use of cookies.[276] The latter amendment aimed to afford Internet users more control over personal information.[277]

Legislation, whether in Europe or the U.S., to curtail privacy rights with a view to facilitating increased access by State security and law enforcement agencies to the telecommunications data of individuals tends to originate in the response of state authorities to outbreaks of terrorism in Europe, the U.S. and elsewhere. Both the terrorist events of 9/11 in the U.S.A. and subsequent similar events in Europe contributed to a change in the European legislative balance between data privacy and national security. The exposure of Europeans to significant external and internal threats led to a perception at EU governmental level that with the states comprising the European Union were under attack, civil liberties, such as data privacy, must be curtailed in the interest of national security, on the basis that 'national security was a condition precedent to securing civil liberties.'[278]

This widely shared perception led to the publication by the Council of the European Union of the Hague Programme for 'Strengthening Freedom, Security and Justice in the European Union', [279] a key objective of which was to counteract the threat of terrorism. This was followed by the promulgation by the European Parliament and Council of the First European Data Retention Directive, 2006/24/EC, which amended Directive 2002/58/EC. This new Directive provided for the retention of data generated or processed in connection with the retention of data generated or processed in connection with the provision of publicly available electronic communications networks. It altered the existing balance between privacy and security by providing for a significant additional degree of interference with individuals' data privacy. While it did not permit the acquisition of knowledge of the content of

[275] Article 4(3) Directive 2002/58/EC, as amended by Article 18 Directive 2009/136/EC.
[276] Article 5(3) Directive 2002/58/EC, as amended by Article 18 Directive 2009/136/EC.
[277] Quinten R. Kroes, *E-Business Law of the European Union* (2nd edn, Wolters Lkuwer, Netherlands, 2010) 13-14.
[278] Robert N. Davis, 'Striking the Balance: National Security vs. Civil Liberties' 29(1) (2004) *Brooklyn Journal of International Law* 175, 176.
[279] 2005/C53/01.

electronic communications, it did permit the retention of an extensive range of metadata.[280]

As Ojanen points out: 'A lot of information, including sensitive information, about an individual can easily be revealed by monitoring the use of communications services through traffic data collection, storage and processing.'[281] Hence, in a modern network environment, from the point of view of privacy protection, the distinction between the content of electronic communications and the metadata associated with these is relatively insignificant. Those who had come to regard the protection of the right to privacy as a fundamental principle in the European Union and an essential element of its legitimacy saw the new privacy/security balance as a betrayal of this fundamental principle. McGarvey, for example, argued that the retention Directive had 'called the legitimacy of the European Union into disrepute as it has ignored the oldest and most important human rights in favour of surveillance and the petitions of law enforcement agencies.'[282] Maras remarks that the Directive 'was passed with indecent haste.'[283]

One area of European life has remained untouched by the EU data protection law. This is intelligence-gathering by national spy agencies and intelligence services generally. The applicability of the EU legal instruments enshrining rights to privacy and data protection, including Articles 7 and 8 of the Charter of Fundamental Rights of the European Union, the Data Protection Directive 95/46/EC and the e-Privacy Directive 2002/58/EC, is subject to the specific legal and policy framework relating to the field of security and particularly to the national security exception. Article 4(2) of the TEU provides that 'national security remains the sole responsibility of each EU member state.' This exemption from EU law is reiterated in Article 3(2) of Data Protection

[280] Directive 2006/24/EC, Article 13.
[281] Tuomas Ojanen, 'Privacy as more than a seven-letter word: the Court of Justice of the European Union sets Constitutional limits on Mass Surveillance' 10(3) (2014) *European Constitutional Law Review* 528, 537.
[282] Stephen McGarvey, 'The 2006 EC Data Retention Directive: A Systemic Failure' 10(1) (2011) *Hibernian Law Journal* 119, 136.
[283] Marie-Helen Maras, 'While the European Union was Sleeping, the Data Retention Directive was passed: The Political Consequences of Mandatory Retention' 6(2) (2011) *Hamburg Review of Social Sciences* 1,5. See also Simone Blakeney, 'The Data Retention Directive: Combating Terrorism or Invading Privacy?' 13(5) (2007) *Computer And Telecommunications Law Review* 153, 157.

Directive 95/46/EC which excludes from the scope of the Directive the processing of personal data concerning public security, defence and criminal law activities, and in Article 1(4) of Framework Decision 2008/977/HA which excludes 'essential national security interests and specific activities in the field of national security' from the rules applicable to 'regular' law enforcement action. The distinction here is between the national security and the 'regular' law enforcement functions of the intelligence services. A recent report by the European Agency for Fundamental rights points out that

> The lack of clarity on the precise scope of the national security exemption goes hand-in-hand with the varied and seldom clearly drawn line between the areas of law enforcement and national security in Member States. This is particularly true with counter-terrorism, since terrorism is generally considered a threat to both national security and to law and order.[284]

However, when EU law does not apply, other international legal instruments do, for example, the ECHR and Convention 108, by virtue of the acceptance by EU Member States of the ECHR. It is also the case that the CJEU refers to Member States' international obligations under the ECHR when a subject-matter is outside the scope of EU law.[285] In this context, the ECtHR has recently reiterated its condemnation of any indiscriminate spying activities.[286]

1.0 The European Union and Human Rights Protection in the Context of the data privacy/national security balance

The main EU secondary legislative instrument regulating the processing of personal data is the Data Protection Directive 95/46/EC, which has been described as 'a milestone towards the emergence of data protection as a fundamental right of citizens in the EU.' [287] Before 1995, provisions on data protection were largely left to national initiatives. For example, the German

[284] Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU. Mapping Member States' legal frameworks. FRA - European Union Agency For Fundamental Rights (Austria, 2015), 10.
[285] Case C-127/08 - *Metock and Ors v Minister for Justice, Equality and Law Reform*, 25 July 2008, paras 74-79.
[286] *Zakharov v Russia* Application no. 47143/06 (2015), at para 348.
[287] See Gonzales Fuster, Gloria and Raphael Gellert, 'The Fundamental Right of data protection in the European Union: in search of an uncharted right' 26(1) (2012) *Review of Law, Computers and Technology* 73-82.

State of Hessen adopted a data protection Act in 1970, followed by Sweden in 1973, on a Federal German basis in 1977 and in France in 1978.[288] The way was paved for a European framework on data protection by the Council of Europe Convention 108 for the protection of individuals with regard to automatic processing of personal data of 1981. Convention 108 was the first legally-binding international instrument in the area of data protection, as well as being a direct influence on the key principles of Directive 95/46/EC. In Article 5, it fixes criteria for making data processing legitimate: data undergoing automated processing must be obtained fairly and lawfully, they must be stored for specified and legitimate purposes, they must be relevant and not excessive in relation to the purposes for which they are stored and must be preserved in a form which permits identification of the data subjects for no longer than is required for the purposes for which they are stored. The continuity between the data protection provisions of Convention 108 and those of Directive 95/46/EC is suggested by the inclusion in the Directive of a similar set of criteria to be satisfied if automated data processing is to be deemed legitimate: the consent of a data subject must be given freely, with no doubt prevailing as to whether consent was given or not;[289] the processing must be necessary for the performance of a contract to which the data subject is party,[290] in order to protect the data subject's vital interests, for the performance of a task carried out in the public interest [291] or in the exercise of official authority, or for the purposes of the legitimate interests pursued by the data controller, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection, and of privacy in particular.[292]

The data subject's right to access to personal data 'without constraints at reasonable intervals and without excessive delay or expense,' is enshrined in Article 12 of the Directive, as is the right to have the data rectified, erased or blocked, particularly if these data are incomplete or inaccurate. These rights were already provided for in Article 8 of Convention 108. The right to access

[288] Herwig C.H. Hofmann, Gerard C. Rowe and Alexander H. Türk, *Administrative Law And Policy Of The European Union* (Oxford University Press, 2011) 480, fn 384.
[289] Data Protection Directive 95/46/EC Article 7(a).
[290] ibid, 7 (b).
[291] ibid, 7 (e).
[292] ibid,7 (f). Article 7 of the Directive 95/46/EC enunciates these principles, while Article 6 reiterates the principles enunciated in Article 5 of Convention 108.

to personal data was also emphasised by the CJEU in the case of *College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer* [293] where the CJEU held that a 'data subject may be certain that his personal data are processed in a correct and lawful manner,' and that 'the basic data regarding him are accurate and that they are disclosed to authorised recipients.'[294] However, Directive 95/46/EC outlines special circumstances in which access rights of data subjects may be restricted or limited. Article 13 of the Directive entitles Member States of the EU to enforce such restrictions when interests such as national security, defence, public security and the prevention, investigation, detention and prosecution of criminal offences are at stake. In the case of *Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert and Others* [295] the CJEU stressed that Member States should not invoke Article 13 of the Directive for the sole purpose of derogating from the Directive itself, and that the derogating measures listed in Article 13 should be adopted only when they are necessary. As the Court expressed it, the latter requirement 'is thus a precondition for the option granted to the States by Article 13(1), and does not mean that they are *required* to adopt the exceptions at issue in all cases where that condition [necessity] is satisfied.'[296] Furthermore, the onus is on the Member State to prove that the exceptions they might have introduced were necessary.[297]

The development of EU fundamental rights law has been influenced by the expansion of anti-terrorism law in the first decade of the 21st century, which has involved the EU in actions involving human rights issues taken before the CJEU. In taking over competence previously exercised by its Member States the EU has been subject to United Nations Security Resolutions under Chapter VII of the U.N. Charter.[298] The case of *Kadi* [299] finally determined by the CJEU, illustrated two aspects of the Court's judicial activism. The first was its

[293] Case C-553/07, 7 May 2009.
[294] ibid, at para 49.
[295] Case C-473/12, 7 November 2013.
[296] ibid, at para 32.
[297] ibid. Article 13(1) of the Directive indicates that Member States 'may adopt the derogating measures listed in Article 13 of the Directive, not that they *must* do so.
[298] For a detailed analysis of the activities of the EU in this regard see Sionaigh Douglas-Scott, 'Fundamental Rights in the EU: The Ambiguity of Judicial Review,' 268-296 in Tom Campbell, K.D., Ewing and Adam Tomkins (eds), *The Legal Protection of Human Rights: Sceptical Essays* (Oxford University Press, 2011).
[299] Joined Cases C-402 and C-415/05 - *P.Kadi and Al Barkakaat International Foundation v Council and Commission* [2008], 1-6351.

willingness to affirm its commitment to fundamental rights as the Court of a Community (the EU) the core values of whose legal order are commitment to the rule of law and respect for fundamental rights. The second was its affirmation of the autonomy of the EU legal order. Kadi was one of a number of those who had been listed as terrorists in a U.N. Security Council resolution and had their assets frozen. The EU took measures to implement the U.N. Resolution. Kadi, claiming that he had never been involved in terrorist activities, claimed that the measures taken by the EU had violated his fundamental rights to his property. Finding that he could not appeal his case to the U.N. Sanctions Committee, he approached the CJEU, which agreed to hear his case. The Court found that Kadi's rights had been violated. Asserting its competency to hear Kadi's case, the CJEU proclaimed the constitutional autonomy and hegemony of the EU legal order:

> It is also to be recalled that an international agreement cannot affect the allocation of powers fixed by the Treaties or, consequently, the autonomy of the Community legal system, observance of which is ensured by the Court by virtue of the exclusive jurisdiction conferred on it by Article 220 EC, jurisdiction that the Court has, moreover, already held to form part of the very foundations of the Community…[300]

The CJEU held that the obligations of an international agreement could not override the constitutional principles of the EU Treaty, and that it was thus empowered to review the EU measure to implement the U.N. Resolution under EU human rights standards. The Court additionally found it pertinent that Kadi's right to proper judicial process had been violated by the failure to communicate to him the reason for his listing as a terrorist, had been deprived of discovering why they were subject to an assets freeze and were prevented from making their views known in relation to it.

The various instruments of secondary EU law - mainly the Directives dealing with data privacy rights, may be regarded as landmarks in a process in which the data privacy/national security balance is tilted in one direction or another, sometimes favouring the data privacy interest, sometimes the national security

[300] ibid, at para 282.

one. Directive 95/46/EC is an example of the former, Directive 2002/58/EC, which provides for interference with data privacy for an unidentified 'limited period,'[301] tends in the other direction, while Data Retention Directive 2006/24/EC, the most controversial and contested of EU secondary law measures, represents a radical shift in the balance in favour of national security. This latter Directive, and its significant consequences for Member States' privacy-protection regimes and for the development of EU jurisprudence in radical new directions, will be considered in detail later in this chapter.

2.0 The Growing Involvement of the EU in Human Rights Protection, particularly in data protection and the circumstances influencing this.

Evidence continues to accumulate that the EU and its institutions are becoming increasingly involved in human rights protection in general and in data protection in particular, to the extent that one commentator believes that the EU 'has the capacity to turn into an unprecedented post-national human rights protection institution.' [302] To account for this phenomenon, it is necessary to consider a number of related developments involving EU primary law and the new, pro-active role of the CJEU in the defence of privacy rights. There was a time when the ECJ, the predecessor of the CJEU had, as its remit, the handling of the practical legalities of business and governmental issues, including economic integration. The predecessor of the EU was originally an economic treaty with the purpose of creating a Common Market. This treaty contained no provision on human rights. The claim in Article 2 of the Treaty of the European Union (TEU) that the EU is 'founded on respect for human rights is not in accord with the evidence that human rights were not a significant concern of the earliest manifestation of the European Union, the EEC.[303] The work of dealing with the human and civil rights, including data privacy, provided for in the ECHR, devolved on the European Court of Human Rights (ECtHR). It is arguable that, by the end of the twentieth century, economic integration was no longer seen as a means to the end of further integration in

[301] Article 15 (1).
[302] Samantha Besson. 'The European Union and Human Rights: Towards A Post-National Human Rights Institution' 6(2) (2006) *Human Rights Law Review* 323.
[303] See Stijn Smismans, 'The European Union's Fundamental Rights Myth' (2010) 48 (1) *Journal of Common Market Studies* 45. See also Sionaidh Douglas-Scott, 'The European Union's Fundamental Rights Myth' Journal of Common Market on and Human Rights after the Treaty of Lisbon' 11(4) (2011) *Human Rights Law Review* 64, 647-8.

the EU and that an alternative unifying principle was needed.[304] Fortuitously, by 2000, human rights had emerged as a major element of institutional activity and constitutional construction in Europe.[305] The growing tendency to place human rights issues at the core of the EU integration project was powerfully reinforced by the adoption of the Charter of Fundamental Rights of the European Union, and further with the coming into force of the Lisbon Treaty in 2009, with the Charter of Fundamental Rights becoming a legally-binding instrument of EU primary law. In turn, this placed human and civil rights issues, such as data privacy, under the remit of the CJEU. Since 2009, the CJEU, the superior judicial mechanism in the EU, adjudicates claims under the Charter and has, between 2014 and 2016, delivered some groundbreaking decisions with profound consequences for data privacy rights and for the data privacy/national security balance. The CJEU demonstrated its willingness to take a strong stand in relation to human rights in decisions which have direct and binding effect on EU Member States, and cannot be appealed. These decisions will be examined later in this chapter.

The substantial increase in the human rights competence of the EU[306] especially since 2009, when, its own legally binding Charter of Fundamental Rights became a powerful agency for the enforcement of human rights, including the right to data privacy, under the exclusive remit of a Court of Justice, the CJEU, which was disposed to enforce these rights to the extent made possible by the Charter, has heralded the prospect of a corresponding decline in ECHR and ECtHR jurisdiction. One contributory factor in this regard is the subsumption in the EU Charter of Fundamental Rights of significant elements in the human rights provisions of the ECHR including the human rights ones. Another is the recognition by the ECtHR of the growing competence of the EU in the field of

[304] See Armin Bogdany, 'The EU as a Human Rights Organisation? - Human Rights and the Core of the European Union' 37(6) (2000) *Common Market Law Review* 1307-1338, 1337.
[305] Samantha Besson. 'The European Union and Human Rights: Towards A Post-National Human Rights Institution' 6(2) (2006) *Human Rights Law Review* 323, 324. See also Koen Lenaertes, 'Fundamental Rights in the European Union' 25(6) (2000) *European Law Review* 575.
[306] In Case C-34/09, Zambrano, Advocate-General Sharpton called for 'a seamless protection of fundamental rights under EU law in all areas of exclusive or shared competence….' at para 170.

human rights, citing CJEU jurisprudence in its judgments,[307] coupled with the growing reluctance of the CJEU to cite ECtHR jurisprudence or ECHR principles in its judgments and to cite the EU Charter instead. Since the passage of the Lisbon Treaty, EU law may, where possible, as Douglas-Scott observes, present advantages to human rights litigants over actions in Strasbourg because, '[u]nlike under the ECtHR, where the applicant must exhaust all domestic remedies in order to get a hearing in Strasbourg, applicants may get a ruling from [the CJEU in] Luxembourg, by way of a preliminary reference from a domestic Court.'[308] There is the further consideration that domestic courts have the power to set aside national measures which conflict with EU human rights law, which provides a much faster remedy than a Strasbourg lawsuit before the ECtHR.[309]

3.0 Data Retention Directive 2006/24/EC and the Alteration of the Data Privacy/National Security Balance

In the aftermath of 9/11, some EU States introduced exceptions to EU data protection rules. Among these exceptions was a requirement that Internet and telephone service providers retain metadata relating to electronic communications and make them available to law enforcement agencies if required. [310] The consequence of these State responses to terrorist threats was a heterogeneous series of derogations from existing data protection provisions: different rules in different states on the retention of data by electronic communications providers. According to Article 1 of the Data Retention Directive,[311] it was adopted with the purpose of harmonising these diverse

[307] *See Scoppolla v Italy* (No 2) Application No 10249/03, Merits, 17 September 2009, where the ECtHR cited Cases C-391/02 and C-403/02 Berlusconi and Others [2005] ECR 1-3565, which were cited as authority for the proposition for the retroactive application of the more lenient penalty under Article 7 of the ECHR.

[308] Sionaidh Douglas-Scott, 'The European Union and Human Rights after the Treaty of Lisbon' 11(4) (2011) *Human Rights Law Review* 645, 657.

[309] ibid.

[310] For example, the Irish Criminal Justice (Terrorist Offences) Act, 2005, Section 64, required telecommunications providers to retain traffic data for a period of three years for the purpose of preventing crime and safeguarding the security of the State.

[311] Directive 2006/24/EC Of The European Parliament And Of The Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC O.J. (L 105/54).

national laws.[312] It is worthy of note that unlike Section 64 of the Irish Criminal Justice Act, which cites both 'preventing crime' and 'safeguarding the Security of the State' as the twin purposes of the requirement for retaining data traffic, Article 1 of Directive 2006/24/EC mentions only one purpose; 'the investigation, detection and prosecution of serious crime.'

While the principal aim of the Directive was to promote cooperation on law enforcement by improving the information to the police, it also had, as Bignami has pointed out, '[b]y standardizing the data retention requirements imposed by police authorities on electronic communications providers, it would be easier for providers to do business in multiple jurisdictions.'[313] Recital 6 of the Directive draws attention to the fact that the variation in the national provisions for data retention tend to jeopardise the smooth and efficient functioning of the internal EU market for electronic communications, since, as the Recital explains, 'the legal and technical differences between national [data retention] provisions……. present obstacles to the internal market for electronic communications, since service providers are faced with different requirements regarding the types of traffic and location data to be retained and the conditions and periods of retention.' These are the official justifications for the new EU regime of data retention.

However, other factors were involved in the decision at the highest levels of EU governance to introduce a Directive inaugurating a new phase in the balance between EU privacy rights and the right of state authorities to derogate from these in the interest of security. Since the introduction of Directive 2002/58/EC, communications providers in Europe have been legally obliged to erase traffic data as soon as such data are not useful for billing purposes.[314] In the aftermath of widespread terrorist attacks in Europe, law enforcement agencies believed that information derived from telecommunications traffic

[312] Article 1 makes it clear that '[t]he Directive aims to harmonize the Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.'
[313] Francesca Bignami, 'Protecting Privacy Against the Police in the European Union: The Data Retention Directive,' (2007) 8(1) *Chicago International Law Review* 233, 239.
[314] Directive 2002/58/EC, Article 6.

data was a necessary component in the fight against terrorism, and that a legal measure such as Directive 2006/24/EC should be introduced to amend Directive 2002/58/EC by making traffic data available to national law enforcement agencies and their counterparts in other Member States. The London bombings of July 7, 2005 [315] proved decisive in creating a unified approach among EU Member States towards arriving at developing a response to terrorist attacks. The EU Commission and Council adopted the 'Declaration on the European Union Response to the London Bombings.' [316] This Declaration contained a number of provisions for combating terrorism. One of these was that agreement had to be reached regarding a decision on the retention of Telecommunications data.[317] The Directive was finally approved at its first reading by the European parliament and was finally approved by the Council of Ministers on February 21 2006. Maras contends that it 'was passed with indecent haste.' [318] It appears unlikely that the Directive would have been adopted so quickly had the United Kingdom not assumed the Presidency of the EU on 30 June 2005, a week before the London bombings. This afforded the British Prime Minister Tony Blair the opportunity and the motivation to expedite a more rapid discussion of data retention mechanisms of the EU Commission, the Council of Ministers and Parliament meetings.[319]

4.0 Features of Directive 2006/24/EC

The most important provisions of the Directive are set out in considerable detail in Article 5, which require Member States to adopt legislation imposing an obligation on Internet and telephone companies to store and retain the metadata relating to the source, address, date, time, length and type of communication.[320] However, the content of the communication was not to be retained or stored.[321] Although the original impulse behind the Directive was

[315] Hugh Muir and Rosie Cowan, 'Four bombs in 50 minutes - Britain suffers its worst ever terror attack,' *The Guardian* 8 July 2005.
[316] Council of the European Union, (13 July 2005) Justice and Home Affairs Press Release 11116/05, (Presse 187), 1 <https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/85703.pdf> accessed 23 October 2016.
[317] ibid, 6.
[318] Marie-Helen Maras, 'While the European Union was Sleeping, the Data Retention Directive was passed: The Political Consequences of Mandatory Retention' 6(2) (2011) *Hamburg Review of Social Sciences* 1,5.
[319] Matthew Tempest, 'Clarke tells MEPs to back EU anti-terror measures' *The Guardian*, 7 September 2005. Charles Clarke was British Home Secretary at this time.
[320] Directive 2006/24/EC, Article 5(1).
[321] ibid, Article 5(2).

the harmonisation of diverse national laws on data retention,[322] Article 6 of the Directive states that retention must last for a period of not less than six months and not more than two years, a provision which perpetuates a regime of diversity rather than harmonisation and in spite of the fact that the general formula of Article 1 of the Directive opens with the claim that:

> This Directive aims to harmonize the Member States' provisions concerning the obligations of the providers of publicly available electronic communications services or of public communications networks with respect to the retention of certain data which are generated or processed by them in order to ensure that the data are available for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.[323]

Yet, as the general formula of Article 1 indicates, Member States are afforded discretion in defining the conditions that justify access to the retained data: 'the data are available for the purpose of the investigation, detection and prosecution of serious crime as defined by each Member State in its national law.'[324] This formulation seems to indicate another digression from the ideal of harmonising Member States' provisions and a regression to the greater diversity that the Directive aimed to remedy. Article 4 of the Directive requires that Member States regulate access to retained metadata in accordance with necessity and proportionality requirements and consistent with EU law and ECHR law as interpreted by the ECtHR.

5.0 Responses to Data Retention Directive 2006/24/EC

1. The Response of Member States

Between its adoption in 2006 and its review by the CJEU in 2014, the Directive gave rise to major concerns among EU Member States regarding its compatibility with existing fundamental rights provisions: in particular data privacy rights protected under both ECHR and EU primary and secondary law. Since 2008, many of the highest national constitutional courts across the EU have upheld challenges striking down national provisions implementing the

[322] See Article 1, Data Retention Directive.
[323] Directive 2006/24/EC, Article 1(1).
[324] Article 1 Directive 2006/24/EC.

Directive. These Constitutional Courts, including the Bulgarian Supreme Administrative Court (2008), the Romanian Supreme Court (2009), the German Constitutional Court (2010) Czech Constitutional Court (2011), Slovakia (2014) and Slovenia (2014), have declared unconstitutional specific provisions of national laws transposing the Directive. The grounds on which these judgments were based related to 'the surveillance regimes' inadequate oversight and security standards and overall incompatibility with the legality, necessity and proportionality requirements under Article 8 of the ECHR.[325]

The Bulgarian Supreme Administrative Court found that the provision of Article 5 of the Data Retention Directive violated the right to privacy as safeguarded in Article 3(2) of the Bulgarian Constitution and Article 8 ECHR, as it did not provide the necessary safeguards against the violation of citizens' constitutional rights and did not specify any conditions on which interference with the right to private life and personal data of citizens would be allowed.

Romania

The Romanian Constitutional Court [326] was asked to consider whether the Romanian data retention legislation in relation to the rights to freedom of movement,[327] family and private life,[328] the secrecy of correspondence [329] and freedom of expression, [330] all guaranteed by the Romanian Constitution. In arriving at its verdict, the Constitutional Court was critical of Article 20 of the Romanian data retention law (Law 298/2008), which referred to 'the prevention and counteracting the threats to national security.' The Court held that the term 'threats to national security,' was too expansive and was not defined by the legislation. [331] In addition, the Court emphasised its concerns with the phrase 'related data necessary for the identification of the subscriber or registered user,' as in common with all provisions of the retention law, captured all those who were users of electronic communications. [332] The Court noted that for the Romanian

[325] Nora Ní Loideáin, 'EU Law and Mass Internet Surveillance in the post-Snowden Era' 3(2) (2015) *Media and Communication Data* 53,56.
[326] Decision of the Romanian Constitutional Court 1258, 08 October 2009. English translation by Bogdan Manolea and Anca Argesiu <http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf> accessed 19 September 2016.
[327] Article 25 Romanian Constitution.
[328] Article 26 Romanian Constitution.
[329] Article 28 Romanian Constitution.
[330] Article 30 Romanian Constitution.
[331] Romanian Constitutional Court, decision 1259, 08 October 2009.
[332] ibid.

data retention law to be compliant with both the Romanian Constitution and ECtHR jurisprudence, it must be both 'foreseeable' and 'accessible'.[333] The Court also found that the government's attempt to justify the mandatory retention of telecommunications data by invoking undefined threats to 'national security' was unlawful.[334] The Court also referred to ECtHR jurisprudence in its verdict, most notably the 1978 ECtHR ruling in *Klass v Federal Republic of Germany*, [335] which stated that 'taking surveillance measures without adequate and sufficient safeguards' can lead to 'destroying democracy on the ground of defending it.'[336]

Significantly, the Romanian Constitutional Court ruled that the domestic data retention legislation served to reserve the presumption that only limited forms of interference can be applied in relation to the rights to privacy and freedom of expression - which is not possible when the domestic legislation complained of targets all electronic communications.[337] Moreover, the Court was critical of the blanket nature of the data retention mandated by the legislation at issue and could not find any justification for it. Significantly, The Constitutional Court also criticised the retention legislation because it mandated that data pertaining to the recipients of electronic communications be retained, a measure, which, in the Court's view served to place a recipient of electronic communications under suspicion on the basis of the actions of another party.[338]

It is instructive to note that throughout the Romanian Constitutional Court's judgment, there is little mention made of EU law, aside from initially emphasising that EU Directives 'are binding as to the result to be achieved.[339]

---

[333] ibid. The Court cited the ECtHR cases of *Sunday Times v United K*ingdom [1979-80] 2 EHRR 245 and *Rotaru v Romania*, Application No. 28341/95 (4 May 2000), in relation to the legal principle of foreseeability.

[334] Romanian Constitutional Court, decision 1259, 08 October 2009.

[335] This case centred on a challenge to amendments made in 1968 to Article 10 of the West German Basic Law which permitted the Federal Government to engage in the surveillance of telecommunications and mails without recourse to prior judicial approval in circumstances where it was deemed that national security interests were being threatened.

[336] *Klass and Others v Federal Republic of Germany* (1979-80) 2 E.H.R.R. 214, 232 at para 49.

[337] Romanian Constitutional Court, decision 1259, 08 October 2009.

[338] ibid.

[339] Cian C. Murphy, "Note on Romanian Constitutional Court, Decision No. 1258 of 8 October 2009 regarding the unconstitutionality exception of the provisions of Law No. 298/2008 regarding the retention of the data generated or processed by the public electronic communications service providers or public network providers, as well as for the modification of Law No. 506/2004 regarding the personal data processing and protection of private life in the field of electronic communication area" 47 (2010) *Common Market Law Review* 933, 935.

Additionally, no mention is made of the Data Retention Directive in the judgment,[340] with a brief reference to the e-Privacy Directive, being the only mention of EU legislation throughout the Court's judgment.[341]

The European Commission threatened to bring full infringement proceedings against Romania before the CJEU for its failure to transpose Directive 2006/24/EC.[342] In the wake of the Commission's initiation of proceedings and having revoked domestic Law 298/2008, the Romanian Parliament, not wishing to involve Romania engaging in litigation before the CJEU, passed a new law (Law 82/2012) which transposed Directive 2006/24/EC.[343] The 2012 legislation was subjected to a similar challenge regarding its constitutionality, with the Romanian Constitutional Court finding that the transposing legislation was invalid.[344] In arriving at its verdict in 2014, the Court was guided by the principles laid down by the CJEU in *Digital Rights Ireland* [345] and further held that the 2012 transposing legislation at issue contained similar constitutional defects which were deemed to apply in the Court's 2009 ruling, giving rise to similar unconstitutionality.[346] The 2009 ruling noted that the 2008 legislation had exceeded justified and proportionate restraints of privacy rights, failed to uphold secrecy attaching to correspondence and freedom of expression and diminished the presumption of innocence principle.[347]

The Romanian Constitutional Court cited the verdicts of the Bulgarian, German and Czech Constitutional Courts, relating to legal principles

[340] ibid.
[341] ibid, fn 16.
[342] The European Commission initiated proceedings against Romania for failing to implement the Data Retention Directive by letter C (2011) 4111 of 16 June 2011, in the case 2011/2089 and was given to months to do so.
[343] See Simona Şandru, 'About Data Protection And Data Retention In Romania' 7(2) (2013) *Masaryk University Journal of Law and Technology* 379, 391.
[344] Viorica Vița, 'The Romanian Constitutional Court and the Principle of Primacy: 1 To Refer or Not to Refer?' 16(6) (2015) *German Law Journal* 1623,1651.
[345] Joined Cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others*. Grand Chamber CJEU, 8 April 2014.
[346] Viorica Vița, 'The Romanian Constitutional Court and the Principle of Primacy: 1 To Refer or Not to Refer?' 16(6) (2015) *German Law Journal* 1623, 1651. See also CCR, Decision 440/2014, published in Official Monitor No 653 of 4 September 2014, http://www.ccr.ro/files/products/Decizie_440_2014_reviz.pdf, cited in Simona Şandru, 'About Data Protection And Data Retention In Romania' 7(2) (2013) *Masaryk University Journal of Law and Technology* 379-399.
[347] Viorica Vița, 'The Romanian Constitutional Court and the Principle of Primacy: 1 To Refer or Not to Refer?' 16(6) (2015) *German Law Journal* 1623, 1648.

concerning data retention.[348] In this regard, there was a notable confluence of approach among the three Courts regarding the question of data retention.[349] The verdict of Romania's Constitutional Court (the CCR) is notable from a variety of perspectives. In its 2009 verdict, the CCR refers extensively to the Data Retention Directive, but does so indirectly and without undertaking an analysis of it.[350] The CCR, with reference to the *Digital Rights Ireland* judgment, in tandem with its 2009 verdict, declared the 2012 Law to be unconstitutional.[351] The 2014 verdict is notable for acknowledging EU law as the overarching source of domestic Romanian law, yet refers to the EU Charter of Fundamental Rights on two occasions, and only when citing the CJEU verdict in *Digital Rights Ireland*.[352] Most significantly, the CCR makes a distinction between, on the one hand, the Data Retention Directive and the EU Charter of Fundamental Rights as resting firmly within the ambit of EU law, and on the other hand, distinguishing these from domestic Romania law. This 'separation position' is deemed by Vița to 'be too rigid, at least in so far as the Charter is involved.' [353]

Germany

In Germany, after legislation transposing the Data Retention Directive into the German Telecommunication Act and Code of Criminal Procedure was passed by the Bundestag, and entered into force in 2008, 34,000 German citizens filed a complaint against the legislation at the Federal Constitutional Court.[354] In 2010, the Court ruled that the transposing provisions constituted a disproportionate interference with Article 10 (confidentiality of communications) of the Basic Law,[355] and contravened legal standards on purpose limitation, data security, transparency and legal remedies.[356] By this time, the EU Commission had initiated infringement proceedings against Germany, and took its case to the CJEU in 2012. The Commission sought to

[348] ibid, 1651.
[349] ibid.
[350] ibid, 1652.
[351] ibid.
[352] ibid.
[353] ibid.
[354] Anna-Bettina Kaiser, 'Case Comment: German data retention provisions unconstitutional in their present form; decision of 2 March 2010, NJW, p. 833' (2010) 6(3) *European Constitutional Law Review* 503.
[355] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Mar. 2, 2010, 1 BvR 256/08.
[356] Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Mar. 2, 2010, 1 BvR 256/08, § 269 et seq.

impose a daily fine of €315,036.54.[357] As an immediate consequence of the CJEU verdict in *Digital Rights Ireland*,[358] the European Commission ceased proceedings against Germany and other Member States which had failed to transpose the Data Retention Directive in conformity with the required times limits.[359] The proceedings taken by the EU Commission against Germany were withdrawn, aside from the costs attaching thereto, as a result of a decision by the President of the CJEU given on 5 June 2014.[360]

Czech Republic

In March 2011, the Czech Republic's Constitutional Court declared national legislation implementing the Directive unconstitutional. It found that the retention period exceeded the requirements of the Directive and that the use of the data was not restricted to cases of serious crime and terrorism. The Court held that the national legislation lacked 'clear and detailed rules for the protection of personal data, as well as the obligation to inform the person whose data had been requested.' On the other hand, it noted that there was nothing in principle preventing implementation of the Directive, provided this was done in conformity with constitutional law, a point which had also been made by the German Federal Constitutional Court.

Slovakia

On 23 April 2014, the Slovak Constitutional Court suspended the effectiveness of the Slovak implementation of the Data Retention Directive. The Constitutional Court emphasised that although blanket data retention does not involve the retention of the content of communications, it gives rise to revealing personal characteristics, habits and relationships of those affected.[361] It further held data retention amounts to a serious interference because of its privacy invasive aspect. The Court noted that the blanket collection of data affects 'a great an unpredictable number of people' as it is intended to act as a

[357] Action brought on 11 July 2012 - *European Commission v Federal Republic of Germany* (Case C-329/12).
[358] Joined Cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others*. Grand Chamber CJEU, 8 April 2014.
[359] Franziska Boehm and Mark D. Cole, 'Data Retention after the Judgment of the Court of Justice of the European Union' (The Greens/European Free Alliance, 2014), 41.
[360] ibid, fn 155.
[361] Case Number PL. US 10/2014 at § 106. Cited in Martin Husovec, 'Slovak Constitutional Court Annuls National Data Retention Provisions' (2015) 1 *European Data Protection Law Review* 227-229.

preventative measure and is not confined by geographical borders.[362] Significantly, the Court held that while the right to privacy is not an absolute one, [363] the legitimate aim of upholding public security cannot by virtue of its importance, justify an interference with privacy.[364] In this regard, it was held that while upholding public security and fighting serious crime often necessitate the use of modern technologies, the application of such needs to be restricted to what would be 'strictly necessary.'[365]

Preliminary suspension of effectiveness means that the Retention laws are still formally valid, but have no legal effect until the Court decides on the merits of a complaint initiated by the European Information Society Institute with the support of thirty Members of the Slovak Parliament. Pending the Constitutional Court decision, providers of electronic communications will be free of any legal obligation to store data about users.[366] Any storage of the metadata of users will need to be limited to the general régime of Directive 2002/58/EC and Directive 95/46/EC. At the same time, any collected data will need to be destroyed.[367]

Slovenia

On July 3rd, 2014 the Slovenian Constitutional Court struck down Articles 162-169 of the Act on Electronic Communications, which regulates data retention and were adopted in order to implement the Data Retention Directive. The decision of the Court is significant because of the alignment of the Slovenian Constitutional Court with the pan-European judicial response to the Data Retention Directive. After the Grand Chamber of the CJEU declared the Data Retention Directive invalid *ab initio* on April 8, 2014 the Slovenian Constitutional Court made its decision on the relevant Article of the domestic legislation. It ordered the operators to destroy all information held on the basis of the annulled provisions immediately after the publication of the Constitutional Court decision. In its main decision, the Constitutional Court

[362] ibid, at **§** 107.
[363] ibid, at § 109.
[364] ibid, at § 114.
[365] ibid, at **§** 119.
[366] Martin Husovec, 'First European Constitutional Court Suspends Data Retention After The Decision Of The Court Of Justice Of The EU,' *The Centre for Internet and Society* 28 April 2014 <http://cyberlaw.stanford.edu/blog/2014/04/first-european-constitutional-court-suspends-data-retention-after-decision-court> accessed 17 September 2016.
[367] ibid.

found that with the annulment of the Data Retention Directive, the obligation of the Member State to transpose it into the domestic legal order had ceased. The readiness of the Constitutional Court to stay proceedings and wait for the decision of the CJEU indicates the relevance of EU law and Court of Justice case law for the Constitutional Court.

United Kingdom

The Data Retention Directive was transposed into UK law by the Data Retention (EC Directive) Regulations 2009. In the aftermath of the invalidation of the Data Retention Directive by the CJEU in *Digital Rights Ireland*,[368] a scheme of emergency legislation providing for Internet and telecommunications data retention was devised and promulgated by way of the Data Retention and Investigatory Powers Act 2014,[369] which provided for a series of retention mechanisms, with a twelve-month maximum time-limit. In July 2015, the provisions of the Act were deemed incompatible with EU Law by the UK High Court, which also held that the Act was silent regarding any rules which might govern the access to and use of communications data and further highlighted the absence of judicial oversight to assess whether access to such communications data was necessary.[370] An appeal against this decision was lodged by the Home Secretary. The Court of Appeal was minded to give favourable consideration to the UK Government's argument that mandatory retention of communications data, which must be captured by domestic legislation, did not follow from the decision in *Digital Rights Ireland* [371] but notwithstanding this, the Court of Appeal opted to refer a question to the CJEU for a preliminary ruling.[372] The CJEU held that its provisions were incompatible with *inter alia*, Articles 7, 8 and 11 of the EU Charter of Fundamental Rights.[373]

[368] Joined Cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others*. Grand Chamber CJEU, 8 April 2014.
[369] Henceforth cited as DRIPA.
[370] *R (Davis) v Home Secretary* [2015] EWHC 2092.
[371] Joined Cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others*. Grand Chamber CJEU, 8 April 2014.
[372] *Secretary of State for the Home Department v R (Davis)* [2015] EWCA Civ 1185, [2015] All ER (D) 196 (Nov).
[373] Case C-203/15 *Tele 2 Severige and Watson* (Grand Chamber) 21 December, 2016. This case will be dealt with in more detail in Section 18.0 Conclusion.

In 2016, the Investigatory Powers Act was introduced which provided for a variety of provisions including the introduction of some new powers in addition to the redefinition of existing powers enabling UK intelligence and law agencies to conduct targeted interception of communications, the bulk of communications data and the bulk interception of communications. The Investigatory Powers Act was colloquially referred to as 'The Snoopers' Charter' due to concerns among privacy advocates and civil liberties organisations. In the aftermath of the Act's promulgation, Edward Snowden commented that the Investigatory Powers Act represents 'the most extreme surveillance in the history of western democracy. it goes further than many autocracies.' [374]

Ireland

Telecommunications Data Retention in Ireland was governed by the Postal and Telecommunications Services Act 1983, which provided for the retention of telecommunications traffic data for three years, to facilitate access to such data by An Garda Síochána and the Defence Forces.[375] The Act provided for the retention of telecom traffic data for three years.[376] While the 'interception' of communications was prohibited by the Act, it was defined narrowly and deemed to constitute 'listening to or recording' but ruled out 'metering.'[377]

Although Ireland had not transposed the Telecommunications Privacy Directive [378] until May 2002, telephone traffic and mobile phone location data were being retained by Irish telecom providers over a six year period prior to this, and being made available to An Garda Síochána.[379] An intervention by the Irish Data Protection Commissioner reduced the length of retention of the data in question to a period of no longer than six months, but a secret direction by the Minister for Public Enterprise, under Section 110(1) of the Postal and

[374] Ewen MacAskill, "Extreme surveillance" becomes UK law with barely a whimper' *The Guardian* (19 November 2016).
[375] Sections 98 (2A) and 98 (2B) of the Postal and Telecommunications Services Act 1983,as inserted by Section13 of the Interception of Postal Packets and Telecommunications Messages (regulation) Act 1993.
[376] Section 110 (1) Postal and Telecommunications Services Act 1983.
[377] ibid, Section 98.
[378] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.
[379] T.J. McIntyre, 'Data retention in Ireland: Privacy, Policy and proportionality' *Computer Law and Security Report* 24 (2008) 326, 328.

Telecommunications Services Act, 1983, obliged telecom providers to retain all traffic data and mobile phone location data for three years.[380]

While debates took place regarding the proportionality of a scheme of data retention involving a three year retention period, world events, particularly bombings in New York in September 2001 and in Madrid in March 2004 prompted greater emphasis on security considerations. This culminated in the passage of the Criminal Justice (Terrorist Offences) Act, 2005. Part 7 of the Act provided for the retention of telecommunications traffic data and location data for three years, such data to be made available with a view to preventing, detecting, investigating and prosecuting crimes[381] and the safeguarding of State security.[382] The 2005 Act was promulgated notwithstanding 'the existence, transposition and supposed operation'[383] of the e-Privacy Directive,[384] with particular reference to Article 15 which enshrined that traffic data should only be retained under stringent conditions, for law enforcement purposes, for a limited period and only when necessary, appropriate and proportionate in a democratic society.

The bombing of London in July 2005 focused attention on the terrorist threat in the digital age and on what would be needed in the form of a legislative response. In March 2006, the EU Data Retention Directive was promulgated.[385] This aimed to harmonise retention periods and ensure an EU-wide approach towards retained Internet and telecommunications traffic data. Ireland, with support from Slovakia, initiated a challenge to the Directive pursuant to Article 230 before the CJEU [386] on the basis that it had been incorrectly adopted.[387] However, as the challenge was merely a procedural one, it did not allow for a

[380] ibid. In this regard, McIntyre contends that the secret direction was issued by the Minister 'to sidestep' the direction of the Data Protection Commissioner, who held that the previous retention scheme in operation prior to the Ministerial direction did not comport with the provisions of the Data Protection Act, 1988 and the Telecommunications Privacy Directive 97/66/EC.
[381] The Criminal Justice (Terrorist Offences) Act, 2005, Section 63. This included, but was not limited to terrorist offences.
[382] ibid.
[383] Ronan Lupton, 'Communications (Retention of Data) Act 2011 (No 3 of 2011) 16(4) (2011) *Bar Review* 85, 86.
[384] Directive 2002/58/EC.
[385] 2006/24/EC. This is dealt with in detail in Chapter 1, Section 3.0.
[386] *Ireland v Council of the European Union and European Parliament* Case C-301/06, 2006 OJ/C 237/5.
[387] T.J. McIntyre, 'Data retention in Ireland: Privacy, Policy and proportionality' *Computer Law and Security Report* 24 (2008) 326, 333.

challenge the retention of data *per se*, only the basis upon which the Directive was promulgated.[388]

Subsequently, the privacy rights group in the form of Digital Rights Ireland Limited, instituted High Court proceedings[389] which challenged the provisions of The Criminal Justice (Terrorist Offences) Act, 2005, in addition to the provisions of the Data Retention Directive. The Plaintiff Company was granted standing by McKechnie J, who referred the questions raised to the CJEU, which ultimately annulled the Data Retention Directive.[390] While the Communications (Retention of Data) Act, 2011 remains part of Irish law, its provisions are likely to be challenged on the basis of the annulment of the Data Retention Directive by the CJEU. An individual convicted of murder is commencing proceedings to seek to overturn his conviction, which will be heard in February 2018. The basis of the appeal is that the Communications (Retention of Data Act, 2011), the Irish transposition of the expunged Data Retention Directive, no longer enjoys legitimacy, owing to the annulment of the Data Retention Directive.[391] In that case, much of the evidence upon which the appellant was convicted, involved the use of telecommunications traffic data.[392]

The cases mentioned above are from countries with Constitutional Courts possessing powers of abstract constitutional review, and all of the Constitutional Courts annulled the national laws implementing the Data Retention Directive. Other Member States, including France, Ireland, the United Kingdom and Sweden took an opposite point of view. In the course of negotiations on a Data Retention Directive the Governments of those countries had submitted a joint proposal for a retention measure which would require communications service providers to retain, for a minimum of 12 months and a

[388] ibid. The challenge was unsuccessful.
[389] *Digital Rights Ireland Limited v Minister for Communications and Others* [2010] IEHC 221.
[390] This is dealt with in Section 8.0 'The Ruling of the CJEU.'
[391] (----------) 'Dwyer's challenge to use of phone records to be heard next year' *RTE.ie* (15 June, 2017) <https://www.rte.ie/news/2017/0615/883049-graham-dwyer/> accessed 18 June 2017.
[392] ibid.

maximum of 36 months, all communications data generated by communications service providers within the EU.[393]

Even after the CJEU had annulled the Data Retention Directive in April 2014, the Dutch Government announced in November 2014 that it would keep data retention laws with only minor modifications. However, in March 2015, the District Court of The Hague ruled that the domestic data retention law violated the rights protected by Article 7 and 8 of the EU Charter of Fundamental Rights and was not limited to retention which was absolutely necessary. On those grounds, the Court annulled the Dutch data retention law.[394]

By contrast, immediately after the *Digital Rights Ireland* judgment,[395] some major Swedish telecommunications providers announced that they had stopped retention and deleted all the retained data.[396] However, the oversight authority, the Swedish Post and Telecom Authority (PTS) changed its policy, requiring some providers to resume retention, [397] after the government had come to the conclusion that the Swedish law meets the strict requirements set out in the *Digital Rights Ireland* judgment. This decision was challenged by Tele 2, a national telecoms operator. In April 2015, a Swedish Court of Appeals referred Swedish data retention once again to the CJEU, to test the compatibility of Swedish retention legislation with the e-Privacy Directive (2002/58/EC) in particular.[398] It is significant that when the validity of the Data Retention Directive was successfully challenged before the CJEU in joined Cases C-293/12 and C-494/12, Spain, France, Italy, Poland and the United Kingdom intervened in the case in support of the Directive, along with the European

[393] Judith Rauhofer, 'Just Because You're Paranoid, doesn't mean they're not after you: Legislative developments in relation to the mandatory retention of communications data in the European Union' 3(4) (2006) *Script-ed*, 323,333.
[394] Decision of the District Court of the Hague, Case Number C/09/480009/KG ZA, 14/1575, 11 March 2015.
[395] Joined Cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others*. Grand Chamber CJEU, 8 April 2014.
[396] Liam Tung, 'Four of Sweden's telecos stop storing customer data after EU retention directive' (11 April, 2014) *ZDNet* <http://www.zdnet.com/article/four-of-swedens-telcos-stop-storing-customer-data-after-eu-retention-directive-overthrown/> accessed 25 November 2016.
[397] Niklas Vainio and Samuli Miettinen, 'Telecommunications data retention after *Digital Rights* Ireland: legislative and judicial reactions in the Member States 23 (2015) *International Journal of Law and Information Technology* 290, 303-04.
[398] ibid, 304.

Parliament, Council and Commission, while the Irish Human Rights Commission and Portugal opposed it.[399]

6.0 Institutional Responses to Directive 2006/24/EC

(a) Response of Peter Hustinx

Peter Hustinx, the European Data Protection Supervisor [400] provided a comprehensive evaluation of the Directive in which he drew attention to the many problems associated with its application. This evaluation is based on the overall premise that the Directive fails to meet its main purpose, 'to harmonise national legislation concerning data retention.'[401] The Hustinx opinion draws particular attention to the consequences of non-harmonisation of retention periods:

> The lack of a fixed single retention period for all Member States has created a variety of diverging national laws which may trigger complications because it is not always evident what national law - on data retention as well as on data protection - is applicable when operators store data in a Member State other than the one in which the data are collected.[402]

In addition, the noted lack of harmonisation is considered detrimental and unhelpful to the various parties and stakeholders involved, namely citizens and business operators in addition to law enforcement authorities.[403] Hustinx contends that the Data Retention Directive 'does not meet the requirements imposed by the rights to privacy and data protection,' further noting that 'the

[399] Elspeth Guild and Sergio Carrera, 'The Political and Judicial Life of Metadata:Digital Rights Ireland and the Trail of the Data Retention Directive' 65 (2014) *CEPS Paper in Liberty and Security in Europe*, 1,5.

[400] Article 41(1) of EC Regulation 45/2001 (Chapter V - on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data) provided for the appointment of an independent supervisory authority known as the European Data Protection Supervisor, which, under Article 42(2) of the Regulation is responsible for monitoring and ensuring that the fundamental rights and freedoms of natural persons throughout the EU regarding the processing of personal data are respected in relation to the processing of personal data, with particular emphasis placed on privacy rights.

[401] Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC), 7, para 35 <www.edps.europa.eu/.../Opinions/2011/11-05-30_Evaluation_Report…> accessed 25 September, 2015.

[402] ibid, 12, para 61.

[403] ibid.

necessity of data retention as provided by the Data Retention Directive has not been sufficiently demonstrated,' and that data retention mechanisms 'could have been regulated in a less privacy-invasive manner.' [404] The opinion considers the issue of data security, noting the conclusions of the Article 29 Working Party in its thirteenth annual report of July 2010, which held that a variety of security measures had been put in place in Member States and that in terms of general principles, when Directives pertinent to data retention, privacy and protection are implemented

> [T]he authorities and courts of Member States must not only interpret their national law in a manner consistent with those directives, but also make sure that they do not rely on an interpretation of them which would be in conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality.[405]

Hustinx also contends that by virtue of the expansive provision relating to 'competent national authorities' retained data have been utilised 'for far too wide a range of purposes and by far too many authorities.' [406] The lack of consistency attaching to the Directive is also highlighted, particularly in relation to 'safeguards and conditions for access to the data.' [407] It is noted that 'access is not made subject to prior approval by a judicial or other independent authority in all Member States.' [408] The opinion is particularly mindful of the issue of foreseeability, noting that '[I]t cannot be said that the Data Retention Directive itself, read in particular in conjunction with the e-Privacy Directive, provides the clarity needed to fulfil the principle of foreseeability at EU level.'[409]

(b) EU Commission Evaluation Report (2011)

In its evaluation of the Data Retention Directive, the EU Commission acknowledged that it has not been implemented in a harmonised fashion across Member States, noting the myriad of retention periods for the retention of

[404] ibid, para 36.
[405] 'Thirteenth Annual Report of the Article 29 Working Party on Data Protection.' European Justice Commission, 109. (14 July 2010) <ec.europa.eu/.../article-29/.../annual-report/.../13th_annual_report_en…> accessed 26 November 2014.
[406] ibid, 11, para 59.
[407] ibid.
[408] ibid.
[409] ibid, 14, para 73.

telecommunications traffic data.[410] It was suggested that in addition to bringing about the harmonisation of retention periods, a reduction in data retention periods should be considered. [411]

The absence of an EU-wide definition of serious crime was highlighted as a cause for concern, particularly as some Members States did not make provision for a domestic definition.[412] The report called for an examination of the legal relationship between the Data Retention Directive and the e-Privacy Directive, with particular emphasis on Article 15 of the latter.[413] In this regard, it was noted that the overall objective should be to promote legal certainty regarding the provisions of both Directives.[414] The question of which public bodies and authorities may have access to retained traffic data was highlighted and initiatives aimed at reducing the numbers having access were recommended in tandem with providing guarantees in relation to independent supervision relating to traffic data access requests. Additionally, the report considered the possibility of narrowing the categories of traffic data to be retained.[415]

The Evaluation Report focused on providing guidance in relation to the use of retained traffic and in particular, how to ensure that retained data should not

[410] European Commission, (2011) Report from the Commission to the Council and the European Parliament. Evaluation Report on the Data Retention Directive (Directive 2006/24/EC) COM 225 final, at 14.
[411] ibid, 32.
[412] ibid, 6.
[413] Article 15 of the e-Privacy Directive permits Member States to place restrictions on privacy rights and obligations 'when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defense, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communication system.' With the promulgation of the Data Retention Directive, Article 11 was inserted into Article 15 of the e-privacy Directive: 'Paragraph 1 shall not apply to data specifically required by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks to be retained for the purposes referred to in Article 1(1) of that Directive.' The CJEU in its verdict of 21 December, 2016, in joined Cases C-203/15 and C-698/15 *Tele 2 and Watson* held that the e-Privacy Directive aimed to give rise to high levels of data protection and privacy. It held that Article 15(1) of the e-Privacy Directive, when read in conjunction with the EU Charter of Fundamental Rights, prohibited domestic legislation for exceeding the requirement that exceptions to this must not become the norm. It further held that instances where measures were taken which departed from the privacy and data protective nature of the Directive to achieve national security objectives, such departures must be strictly necessary and adhere to the 'strictly proportionate' requirement as enshrined in Recital 11 of the e-Privacy Directive. See inter alia, para 95 of joined Cases C-203/15 and C-698/15 *Tele 2 and Watson.*
[414] ibid, 4.
[415] ibid, 12.

become part of any data mining objectives.[416] The Report acknowledged the paucity of statistical analysis from some Member States in relation to individual 'requests' for data.' [417] It was noted that statistics provided by Member States 'differed in scope and detail,'[418] with some Member States distinguishing between the various types of communications, with some giving details of the age of the data at the time a request was made.[419] However, some Member States submitted annual statistical returns devoid of 'any detailed breakdown.'[420]

(c) Leaked Commission Consultation Paper

The leaked opinion from the EU Commission to the Working Party on Data Protection and Exchange of Information provides a candid assessment of problems associated with the framework and the implementation of Directive 2006/24/EC.[421] Significantly, the Commission notes that following consultation among 'all interested groups,'[422] a perception exists 'that there is little evidence at an EU and national level,' regarding the value of data retention 'in terms of public security and criminal justice.'[423] It also pointed out that uncertainty exists as to 'whether data requested would be available anyway,' in default of data retention obligations.[424] The Commission highlighted the lack of separation between stored and accessed data in respect of business purposes, serious crime purposes and for purposes other than fighting serious crime.[425]

---

[416] ibid, 32. Alexander provides a concise summary of what data mining entails. Data mining, or knowledge discovery, is the computer-assisted process of digging through and analyzing enormous sets of data and then extracting the meaning of the data. Data mining tools predict behaviours and future trends, allowing businesses to make proactive, knowledge-driven decisions. Data mining tools can answer business questions that traditionally were too time consuming to resolve. They scour databases for hidden patterns, finding predictive information that experts may miss because it lies outside their expectations. Data mining derives its name from the similarities between searching for valuable information in a large database and mining a mountain for a vein of valuable ore. Both processes require either sifting through an immense amount of material, or intelligently probing it to find where the value resides. See Doug Alexander, 'Data Mining.' <http://www.laits.utexas.edu/~norman/BUS.FOR/course.mat/Alex/> Accessed 20 July 2013.

[417] European Commission, (2011) Report from the Commission to the Council and the European Parliament. Evaluation Report on the Data Retention Directive (Directive 2006/24/EC) COM 225 final,19.

[418] ibid.

[419] ibid.

[420] ibid.

[421] The leaked opinion, 'Consultation on reform of Data Retention Directive: emerging themes and next steps,' <http://quintessenz.org/doqs/000100011699/2011_12_15,Eu_Commission_data_retention_reform.pdf> accessed 20 May 2013.

[422] ibid, 2.

[423] ibid, 3.

[424] ibid.

[425] ibid.

It was noted that at present 'no monitoring system' exists which allows EU citizens to discern that data would otherwise be unavailable to agencies of law enforcement with data retention obligations and what impact the use of data had in relation to 'investigations and prosecutions.'[426] The consultation paper highlighted difficulties encountered by law enforcement agencies, regarding 'unclear definitions in the DRD' [Data Retention Directive], and noted that:

> [I]nstant messaging, chat uploads and downloads (but not anonymous SIM cards) are types of data held by information society services which is almost identical to traffic data but which is outside the scope of the DRD.[427]

In the absence of a harmonised EU-wide approach to accessing such data, law enforcement agencies experience difficulties when trying to obtain 'this data on time for their investigations.'[428] The lack of a definition of 'serious crime' in the Directive and in Member States is highlighted as a serious concern, but in this regard, it is noted by the Commission that a statement made by the Council in relation to the adoption of Directive 2006/24/EC advises Member States to 'have due regard to the crimes listed in…….the European Arrest Warrant….and crime involving telecommunication.' [429] With regard to what might be in keeping with the concept of serious crime, the paper notes that crimes such as hacking might not be deemed to be serious in nature, 'but can only be tackled through telecoms data.' [430] It was further noted that Directive 2006/24/EC 'does not cover urgent cases for protection of life and limb not related to crime,' examples including instances of suicide, self-harm, missing persons and emergencies.[431]

The paper outlines concerns of NGOs and data protection authorities,[432] particularly from the perspective of 'the purposes for which data may be

[426] ibid.
[427] ibid.
[428] ibid.
[429] Joint Statement by the Council and the Commission in relation to Article 12 (Evaluation) of the Draft Directive, 5777/06 ADDI February 10, 2006.
[430] The leaked opinion, 'Consultation on reform of Data Retention Directive: emerging themes and next steps,' is Available at <http://quintessenz.org/doqs/000100011699/2011_12_15, Eu_Commission_data_retention_reform.pdf> accessed 20 May 2013, 4.
[431] ibid.
[432] ibid. The NGOs and data protection authorities are not specifically referred to.

retained.' [433] In some Member States, the requirement to retain data is not restricted to any specific objective or purpose. The example of the ECJ decision in *Promusicae v Telefonica* which *inter alia* enshrined that Directive 2006/24/EC does not prevent personal data being admitted by way of evidence in civil proceedings, in the instant case relating to copyright infringements.[434] The paper commented on initiatives to formally extend the scope of the Directive to include detection and investigation of copyright infringement, piracy and illegal downloading.[435]

(d) Other Responses

In their critique of the Data Retention Directive, immediately following the CJEU decision annulling it, Guild and Carrera focus on the fact that the kind of data retention provided for in the Directive involved the collection of bulk metadata, which meant that 'everyone's data had to be collected without the requirement of any suspicion or the intercession of a judge.'[436] They also point out that while the Preamble to the Directive refers to law enforcement authorities in three places and declares that the Directive is compliant with the ECHR, the text of Article 4 of the Directive permits Member States to allow access to data retained by whatever competent law enforcement agency they choose, with the consequence that there is no necessary monopoly of criminal justice authorities over access to data. Guild and Carrera find it difficult to escape the conclusion that 'the retention of data is arbitrary and access to it is unlimited. In the wake of the CJEU decision of April 8, 2014 they suggested that the majority of the EU institutions participating in the drafting of the Directive seems to have been 'asleep on the job when it came to protecting EU citizens' privacy while addressing the pressures emerging from the Madrid and London bombings.' [437] They concluded that only the European Data Protection Supervisor (EDPS) 'comes out of this affair looking good, as that office had consistently warned that the Directive was not compliant with the EU

[433] ibid.
[434] *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU* (C-275/06) Unreported January 29, 2008 (ECJ).
[435] The leaked opinion, 'Consultation on reform of Data Retention Directive: emerging themes and next steps,' is Available at <http://quintessenz.org/doqs/000100011699/2011_12_15, Eu_Commission_data_retention_reform.pdf> accessed 20 May 2013, 4.
[436] Elspeth Guild and Sergio Carrera, 'The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive' 65 (2014) *CEPS Paper in Liberty and Security in Europe*, 2.
[437] ibid, 5.

Charter,'[438] which was also a key element in the CJEU invalidation of the Directive.

In addition to the Data Protection Supervisor, Guild and Carrera might also have given honourable mention to the Article 29 Data Protection Working Party, which had taken part in the negotiations leading to the adoption of the Data Retention Directive, but had also warned both beforehand and after the passage of the Data Retention Directive, about its consequences for fundamental rights. In its Opinion, the Working Party raised issues which anticipated the findings of the CJEU in 2014. Among the points it made were that 'traffic data retention [i.e. metadata retention] interferes with the inviolable, fundamental right to confidential communications,' and that '[p]roviders of publicly available communication services would be forced unprecedentedly to store billions of data relating to the communications of any and all citizens for investigational purposes,'[439] and that imposing the said data retention obligations on communication service providers without having first realised adequate, specific safeguards is not to be accepted within the existing European legal framework.' [440] In its March 2006 Opinion following the passage of the Directive, the Working Party noted that the Directive 'lacks some adequate and specific safeguards as to the treatment of communications data and leaves room for diverging interpretation and implementation by the Member States in this respect.'[441] It is also noted that such safeguards 'are necessary to protect the vital interests of the individual as mentioned by Directive 2002/58/EC, in particular the right to confidentiality when using publicly available electronic communications services.'[442]

[438] ibid. The warning is contained in: 'Evaluation shows that the Data Retention Directive does not meet privacy and data protection requirements, says EDPS' European Data Protection Supervisor, Press Release, EPDS/11/6, Brussels, 31 May, 2011 <http://europa.eu/rapid/press-release_EDPS-11-6_en.htm> accessed 13 September 2016.

[439] Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005), Article 29 Working Party, 1868/05/EN WP 113, Adopted on 21st October 2005, 1, 2. <http://ec.europa.eu/justice/dataprotection/article29/documentation/opinion recommendation/files/2005/wp113_en.pdf> accessed 21 September 2016.

[440] ibid.

[441] Article 29 Data Protection Working Party, 'Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC,' 654/06/EN WP 119, 1, 2.

[442] ibid.

Although Recital 9 of the Data Retention Direction describes it as 'an instrument of data retention that complies with the requirements of Article 8 of the ECHR [and] is therefore a necessary measure,' human rights and data privacy advocates argue that contrary to this contention in Recital 9, the mandatory retention of all types of metadata is not in conformity with Article 8 ECHR, and the right to privacy is not recognised by the Directive.[443] In order to conform to this Article, any interference with the right to private life is not legitimate unless it conforms to the three criteria set down in Article 8(2) ECHR: (a) there must be a legal basis; (b) there must be a need for the measure in a democratic society and (c) it must conform to one of the legitimate aims listed in the ECHR. Criterion (b) has been interpreted by the ECtHR as meaning that there must be a 'pressing social need.' [444] When the Working Party published its Opinion on the mandatory retention of all types of data and the conformity of this with the ECHR, it found that this provision would not meet the 'democratic society requirement' of Article 8 since, '[n]ot everything that might prove to be useful for law enforcement is desirable or can be considered as a necessary measure in a democratic society,' [445] and that the proposal to retain all categories of metadata was not backed by any 'persuasive arguments that retention of traffic data to such a large-scale extent is the only feasible option for combating crime or protecting national security.' [446]

From the perspective of the data privacy/national security balance, although the Directive made it clear that it relates not to the content of communications but to the metadata associated with these, it still represents a significant shift in the balance between the privacy of the individual and the right of the State to protect its national security. Davis and Trigg observe that:

---

[443] See Simone Blakeney, 'The Data Retention Directive: combating terrorism or invading privacy?' 5(13) (2007) *Computer and Telecommunications Law Review* 153,155.

[444] *Klass v Federal Republic of Germany* of 18 November 1977, European Court of Human Rights, Series A No 28.

[445] Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism. Proposal presented by France, Ireland, Sweden and Great Britain (Document of the Council 8958/04 of 28 April 2004)], Article 29 Data Protection Working Party, 11885/04/EN WP 99, Adopted on 9th November 2004, 1, 4. <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion recommendation/files/2004/wp99_en.pdf> accessed 23 September 2016.

[446] ibid.

> With the Directive requiring ISPs and Telecos to retain location and traffic data for a period of six months up to a maximum of two years, and Member States' "law enforcement authorities" able to obtain such retained data without undue delay, civil liberties, such as privacy, seem to have taken a back seat to national security.[447]

The Directive is an illustration of what happens when governments are faced with threats to the security of their states. In these cases, human rights groups campaigners represent themselves as strict protectors of human rights, while governments, faced with a security crisis, have a more permissive attitude to the restriction of privacy and other fundamental rights. As Vainio and Mieltinen observe, 'the Courts take seriously the idea that restrictions of rights must be limited to what is strictly necessary even when restrictions are [legally] justified by reference to security, while the governments seem to view legal safeguards as a technicality that must be implemented but in a way that least interferes with the policy objective of security.[448]

The arguments brought forward by human rights advocates opposed to the Data Retention Directive are analogous at many points to those advanced by the Article 29 Working Party and the EU Data Protection Commissioner. Taken together, these constitute a convincing body of evidence that the Data Retention Directive fails to satisfy the requirements set out in Article 8 of the ECHR. These arguments give additional reinforcement to the reasoning of the CJEU in finding that the Data Retention Directive entailed a wide-ranging interference with the right to respect for private life and communications guarantee by Articles 7 and 8 of the EU Charter of Fundamental Rights.

Among the arguments presented by those who invoke Article 8 of the ECHR as the basis for finding the Directive unacceptable are that metadata will be stored in respect of everyone, regardless of identity; that the retained data can be accessed without a court order, and will therefore be subject to misappropriation and abuse; that law enforcement authorities may access

[447] Gareth Davies Gayle Trigg, 'Being data retentive: a knee jerk reaction? *Communications Law* 11(1) (2006) 18.
[448] Niklas Vainio and Samuli Miettinen, 'Telecommunications data retention after *Digital Rights Ireland:* legislative and judicial reactions in the Member States' 23(3) (2015) *International Journal* 290, 308.

metadata without the knowledge of the data subject; the Directive does not indicate who is entitled to have access to data; there is no specific indication of the purpose or purposes for which the data may be used; the Directive does not define serious crime, and leaves it to Member States to define this in their national laws, leaving the way open for disparate definitions to emerge among Member States and consequent inconsistencies in the application of the Directive. There is also the consideration that the metadata surveillance facilitated by the Directive differs little in its practical effects on privacy rights than would the collection, processing and access to content data by unspecified state agencies not permitted by the Directive. In the 21st century, as Ní Loideáin points out, 'the depth and breadth of information concerning an individual's private life that can now be revealed through the metadata surveillance of communications have advanced in tandem with dramatic technological developments', resulting in the availability of 'very detailed information regarding an individual's beliefs, preferences and behaviour'.[449]

For the reasons outlined above, Digital Rights Ireland, an Irish civil rights lobby group, sought inter alia, but principally, an order pursuant to Article 267 TEFU seeking to have a number of questions adjudicated upon by the CJEU by way of preliminary reference.[450] The Irish High Court, per McKechnie J granted the Applicants' request that the reference be made to the CJEU.[451]

7.0 Judgment of the CJEU (Grand Chamber) on the Validity of Directive 2006/24/EC

In 2012, the CJEU was asked to rule on the validity of the EU Data Retention Directive, upon referral by the Irish High Court and the Austrian Constitutional Court, the standard procedure for challenging EU legislation being to commence proceedings before state courts. When the validity or the

[449] Nora Ní Loideáin, 'EU Law and Mass Internet Surveillance in the post-Snowden Era' 3(2) (2015) *Media and Communication Data* 53, 54.

[450] *Digital Rights Ireland Limited v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of An Garda Síochána, Ireland and the Attorney General and the Human Rights Commission* (notice party) [2011] 1 I.L.R.M. 258 at 265, para 14. The questions being referred were: 'Whether Directive 2006/24/EC is valid notwithstanding: a) Article 6 (1) and (2) of the Treaty on European Union ("TEU"); b) Article 3a TEU and 21 TFEU (formerly arts 10 and 18 TEC) ; c) Articles 7, 8, 11 and 41 of the CFR a) Article 6(1) and (2) of the Treaty on European Union ("TEU")) Article 3a TEU and 21 TFEU (formerly arts 10 and 18 TEC) ; (c) Articles 7, 8, 11 and 41 of the CFR and d) Article 5 TEU (formerly art.5 TEC) (the principle of proportionality).

[451] ibid, 300, at para 113.

interpretation of an EU measure is in question, state courts have an obligation, under Article 267 TFEU, to refer the matter to the CJEU. Individual applicants, on behalf of Digital Right Ireland, had complained before the Irish High Court and an Austrian provincial government (Carinthia) and individual applicants before the Austrian Constitutional Court, that the Data Retention Directive violated fundamental principles of privacy and data protection. Because these cases involved issues of EU law, the Irish High Court and the Austrian Constitutional Court requested the highest EU Court, the CJEU to examine the validity of Directive 2006/24/EC. Because both the Irish and Austrian cases dealt with similar issues, the CJEU decided to treat them as joined cases.[452]

On December 12, 2013, the Advocate-General (AG), Cruz-Villalón, an independent legal Counsel to the CJEU, advised on how the case might be decided. The AG examined, as a first step, the proportionality of the Data Retention Directive in terms of the overall appropriateness of the means it deployed to achieve its stated objectives, and secondly, its compatibility with the EU Charter of Fundamental Rights, in particular, the Charter's proportionality clause contained in Article 52(1) CFR.[453] The AG emphasised the 'functional duality' of the Data Retention Directive as both an internal market harmonisation directive and an instrument imposing data collection and retention for law enforcement purposes.[454] In the AG's view, this second aspect, collection and retention for law enforcement purposes, demanded a corresponding responsibility on the part of EU legislators to adopt effective guarantees to protect fundamental rights.[455] The AG referred to ECtHR case law [456] which treated the mere storing by a public authority of data relating to the private life of an individual as an interference with Article 8 ECHR (respect for private life). He considered the Directive's interference with the right to privacy of EU citizens as 'particularly serious'[457] because of the length and scale

[452] Joined Cases C-293/12 and C-594/12.
[453] Article 52 of the Charter of Fundamental Rights reads: Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.
[454] AG's Opinion, para 46.
[455] ibid, paras 117 and 128.
[456] *Amann v Switzerland*, Application No. 27798/95, 16 February 2000.
[457] AG's Opinion at para 70.

of data collection, the mapping and profiling potentials of metadata and the risk of unlawful use of the data.[458]

Examining the Directive's compatibility with the EU Charter of Fundamental Rights, the Advocate-General applied traditional human rights reasoning set out in Article 52(1) of the Charter, the Advocate-General considered whether the interference was provided by law, respected the essence of the right to privacy and was proportionate, i.e. that the interference was necessary, and that it genuinely met legitimate objectives of general interest, or the rights of others.[459] On the 'quality of law' element, he found the behaviour of the EU legislator who drafted the Directive 'irresponsible,' holding that '[t]he EU legislature [could] not when adopting an act imposing obligations which constitute serious interference with the fundamental rights of citizens of the Union entirely leave the Member States the task of defining the guarantees capable of justifying that interference…….it must fully assume its share of responsibility.' [460] The Advocate-General went further when he held that the fact that many Member States had provided suitable safeguards against abuse could not absolve the EU legislature from its responsibility to secure guarantees against abuse 'at least in the form of principles,' finding that this deficiency would already justify the annulment of the Directive.[461] The Advocate-General expressed scepticism about the 'indiscriminate and long' data retention periods which he deemed unnecessary in the absence of 'exceptional circumstances.' [462] While proposing that the Court declare the Directive invalid, the Advocate-General recommended a limitation on the temporal effect of the ruling, on the ground that this kind of compromise was appropriate because most Member States had offered appropriate guarantees against abuse and imposed moderate retention periods. This compromise was not found acceptable by the CJEU.

8.0 The Ruling of the CJEU

The CJEU began its analysis, not by reference to the primary provisions of the ECHR, as the Advocate-General had done, but by considering how Articles 7,

[458] ibid, at paras 71-76.
[459] ibid, at para 107.
[460] ibid, at para 120.
[461] ibid, at para 131.
[462] ibid, at para 151.

8 and 11 of the EU Charter were relevant to the question of the validity of the Data Retention Directive. This analysis began with an outline of what the Directive required: the collection and storage of metadata produced in the course of electronic communications. The Court observed that the collection of metadata:

> [T]aken as a whole, may allow very precise conclusions to be drawn concerning the private lives of the persons whose data have been retained, such as the habits of everyday life, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them.[463]

From this, the Court deduced that the retention of the data in question could impact on freedom of expression, guaranteed by Article 11 of the EU Charter.'[464] At the same time, the Court considered that the measure 'directly and specifically affected the right to private life guaranteed in Article 7 of the EU Charter of Fundamental Rights and the Protection of personal data, guaranteed by Article 8 of the same Charter, in the case of the latter because it constitutes the processing of personal data.[465]

Having established that Articles 7,8 and 11 of the EU Charter of Fundamental Rights had a bearing on the case, the Court focused on the possible violation by the Directive of the right to privacy and data protection.[466] At this point it adopted an approach similar to the one followed by the ECtHR in cases

[463] Joined Cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others*. Grand Chamber CJEU, 8 April 2014, at para 27.
[464] ibid, at para 28. Article 11 of the EU Charter of Fundamental Rights declares that: 'Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.'
[465] ibid, at para 29. Article 8(1) of the Charter reads: Everyone has the right to the protection of personal data concerning him or her; Article 8(2) reads: 'Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified' and Article 8(3) reads: 'Compliance with these rules shall be subject to control by an independent authority.'
[466] In the light of its finding that the Directive was in violation of Articles 7 and 8 of the Charter, the Court did not in the end consider it necessary to rule whether it was also in violation of Article 11.

involving interferences with fundamental rights guaranteed in Article 8 of the ECHR. It first raised the question whether the Data Retention Directive constituted an interference with Articles 7 and 8 of the EU Charter of Fundamental Rights, and also whether such interference was justified. The CJEU disposed of the first question by holding that the obligation imposed by Articles 3 and 6 of the Data Retention Directive to retain metadata 'constitutes in itself an interference with the rights guaranteed by Article 7 of the Charter.'[467] It also ruled that the fact that national authorities could access metadata constituted 'a further interference with that fundamental right.' [468] It further held that the Directive was in violation Article 8 of the EU Charter of Fundamental Rights,[469] making the general point that the interference resulting from the Directive was 'wide-ranging' and 'particularly serious.' [470] It emphasised the point that the retention and subsequent use of metadata without the subscriber or registered user being informed 'is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance.' [471]

On the second question, whether the interference with the rights guaranteed by Articles 7 and 8 of the EU Charter of Fundamental rights was justified, the CJEU held that the Data Retention Directive pursued a legitimate 'objective of general interest' : 'the fight against serious crime' and the 'fight against international terrorism in order to maintain international peace and security.'[472] The CJEU qualified this holding by ruling that the Data Retention Directive interfered with the right to privacy in a disproportionate way. It employed the multi-tier proportionality analysis developed in its case law and characteristic of the case law of the ECtHR to verify the proportionality of measures restricting fundamental rights. The CJEU found that the Data Retention Directive satisfied the requirements of the first tier of the proportionality analysis, the suitability test, because it was appropriate to the objective of providing national authorities with 'opportunities to shed light on serious

[467] Joined Cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others*. Grand Chamber CJEU, 8 April 2014, at para 35.
[468] ibid, at para 35.
[469] ibid, at para 36.
[470] ibid, at para 37.
[471] ibid.
[472] ibid, at para 42.

crime.'[473] However, the CJEU found that the Data Retentive Directive failed the necessity test, the second tier of the proportionality analysis. The CJEU acknowledged that: '[t]he fight against serious crime, in particular against organised crime and terrorism, is indeed of the utmost importance in order to ensure public security, and its effectiveness may depend to a great extent on the use of modern investigation techniques. However, the CJEU held that such an objective of general interest, 'however fundamental it may be, does not, in itself, justify a retention measure such as that established by Directive 2006/24/EC being considered to be necessary for the purpose of that fight.' [474] In support of this argument, the CJEU emphasised that the Data Retention Directive set up a regime which failed to provide an interference 'Limited to what is strictly necessary.' On the contrary the Data Retention Directive entailed 'an interference with the fundamental rights of practically the entire European population.'[475]

In summary, the Court struck down the Directive because of the unlimited scope of its application, [476] but it did not impose any limit in the ability of national authorities to access data retained by private companies.[477] The Court did not prescribe a sufficiently restrictive time-frame for the retention of data;[478] it did not provide adequate safeguards for the security and protection of data retained by private provisions of electronic communications;[479] the Directive did not impose a requirement that the data be retained within the European Union [480] The Court held that the absence of a requirement to keep within the European Union, the data retained by private providers of electronic communications had the result that 'it cannot be held that the control, explicitly required by Article 8(3) of the Charter, by an independent authority of compliance with the requirements of protection and security…. is fully

[473] ibid, at para 49.
[474] ibid, at para 51.
[475] ibid, at para 56.
[476] The Directive affects 'in a comprehensive manner, all persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime,' judgment at para 58.
[477] The Directive did not make access to metadata subject to 'a prior review carried out by a court or by an independent administrative body,' judgment at para 62.
[478] The Directive did not make any distinction between the categories of data required to be retained under its Article 5 'on the basis of their possible usefulness for the purposes of the objective pursued,' judgment at para 64.
[479] Judgment at para 66.
[480] ibid, para 68.

ensured.' [481] The CJEU concluded that the EU legislators, in drafting the Data Retention Directive, 'exceeded the limit imposed by compliance with the principle of proportionality in light of Articles 7, 8 and 52(1) of the Charter' and without dealing with the other questions raised, declared that Directive to be invalid, without temporal restrictions.[482]

9.0 Significance of the *Digital Rights Ireland and Seitlinger* Judgment and its Context

The judgment of the CJEU in the *Digital Rights Ireland* [483] case is a landmark one in many respects. It marks the first time that the highest Court in the EU has invalidated an entire EU legal instrument due to its incompatibility with the EU Charter of Fundamental Rights.

This case resulted from a preliminary reference from the Irish High Court under article 267 TFEU regarding the 2006 Data Retention Directive 2006/24/EC.[484] The CJEU was asked to consider whether the restriction on the Plaintiff's rights regarding its use of mobile phone telephony emanating from Articles 3,4 and 6 of Directive 2006/24/EC were incompatible with Article 5.4 of the TEU as being disproportionate, unnecessary or inappropriate in achieving the legitimate aims of ensuring that certain data are available for the purposes of investigation, detection and prosecution of serious crime.

The CJEU was asked specifically to consider whether: the Directive was compatible with the right of EU citizens to move and reside freely within the EU; was compatible with the right to privacy as enshrined by Article 7 of the EU charter of Fundamental Rights and under Article 8 of the ECHR; was compatible with the right to protection of personal data enshrined in Article 8 of the EU Charter; was compatible with the right to freedom of expression as enshrined in Article 11 of the EU Charter and article 10 of the ECHR and

[481] The CJEU added that: 'Such a control, carried out on the basis of EU law, is an essential component of the protection of individuals with regard to the processing of personal data,' citing Case C-614/10, *Commission v Austria*: EC C: 2012:631, at para 37.
[482] Judgment at para 69. This means that, following the CJEU judgment, the Data Retention Directive was made immediately inapplicable in the EU legal order, but also to be considered as having never existed, Judgment at para 71.
[483] Joined Cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others*. Grand Chamber CJEU, 8 April 2014.
[484] *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources* (Irish Human Rights Commission, Amicus Curiae) [2010] IEHC 221.

whether Directive 2006/24/EC was compatible with the right to Good Administration as enshrined in Article 41 of the EU Charter. In its verdict of 8 April, 2014, the Grand chamber of the CJEU held that Directive 2006/24/EC was incompatible with EU law. Fabbrini describes the judgment as

> [A]rguably the most advanced court pronouncement to date—in the area of privacy rights in the digital age. The effects of the ECJ's decision may extend beyond the borders of the EU by enshrining in clear, more-explicit-than-ever language the idea that core constitutional protections of privacy rights must be strengthened— not weakened—in an era of increasing digitalization in which governments have acquired greater technological capacity to surveil citizens on a mass scale. Thus, the ECJ's decision provides arguments for further trans-national enhancement of personal data and privacy rights protections and may serve as a model for other jurisdictions to consider in their own reform processes.[485]

The decision also marks a major adjustment of the data privacy/national security balance in favour of data privacy, and the confirmation of the CJEU as a leading forum for the protection of fundamental rights and liberties, among these rights and liberties being the right to privacy in general and to data protection as a species within the broader genus of privacy rights. Ojanen argues that the CJEU judgment is 'undoubtedly one of the most significant judgments ever given by the Court of Justice on fundamental rights within the EU legal order in general, particularly insofar as judicial review of the compatibility of EU legislation with fundamental rights is concerned' and that it will feature as a precedent which sets out the EU law approach to electronic mass surveillance in the light of the right to private life and the protection of personal data.[486]

[485] Federico Fabbrini, 'Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and surveillance in the United States' 28 (2015) *Harvard Human Rights Journal* 67-68.
[486] Tuomas Ojanen, 'Privacy is more than a seven-letter word: the Court of Justice of the European Union sets Constitutional limits on Mass Surveillance' 10(3) (2014) *European Constitutional Law Review* 528, 529.

The judgment in the *Digital Rights Ireland* [487] case is one element of a dynamic involving not only the status of fundamental rights, specifically the protection of data privacy rights in the context of counter-terrorism. Other elements include the transformation of the CJEU from an economic Court to one actively committed to privacy rights in a climate where these have been threatened not merely by privacy-invasive legislative measures in Europe, but worldwide. The case-law of the CJEU prior to its striking down of the Data Retention Directive, demonstrated its willingness to undertake a rigorous rights-based review of EU privacy-restrictive measures in the light of the privacy of guarantees of the EU Charter of Fundamental Rights, particularly after the Charter had become part of EU primary law in 2009.[488]

The privacy provisions of the Charter of Fundamental Rights gave the CJEU an effective platform from which to challenge infractions of privacy law. The *Digital Rights Ireland* [489] judgment should also be viewed in the light of the Snowden revelations of June 2013, which implicated the United States and British intelligence services in mass metadata surveillance of entire populations in which the United States and British Governments were directly complicit. Snowden revealed that United States national security agencies had been sharing personal data obtained from their large-scale surveillance regimes with government authorities outside of the United States. It became public knowledge worldwide that one of the United States monitoring programmes, which had been operating for more than seven years, involved the mass retention and access to metadata, for national security and law enforcement purposes, from the use of mobile phones – a practice also instituted by the EU

[487] Joined Cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others*. Grand Chamber CJEU, 8 April 2014.
[488] Examples of judgments where the ECJ upheld the concept of fundamental rights with regard to counter-terrorism are Joined Cases C-402/05 P and C-415/05 P *Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities* [2008] ECR I-6351 and Joined Cases C-584/10 P, C-593/10 P and C-595/10 P, *Commission, Council, United Kingdom v Yassin Abdullah Kadi* 18 July 2013.
[489] Joined Cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others*. Grand Chamber CJEU, 8 April 2014.

Data Retention Directive, which also involved the monitoring entire European populations.[490]

The worldwide media publicity given to the Snowden revelations following detailed analysis of these in major United Kingdom and United States newspapers *The Guardian* and *The Washington Post* helped to generate a growing concern in Europe that on foot of the Data Retention Directive, the EU legislature permitted EU Member States to require the private sector to retain customers' metadata for up to two years, and that while this practice prevailed in Europe, news media outlets worldwide were exposing the questionable legality of United States security authorities harvesting massive quantities of metadata and sharing these with governments outside the United States. In this climate, it was inevitable that the CJEU, given its record of robust scrutiny of EU measures compromising the citizens' right to privacy and data protection, would intervene actively in protecting these rights when the opportunity arose, as it did in the case of *Digital Rights Ireland*.[491] Ní Loideáin, among other commentators, regarded the Snowden revelations as having an influence on that landmark judgment.[492]

In a further case *Maximilian Schrems v Data Protection Commissioner*[493] involving the protection of data privacy brought before the Irish High Court and referred by that Court to the CJEU pursuant to Article 267 TFEU, the applicant maintained that, 'as the Snowden disclosures demonstrate that there is no effective data protection in the United States, the Irish Data Protection Commissioner 'should exercise his statutory powers to direct that the transfer of personal data from Facebook Ireland to its parent company in the United States should cease.' [494] The Commissioner countered by citing a finding of the

[490] These issues were raised by the Article 29 Working Party: Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, Brussels, Secretariat of the European Commission 919/14/EN <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf> accessed 23 August 2015. See also: Glenn Greenwald, 'No place to hide: Edward Snowden, the NSA and the U.S. Surveillance State (Picador, London 2014). See also Luke Harding, The Snowden Files: The Inside Story Of The World's Most Wanted Man (London 2014).
[491] Joined Cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others*. Grand Chamber CJEU, 8 April 2014.
[492] Nora Ní Loideáin, 'EU Law and Mass Internet Surveillance in the post-Snowden Era' 3(2) (2015) *Media and Communication Data* 53.
[493] [2014] IEHC 310.
[494] ibid, para 2.

European Commission in July 2000 that the data protection regime in the United States is 'adequate and effective where the Companies which transfer or process the data to the U.S. self-certify that they comply with the principles set down in this Commission decision.'[495]

The European Commission decision establishes a regime known as the Safe Harbour Regime, which gives the *imprimatur* to data transfers on the basis that the European Commission concluded that 'the U.S. does, in fact, provide for data protection.'[496] However, as Mr. Justice Hogan, of the Irish High Court, who heard the appeal remarked, one of the many issues arising from the Court proceedings was 'whether the Safe Harbour Proceedings are still effective and functional some fourteen years after that decision and finding.'[497] It is significant that Hogan J. declared that the Snowden revelations form the backdrop 'to the judicial review application' made by Maximilian Schrems.[498] It is also clear that Hogan J. was convinced of the veracity of what Snowden was saying, and more importantly that he regarded the personal data transferred by companies such as Facebook Ireland to its parent company in the United States as 'capable of being accessed by the NSA in the course of a mass and indiscriminate surveillance of such data. Indeed, in the wake of the Snowden revelations, the available evidence presently admits of no other realistic conclusion.'[499]

Voices other than Snowden's made themselves heard in the public debate about the implications of the indiscriminate mass metadata surveillance of entire populations and in particular the threat posed by this practice to the privacy and liberty of individuals. On the other hand, national security and law enforcement authorities worldwide have long regarded the monitoring of metadata as an essential tool in the fight against terrorism and the protection of national security. Michael Hayden, former director of the United States National Security Agency and the CIA, commented in the course of a public discussion

[495] ibid.
[496] ibid, para 3.
[497] ibid, para 2.
[498] ibid.
[499] ibid, para 13.

about privacy and the NSA that: 'We kill people based on metadata.'[500] An important feature of the *Digital Rights Ireland* [501] judgment is that it shifts the responsibility to protect human rights to the EU legislator. Granger and Irion suggest that the legal weight of the EU Charter [since 2009] and the nearing prospect of EU accession to the ECHR contributed to this shifting of responsibility. They add, however, that the timing of this may be explained by the Snowden revelations, 'which exposed the scale of electronic surveillance carried out by government agencies on both sides of the Atlantic and cast doubts as to the ability of national authorities to afford sufficient guarantees to basic rights.'[502] Granger and Irion also suggest that the shifting of responsibility for compliance with human rights standards to the EU institutions may be read as the CJEU response to the mounting concerns regarding respect for privacy rights in some Member States, notably Hungary,[503] and the contribution of the CJEU 'to the development of mechanisms at better securing respect for the core principles and values on which the European Union is based.'[504]

10.0 Consequences of the Digital Rights Ireland Judgment for Data Privacy/National Security in Europe

One important consequence of the judgment is that from now on, the EU legislator has reduced discretion when adopting legislative measures, such as Directives and Regulations, that interfere to a significant degree with the right to privacy or other fundamental rights protected by the EU Charter of Fundamental Rights and the ECHR and that the CJEU will exercise strict control over such acts.[505]

---

[500] Bruce Schneier, *Data And Goliath. The Hidden Battle to Collect Your Data and Control Your World* (W.W Norton and Company New York, 2015), 23.

[501] Joined Cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others*. Grand Chamber CJEU, 8 April 2014.

[502] Marie-Pierre Granger and Kristina Irion, 'The Court of Justice and the Data Retention Directive in Digital Rights Ireland; telling off the EU legislator and teaching a lesson in privacy and data protection' 39(6) (2014) *European Law Review* 835, 845.

[503] On the same day that the judgment in the *Digital Rights Ireland* was delivered, the CJEU also condemned the premature dismissal of the Hungarian Data Protection Officer, as a violation of the Data Protection Directive - Commission v Hungary C-288-12 (2014).

[504] Marie-Pierre Granger and Kristina Irion, 'The Court of Justice and the Data Retention Directive in Digital Rights Ireland; telling off the EU legislator and teaching a lesson in privacy and data protection' 39(6) (2014) *European Law Review* 835,845.

[505] 'As a result, the obligation imposed by Articles 3 and 6 of Directive 2006/24 on providers of publicly available electronic communications services or of public communications networks to retain, for a certain period, data relating to a person's private life and to his communications, such as those referred to in Article 5 of the directive, constitutes in itself an interference with the rights guaranteed by Article 7 of the Charter.' Joined Cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others*. Grand Chamber CJEU, 8 April 2014, at para 34.

The Report of the Council of the European Union on the consequences of the Digital Rights Ireland judgment acknowledged that the judgment was 'of crucial importance in view of further action of the Union in the field of privacy and data protection,' [506] and further acknowledged that henceforth the CJEU 'will not satisfy itself with anything less than a strict assessment of the proportionality and necessity of measures that constitute serious restrictions to fundamental rights, however legitimate the objectives pursued by the EU legislature.' [507]

The Council also interpreted the judgment as indicating that retention measures which constitute serious restrictions to fundamental rights:

> [D]o not stand a serious chance of passing the legality test unless they are accompanied by adequate safeguards in order to ensure that any serious restriction of fundamental rights is circumscribed to what is strictly necessary and is decided in the framework of guarantees forming part of Union legislation instead of being left to the legislation of Member States.[508]

It accepted that the requirement of a high level of protection applies 'with particular strength in cases where EU legislation foresees mass data collection, storage of the data of a very large number of unsuspected persons and access to and use of such data by law enforcement authorities.'[509] Finally, the EU Council held that it had the duty 'to take the necessary steps stemming from the judgment of the Court as regards existing, proposed and future legislation of the European Union on data protection.'[510]

From the perspective of the data privacy/national security balancing paradigm, the *Digital Rights Ireland* judgment,[511] has two positive consequences for the data privacy side of the balance for four reasons. The first is that the CJEU has

[506] Council of the European Union, 'Judgment of the Court of 8 April 2014 in joined cases C-293/12 and 594/12,' 5 May 2014, 9009/14, 8, para 19.
[507] ibid.
[508] ibid.
[509] ibid, para 20.
[510] ibid, para 21.
[511] Joined Cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others*. Grand Chamber CJEU, 8 April 2014.

imposed major restrictions on the capacity of EU legislators to introduce measures that interfere in a significant way with the right to privacy in contravention of the provisions of the EU Charter of Fundamental Rights or of the ECHR. The second is that the judgment places an onus on the EU legislators to ensure that with regard to existing, proposed and future legislation relating to data privacy, they adhere to the principles laid down in the *Digital Rights Ireland* judgment. The third is that the judgment obliges EU legislators to ensure that when measures, such as those designed to protect national security or combat serous crime, are prepared, adequate safeguards must be included in order to avoid abuses of fundamental rights, such as the right to individual privacy. The fourth is that the CJEU has invalidated the single most privacy-invasive EU privacy measure, the Data Retention Directive, and in the process demonstrated its willingness to take a firm line in the future, as it asserts its power to arbitrate on human rights issues in judgments that are not subject to appeal.

There is general consensus that the *Digital Rights Ireland* [512] judgment marks a significant advance on the protection of fundamental rights at EU level, and for data protection and the right to privacy in Europe. However, it is important to remember that the *Digital Rights Ireland* judgment invalidated one measure, the Data Retention Directive, involving the retention of metadata on a Europe-wide scale, but that it did not rule against mandatory data retention *per se*. As Ojanen suggests, the undertone of the judgment in *Digital Rights Ireland* 'seems to be that some form of mandatory data retention in order to control serious crime and terrorism might indeed be compatible with human rights.'[513] In the course of the *Digital Rights Ireland* judgment, the CJEU held that the retention of data for the purpose of allowing the competent authorities to have possible access to those data as required by the Data Retention Directive 'genuinely satisfies an objective of general interest.'[514] Observing that the material objective of the Data Retention Directive is to contribute to the fight against serious crime, and thus, ultimately, to public security, the Court

[512] ibid.
[513] Tuomas Ojanen, 'Privacy is more than a seven-letter word: the Court of Justice of the European Union sets Constitutional limits on Mass Surveillance' 10(3) (2014) *European Constitutional Law Review* 528,540. For the basis of Ojanen's contention, see in particular, Joined Cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others*. Grand Chamber CJEU, 8 April 2014, at para 42.
[514] ibid, [Joined Cases], at paras 41-44.

recalled that, according to its previous case-law, the fight against international terrorism in order to maintain international peace and security, constitutes an object of general interest,[515] and that the same was true of the fight against serious crime in order to maintain public security.[516]

The Court further noted that Article 6 of the EU Charter of Fundamental Rights lays down the right of any person not only to liberty, but also to security.[517] The Court also noted the view of the EU Justice and Home Affairs Council expressed in December 2002 that data relating to the use of electronic communications are particularly important and therefore a valuable tool in the prevention of offences and the fight against crime, and in particular organised crime.[518] These observations of the Court make it clear that it recognises the legitimacy of data retention and its utility in the fight against international terrorism and other forms of crime, and from this it may be inferred that it recognises the need for a balancing exercise when EU legislation with the objective of fighting terrorism and crime in general impinges on data privacy rights.

On 29 October 2014, the Chairman of the Committee on Civil Liberties, Justice and Home Affairs asked the EU Legal Service for an opinion on various questions arising from the *Digital Rights Ireland* judgment. This legal opinion was delivered on 8 January 2015. One of these questions dealt with the consequences of the judgment for existing Union law requiring mass personal data collection other than traffic data of a very large number of persons and access to and use of such data by law enforcement authorities. In dealing with this question the Legal Service stated that, from a purely legal point of view, 'the *Digital Rights Ireland* judgment itself concerns only the validity of the Data Retention Directive' and therefore does not have any *direct* consequences for the validity of any other EU act, adding that existing EU Acts benefit from

[515] See Cases C-402/05 P, *Kafi and Al Barakaat International Foundation v Council and Commission* EU:C:2008:461, at para 363. See also Cases C-539/10 P and C-550/10 P *Al-Aqsa v Council* EU:C:2012:711, para 130.
[516] Case C-145/09 *Tsakouridis* EU:C:2010:708, paras 46-47.
[517] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others*. Grand Chamber CJEU, 8 April 2014, at para 42.
[518] ibid, at para 43.

a presumption of legality.[519] However, the Legal Service pointed out that the presumption of legality can also be rebutted, so that any other EU measure could suffer the same fate as the Data Retention Directive in a separate legal procedure. If any other measure were challenged, the CJEU reasoning in *Digital Rights Ireland* could be invoked to lead to the same or a similar outcome as that in the *Digital Rights Ireland* case. On the question whether the *Digital Rights Ireland* [520] judgment produced any effect on the laws of Member States enacted to implement the Data Retention Directive, the answer was that the judgment produces a twofold effect as regards those laws. Firstly, since the Data Retention Directive has been declared invalid, the Member States can decide to repeal the laws relating to it, as countries such as Austria or Romania have done since the ruling. Secondly, if Member States were to keep measures for the retention of data, those States must ensure that their national laws on data retention comply with the EU Charter of Fundamental Rights and fulfil the requirements laid down in the e-Privacy Directive of 2002.[521] Directive 2002/58/EC was promulgated on 12 July 2002 as a replacement for Directive 97/66/EC which concerned personal data processing and the protection of telecommunications privacy.[522] In common with its predecessor Directive 97/66/EC, Directive 2002/58/EC provides safeguards regarding the confidentiality of communications,[523] and encompasses the provisions of the

[519] European Parliament, Legal Opinion, questions relating to the judgments of the Court of justice of 1 April 2014 in Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others*. Grand Chamber CJEU, 8 April 2014; Directive 2006/24/EC on data retention - Consequences of the Judgment, SJ-0890/14 22 December 2014), 12. Available at: <http://statewatch.org/news/2015/jan/ep-digital-rights-legal-opinion.pdf> Accessed 10 June, 2017.

[520] Joined Cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others*. Grand Chamber CJEU, 8 April 2014.

[521] European Parliament, Legal Opinion, questions relating to the judgments of the Court of justice of 1 April 2014 in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and others* - Directive 2006/24/EC on data retention - Consequences of the Judgment, SJ-0890/14 22 December 2014) 15. Available at: <http://statewatch.org/news/2015/jan/ep-digital-rights-legal-opinion.pdf> Accessed 10 June, 2017.

[522] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. OJ L201/37.

[523] ibid, Recital 3.

Data Protection Directive (95/46/EC).[524] Directive 2002/58/EC was amended by Directive 2009/136/EC.[525]

It is also important to note that even in the wake of the invalidation of the Data Retention Directive, two measures still exist which facilitate the processing of personal data by EU Member States. The processing of personal data in the internal market is regulated by the Data Protection Directive.[526] The processing of personal data in the electronic communications sector is regulated in the e-Privacy Directive.[527] Directive 2002/58/EC imposes an obligation on the Member States to ensure the confidentiality of communications (Article 5) and the obligation to erase traffic data after it is no longer needed for the purpose of a communication. (Article 6). However, Article 15(1) of this Directive allowed the Member States to restrict the scope of these two rights and adopt measures for the retention of data for a limited period. The justification for this restriction, which echoes that provided for in Article 13(1) of the Data Protection Directive 95/46/EC and Article 8 ECHR, and which is based on defending national security, public security and preventing crime.

Article 15(1) of Directive 2002/58/EC allows the restriction when 'it constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security and the prevention, investigation and prosecution of criminal offences or of unauthorised use of electronic communications systems, as referred to in Article 13(1) of Directive 95/46/EC. To this end, 'Member States *may*, inter alia adopt legislative measures providing for the retention of data for a limited period, justified on the grounds laid down in this paragraph,'

[524] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. OJ L201/37, Article 2(1).
[525] Directive 2009/136/EC Of The European Parliament And Of The Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.
[526] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. OJ L281, 23.11.1995, at 31.
[527] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. OJ L201/37.

The rules mentioned above applied to data retention in the electronic communications sector before the Data Retention Directive introduced a derogation as the CJEU pointed out in the *Digital Rights Ireland* judgment, 'from the system of protection of the right to privacy established by Directives 95/46/EC and 2002/58/EC.' [528] Prior to the introduction of the Data Retention Directive, Member States had an *option* to adopt legislative measures providing for the retention of data. With the adoption of the e-Privacy Directive, the *option* became an *obligation* to adopt such measures. As a result of the invalidation of the Data Retention Directive, Article 15(1) of the e-Privacy Directive is once again applicable to national measures providing for data protection in the electronic communications sector. The important point here is that being now subject to Article 15(1) of the e-Privacy Directive, national rules are implementing EU law, which entails the applicability of the EU Charter of Fundamental Rights. As a result, Member States must ensure that national measures dealing with data retention in the electronic communications sector are compatible with the EU Charter, in particular with Articles 7, 8 and 52(1), as interpreted by the CJEU in the *Digital Rights Ireland* judgment. This includes all the criteria set out by the EU in this judgment, with regard to the proportionality of the interference, including the existence of 'clear and precise rules' to limit the interference to what is 'strictly necessary, as well as the inclusion of 'minimum safeguards.'[529]

The EU Legal Services, when asked what options would be available to Member States with regard to national data retention laws, following the *Digital Rights Ireland* [530] judgment, responded that that Member States have a choice as between *repealing* their national measures on data retention or *maintaining* them:

> If a Member State chooses the latter option, its national legislation should be examined to see whether it fulfils the requirements laid down in

[528] Joined Cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others*. Grand Chamber CJEU, 8 April 2014, at para 32 and paras 39,40 and 106 of the Opinion of Advocate-General Cruz-Villalón, on The Data Retention Directive.
[529] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others*. Grand Chamber CJEU, 8 April 2014, at para 54. For relevant case law, see Case C-390/12, *Pfleger* [2014] EU-C: 281, at para 36.
[530] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others*. Grand Chamber CJEU, 8 April 2014.

> Article 15(1) of the e-Privacy Directive and whether it is compatible with Articles 7, 8 and 52(1) of the Charter, as interpreted by the Court of Justice in the DRI judgment. If this assessment concludes that the national legislation does not comply with these fundamental rights requirements, this should lead to the amendment of the Member State's legislation.[531]

On 8 April 2014, the same day as the Data Retention Directive was declared invalid, the European Data Protection Supervisor issued a statement welcoming the CJEU judgment, commenting that the EU 'cannot leave the full responsibility for the use of the data with Member States.'[532] The EDPS anticipated that, taking into account the Court's judgment, 'will now reflect on the need for a new Directive, which will prevent Member States from keeping or imposing the same legal obligations nationally as laid out in the now invalid Data Retention Directive.'[533]

The question of how such a new Directive would differ from, the measure struck down by the CJEU is significant. As has been indicated earlier in this section, the Court's judgment implies that some form of mandatory data retention with the objective of combating serious crime and terrorism is acceptable from the perspective of the EU Charter of Fundamental Rights. It is also the case that the CJEU sets out detailed guidelines for the EU legislature and for national legislators in its judgment. In a comment on the likely shape of a new Directive, Peers visualises a number of essential features. Firstly, this measure would have to be targeted on communications with a particular link to terrorism and crime. It would need to avoid any provision for mass surveillance, which would constitute an unjustifiable interference with rights

[531] Opinion SJ-0890/14 LIBE - Questions relating to the judgment of the Court of Justice of 8 April2014 in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* and *Seitlinger and others* - Directive 2006/24/EC on data retention - Consequences of the judgment. at 19, para 84 <http://www.statewatch.org/news/2015/apr/ep-ls-opinion-digital-rights-judgment.pdf> accessed 21 September 2016.

[532] 'The CJEU rules that Data Retention Directive is invalid' *European Data Protection Supervisor* (Press Statement, 8 April, 2014). <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2014/14-04-08_Press_statement_DRD_EN.pdf> accessed 8 April 2014.

[533] ibid.

emanating from the EU Charter of Fundamental Rights.[534] Secondly, a new Directive would have to embody rules on the definition of 'serious crime,' the purpose of subsequent access to data; limits on the number of persons who could access the data; and control of access to the data by means of a Court or other independent administrative body.[535] Thirdly, the new Directive would have to include stronger rules on the length of time for which data would be retained, for instance as to the categories of data to be retained for the entire period, as well as the protection of the data from unlawful access and use, and require that the data be retained within the EU only.[536] Any future proposal seeking to retain communications data by means of a Directive, or other instrument, at EU or Member State level will prove difficult in the light of the *Digital Rights Ireland* verdict.[537] The ruling provides the basis of a framework for the strict scrutiny of surveillance practices in the EU and as a consequence, the standards of human rights protection in this regard have been enhanced.[538]

11.0 Judgments of the CJEU in the *Google Spain* and *Schrems* Cases

The CJEU judgment in *Digital Rights Ireland* [539] was followed on May 13, 2014 by its decision in *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González.*[540] The genesis of this case may be traced to January and March, 1998, when a Spanish Newspaper, on foot of an order from the Spanish Ministry of Labour and Social Affairs, published formal notices stating that assets connected to Mr. González were to be auctioned to defray social security debts. These notices were later made accessible via the newspaper's website, which was trawled and indexed by the Google search engine.

Mr. González, noting that a Google search against his name returned these notices, filed a complaint in 2010 with the AEPD in which he demanded the removal by Google of the links to the 1998 newspaper articles, on the ground

[534] Steve Peers, 'The data retention judgment: The CJEU prohibits mass surveillance,' *EU Law Analysis* (8 April 2014) <http://eulawanalysis.blogspot.ie/2014/04/the-data-retention-judgment-cjeu.htm> accessed 26 September 2016.
[535] ibid.
[536] ibid.
[537] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* and *Seitlinger and others.*
[538] Hielke Hijmans, *The European Union as Guardian of Internet Privacy. The Story of Article 16 TFEU* (Springer, 2016) 249.
[539] Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* and *Seitlinger and others*
[540] *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González,* Case C-131/12, 13 May 2014.

that linking to these notices violated his data protection rights. The AEPD rejected the Applicant's complaint against the newspaper on the basis that the materials pertaining to him on its website were lawfully advertised and had a legitimate purpose, but upheld his complaint in relation to Google and found that operators of search engines are responsible for data made available through them in instances when information could breach data protection rights and where an individual does not want data relating to them to become known to a third party.

Google appealed the decision of the Spanish Data Protection Authority to the Spanish High Court which stayed the proceedings on the basis that the matters before it constituted a question captured by EU law and sought a reference from the CJEU for a preliminary ruling. The Spanish National High Court asked the CJEU to consider inter alia whether (1) the Spanish Data Protection Authority is mandated to compel Google to de-list from its search results information published online by third parties and (2) does a right to have information erased and/or a right to object to the provision of such information, mandated by the Data Protection Directive, permit a data subject to submit a direct request search engine providers to prevent information related to a data subject which could serve to prejudice them or in instances where a data subject wishes to be forgotten following the elapse of a period of time, notwithstanding that the information had been lawfully published by a third party.

On 13 May 2014, the CJEU approved the AEPD decision in relation to Google. In its verdict, the CJEU considered the question of data privacy and held that Internet search operators, in their capacity as data controllers, are responsible for the processing of personal data which is conducted on web pages published by third parties and that such processing must be conducted in conformity with privacy safeguards enshrined in the Data Protection Directive.[541] In its judgment, the CJEU referred to Article 12(b) of the Data Protection Directive, which confers a right of erasure or blocking of data on data subjects in instances where the processing of personal data is not in conformity with the provisions of the Data Protection Directive, in particular when data processed

[541] ibid, at para 83.

are inaccurate, irrelevant, inadequate or excessive when measured against the basis for any data processing.[542] The CJEU further held that although data processing which might have been initially lawful, could, following the passage of time become incompatible with the provisions of the Data Protection Directive, when such data are deemed no longer necessary when measured against the reasons for which they were processed.[543]

The gravamen of the CJEU decision is that the right of data subjects to compel an Internet search engine provider to remove links relating to them, not only in the 'economic interest of the operator of the search engine,' but also in 'the interest of the general public in finding that information upon a search relating to the data subject's name.' [544] The CJEU did, however, emphasise that it would be permissible to depart from the foregoing in relation to a data subject who occupied a role in public life and that interference with the data processing rights of such individuals would be permissible and justified due to 'the preponderant interest of the general public in having access to information.' [545] The CJEU held that in the instant case, that the public interest consideration in relation to the processing of the Applicant's data, which concerned access to information relating to a real estate auction some sixteen years previously, did not pass muster.[546]

11.1 Implications of the *Google Spain* Judgment

The *Google Spain* judgment has two significant aspects. It represents an acknowledgement by the highest judicial tribunal in Europe of the rights of Internet users to have personal data pertaining to them expunged from search engines by request, even if, as was the case in *Google Spain*, such data were true and accurate. Furthermore, by extension, in thus expanding the scope and application of data protection law, the CJEU was also reducing the protection of free speech in the EU legal order. In this regard, the following observations are instructive:

[542] ibid, at para 92.
[543] ibid, at para 93.
[544] ibid, at para 97.
[545] ibid, at para 97.
[546] ibid, at para 98.

> [D]ata protection only became a fundamental right across Europe as a result of the adoption of the Lisbon Treaty. In contrast, free speech and the right to freely receive and impart information are core and well established human rights, well recognised in the legal orders of most EU states. Notwithstanding this, the Court appears to have found that the new right to data protection takes precedence over, and as a result erodes, the traditional protection of free expression.[547]

In finding that the right to privacy and data protection takes precedence *'as a rule'*[548] over the right of the public to access and communicate true information about an individual, the Court did not advert to the EU Charter of Fundamental Rights, regarding the provisions of which the CJEU had considered in the *Digital Rights Ireland* judgment.[549] Article 11(1) of the EU Charter of Fundamental Rights protects 'the right to freedom of expression,' and which includes 'freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.'

The CJEU ruling was based on a number of findings. One was that, since Google whose search engine is operated by Google, Inc. a U.S. Company, had a Spanish office, this justified the application of Spanish jurisdiction data protection law to the Google search implicated in this case. Further, the Court somewhat dubiously found that a search engine processes personal data and functions as a data controller, in spite of the fact that Google's processing is conducted by algorithms and that it does not know, or control the data returned in search results. The CJEU also found that a search engine can be required to remove links to lawful information published on another website. Having found that a search engine is a data controller and thus liable under data protection law for the results that it returns, the Court concluded that non-compliance with data protection by the search engine gives the individual

[547] 'Google and the "Right to be Forgotten" - What the Court Said and Why it Matters' (15 May 2014). *Mason Hayes and Curran Technology Law Blog* <http://www.mhc.ie/latest/blog/google-and-the-right-to-be-forgotten-what-the-court-said-and-why-it-matters> accessed 11 September 2016.
[548] *Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González,* Case C-131/12, 13 May 2014, at para 97.
[549] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others*. Grand Chamber CJEU, 8 April 2014.

named in a search result the right to have the offending link removed from the search results and so exercise 'the right to be forgotten.'[550]

The CJEU verdict is silent in relation to a number of key questions. Firstly, what constitutes the territorial extent of the right to be forgotten doctrine - does it extend beyond the EU? Secondly, In light of the verdict, how is Google to deal with delisting requests from parties who gave consent that information pertaining to them be made available online? Thirdly, should it be mandatory that when a delisting decision is made, it must be accompanied by an obligation to inform the publisher of such information in advance? [551] Dawson observes that these questions have implications for 'the concrete realisation of the Court's ruling,' and given the complexity of the issues captured by the case, the CJEU has failed to address them.[552]

The *Google Spain* verdict has additional and profound implications. The CJEU's interpretation of the Data Protection Directive as encompassing a right to be forgotten, accords it the role of being arbiter in relation to the right throughout the EU and removes this role from the legal ambit of Member States.[553] However, Stute contends that the CJEU verdict might not have adequately balanced the competing rights at play and questions the Court's approach in seeming to presume that the rights of a data subject take primacy over the rights of others.[554] Moreover, the absence of a precise definition and scope of the right to be forgotten in terms of geographic scope, applicable domains and standing requirements represent a shortcoming of the judgment.[555]

It is also the case that the judgment is silent regarding exceptions applicable to the rights of a data subject in relation to the right to be forgotten. The judgment is notable for its treatment of two competing rights which are key normative

[550] For commentary on the *Google Spain* decision, see Eleni Frantziou, 'Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in case C-132/12, *Google Spain, SL, Google Inc v Agencia Espanola de Protection de Datos*' 14 (2014) *Human Rights Law Review* 761.
[551] See Mark Dawson, *The Governance of EU Fundamental Rights* (Cambridge University Press, 2017) 125.
[552] ibid.
[553] David J. Stute, 'Privacy Almighty? The CJEU's Judgment on *Google Spain Sl v. AEPD*' 36(4) (2015) *Michigan Journal of International Law* 649, 679.
[554] ibid.
[555] ibid.

concerns in the digital age - those of freedom of expression and the data privacy. The Court's handling of these competing interests is viewed by Byrne as having been conducted with a 'blind eye,' thus involving an injustice to the people of Europe.[556]

11.2 *Schrems v Data Protection Commissioner*

In its judgment in the *Schrems* case, delivered on 6 October 2015,[557] the CJEU invalidated the Safe Harbour Agreement which allowed content providers to process the data of the EU citizens in the U.S.A. The Applicant, an Austrian national and Facebook user, objected to the transfer of his personal data to the United States, owing to the Snowden revelations which highlighted the activities of the NSA. The Applicant tendered a complaint to the Irish Data Protection Commissioner, contesting the validity of the Safe Harbor Scheme, relating to the transfer of personal data from the EU to the US and whether such transfers comported with the privacy rights enshrined by Articles 7, 8 and 47 of the European Charter of Fundamental Rights. The Irish Data Protection Commissioner declined to investigate the Applicant's complaint, and he then sought judicial review of the decision before the Irish High Court, from where a reference was directed to the CJEU. The reference posited a question to the CJEU asking for a determination as to whether a national data protection supervisory authority is obliged to abide by a decision made by the EU Commission regarding the adequacy of EU-US data transfers and associated safeguards.

Schrems based his case on the fact that some or all of the data provided by him to Facebook is transferred from Facebook's Irish subsidiary to servers located in the U.S.A., where it is processed. Schrems took the view that, in the light of the revelations made in 2013 by Edward Snowden concerning the privacy-invasive activities of the U.S. intelligence services, particularly the National Security Agency, the law and practice of the U.S.A. do not offer sufficient protection against surveillance by the public authorities of the data transferred to that country.

---

[556] Adam Byrne, 'European Data Protection Uncapped: A Critical Analysis of *Google Spain v. AEPD*' 38 (2016) *Loyola of Los Angeles International and Comparative Law Review* 115, 139.
[557] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* Judgment of 6 October 2015.

The issue before the CJEU was whether the EU Commission Decision of 2000[558] had the effect of preventing a national supervisory authority from investigating a complaint alleging that the U.S.A. does not ensure an adequate level of protection, and where appropriate, from suspending the contested transfer of data. In its judgment, the CJEU held that the existence of a Commission decision finding that a third country ensures an adequate level of protection of the personal data transferred cannot eliminate or even reduce the powers available to both the national supervisory authorities under the EU Charter of Fundamental Rights and the Data Protection Directive.[559]

The CJEU held that no provision of the Data Protection Directive prevents oversight by the national supervisory authorities of transfers of personal data to third countries which have been the subject of a Commission decision. Thus, the Court argued, even if the Commission has adopted a decision, the national supervisory authorities, when dealing with a claim, must be able to examine with complete independence, whether the transfer of a person's data to a third country complies with the requirements laid down by the Directive.

The CJEU then laid out its own role as final arbiter in the matter under consideration in this case, pointing out that it alone has jurisdiction to declare that an EU act, such as a Commission decision, is invalid. It then outlined the procedure to be followed where a national authority, or a person [such as *Schrems*] who has brought the matter before the national authority, considers that a Commission decision is invalid, that the authority or person must be able to bring the matter before the national courts, so that they may refer the case to the CJEU if they too have doubts as to the validity of the Commission decision. This meant the Court held, that it is thus ultimately the CJEU which has the task of deciding whether or not the Commission decision is invalid.

Having established this principle, the CJEU went on to consider whether the Safe Harbour decision was invalid. In this regard, the CJEU found that the

[558] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (2000/520/EC).

[559] The Data Protection Directive provides that the transfer of personal data to a third country may, in principle, take place only if that third country ensures an adequate protection of the data.

Commission was required to find that the U.S. in fact ensured that by reason of its domestic law or its international commitments, a level of protection of fundamental rights essentially equivalent to that guaranteed within the EU under the Data Protection Directive read in the light of the EU Charter of Fundamental Rights. On this point, the CJEU observed that the Commission failed to make such a finding, but merely examined the Safe Harbour Scheme.

The Court then considered the deficiencies of the Safe Harbour scheme, observing that the scheme is applicable solely to the U.S. undertakings which adhere to it, and that the U.S. public authorities are not themselves subject to it. From the standpoint of the data privacy/national security balance, the fundamental problem, as the CJEU pointed out, is that the national security, public interest and law enforcement requirements of the U.S. prevail over the Safe Harbour scheme. Thus, the U.S.-EU Safe Harbour Scheme enables interference with the fundamental rights of EU citizens, and the Commission decision does not refer to the existence, in the U.S. of rules intended to limit any such interference or the existence of effective legal protection against the interference. The CJEU cited two EU Commission communications to the European Parliament and Council [560] in support of its own analysis. The two Commission communications indicated that the U.S. authorities were able to access the personal data transferred from EU Member States to the US and process these data in a manner incompatible with the purposes for which they were transferred, beyond what was strictly necessary and proportionate to the protection of national security. Also the Commission noted in its communications that the persons in the EU whose data was being processed in the U.S. had no administrative or judicial means of redress enabling them to access their own data and, as the case may be, have these data rectified or erased.

The CJEU found that the legislation permitting such schemes as the Safe-Harbour Agreement, enabled U.S. public authorities to have access on a generalised basis to the content of electronic communications, and must be

[560] Communication from the Commission to the European Parliament and the Council entitled 'Rebuilding Trust in EU-US Data Flows') COM (2013) 846 final, 27 November 2013) and Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU (COM (2013) 647 final, 27).

regarded as compromising the essence of the fundamental right to respect for private life. It also observed that legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or obtain the erasure of such data, compromises the essence of the fundamental right to effective judicial protection, the existence of such a possibility being inherent in the rule of law. The Court also found that the Safe Harbour Decision denied the national supervisory authorities their powers where a person calls into question whether a decision is compatible with the protection of the privacy and of the fundamental rights of individuals. It held that the EU Commission did not have the competence to restrict the national supervisory authorities in that way. This conclusion was based on the powers and independence of the DPAs guaranteed in the EU Charter of Fundamental Rights, which refers to the DPA's role as being an independent one. In this regard, the CJEU held that that a national supervisory authority 'must be able to examine, with complete independence, whether the transfer of that data complies with the requirements laid down by the directive.'[561] For all of the above reasons, the CJEU declared the Safe Harbour Agreement invalid.

11.3 Consequences of *Schrems v Data Protection Commissioner*

The consequences of the CJEU judgment are that the Irish supervisory authority (The DPA) was required to examine Mr. Schrems' complaint with all due diligence, and, at the conclusion of its investigation to decide whether transfer of the data of Facebook's European subscribers to the US should be suspended on the ground that the U.S. does not afford an adequate level of protection of personal data. In common with the verdict in *Digital Rights Ireland* it appears that the Snowden revelations have had an impact on CJEU thinking in relation to data privacy and fundamental rights, particularly in the context of the ongoing emphasis on the provisions of the EU Charter of Fundamental Rights. While the CJEU judgment referred to Articles 7 and 8 of the Charter with regard to privacy rights, an interesting feature of the judgment was its reliance on Article 47 (the right to an effective remedy and a fair trial). In this connection, the CJEU held that the Safe Harbour Agreement did not comport with the provisions of Article 47 of the Charter, as it did not refer to any U.S. rules or legal safeguards which would serve to limit any U.S.

[561] Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* Judgment of 6 October 2015, at para 57.

interferences with data privacy, an example being the provision of an effective judicial remedy.[562]

As the Safe Harbour Agreement was predicated on a self-certification system, enabling a company to state that it had complied with Safe Harbour principles, the Court deemed this to be inadequate as mechanisms did not exist to identify and sanction non-compliant US companies.[563] Significantly, the CJEU held that the EU Commission is obligated to evaluate any third country's legal arrangements, before making a determination on that country's standards of data protection.[564] In this regard, the Court relied on Article 25 of the Data Protection Directive and in so doing, acknowledged its weight as a data protective instrument in relation to trans-national data transfers. However, this aspect of the verdict has a profound implication - whether by invoking a extraterritorial dimension of data transfers emanating from its interpretation of Article 25 of the Data Protection Directive, the CJEU has potentially exceeded its jurisdiction of adjudication.

Another significant implication which stemmed from the CJEU judgment was the fact that the EU Commission had not engaged in any evaluation of U.S. laws or international commitments when the Safe Harbour Agreement was agreed in 2000.[565] This situation is unlikely to be replicated, but whether the EU would take the significant step of annulling data transfers with the U.S. and other third. countries remains and unlikely prospect, with political pragmatism likely to determine developments in this area.

12.0 Developments following the Invalidation of the Safe Harbour Agreement

As the Safe Harbour Scheme was invalidated, the EU Commission wanted to replace it with a new data transfer scheme. On 2 February 2016, in response to the invalidation by the CJEU of the Safe Harbour Agreement, the European Commission announced an agreement between the EU and the US on a new framework for transatlantic data flows: the EU-US Data Privacy Shield. The Commission announcement claimed that the EU-US Data Privacy Shield

[562] ibid, at paras 81, 89 and 95.
[563] ibid, at para 81.
[564] ibid, at para 83.
[565] ibid.

'reflects the requirements set out by the European Court of Justice in its ruling on 6 October 2015.' The Vice-President of the EU Commission declared that authorities on both sides of the Atlantic had agreed on 'a new strong framework on data flows with the U.S.[566] Under the terms of the Privacy Shield, the U.S. has given written assurances to the EU that the access of public authorities to EU citizens' data for law enforcement and security purposes will be subject to clear limitations, safeguards and oversight mechanisms.[567] The U.S. has ruled out indiscriminate mass surveillance on the personal data transferred to the U.S. under the new arrangement. An annual joint review would monitor the functioning of the Privacy Shield. American companies will self-certify that they meet the requirements laid down in the new framework. [568] The agreement will involve an annual privacy summit with NGOs and stakeholders on developments in the areas of U.S. privacy law and its impact on Europeans.[569]

On April 13, 2016, the Article 29 Data Protection Working Party issued an opinion on the Data Privacy Shield. The Working Party welcomed the 'significant improvements brought by the Privacy Shield compared to the Safe Harbour decision.'[570] However, it is considered that, notwithstanding these improvements 'some key data protection principles as outlined in European law are not specified in the draft adequacy decision, or have been inadequately substituted by alternative motions.'[571] Furthermore, 'the data retention principle is not expressly mentioned and cannot be clearly construed from the current wording of the Data Integrity and Purpose Limitation principle.'[572] Despite the fact that the U.S. has ruled out indiscriminate mass surveillance, representatives of the Article 29 Working Party still declared that an area of concern was 'the possibility that is left in the shield for bulk collection, which, if massive and indiscriminate, is 'not acceptable,'[573] and 'we think that the limits

[566] EU Commission and United States agree on a new framework for transatlantic data flows: EU-US <http://europa.eu/rapid/press-release_IP-16-216_en.htm> accessed 21 October 2016.
[567] ibid.
[568] ibid.
[569] ibid.
[570] Article 29 Working Party. Opinion 01/2016 on the EU-US Privacy Shield draft adequacy decision. 16/EN WP 238. Adopted 13 April 2016, at 2 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf> accessed 29 October 2016.
[571] ibid, at 3.
[572] ibid.
[573] ibid, 40.

are still very broadly defined and can't count as targeted data collection, so it's still indiscriminate and mass data collection.'[574]

After the CJEU invalidated the Safe Harbour arrangement between the EU and the US, Facebook, like many other companies, switched to Standard Contractual Clauses (SCCs) as the new basis for the transfer of EU user data to the U.S. SCCs are template agreements adopted by the European Commission through its decisions 2001/497/EC, 2004/915/EC and 2001/87/EU (the SCC Decisions), which conform to EU law principles and which EU companies can enter into with their foreign counterparts to serve as a basis for transferring personal data.[575]

On the other hand, it might be argued that SCCs are no better that the Safe Harbour Agreement from the point of view of data protection in that they do not prevent generalised surveillance by U.S. State agencies, and are not effectively monitored by a public authority in the U.S. Against this, as Van Overstraten and Entrayhues point out, SCCs are more privacy-protective because (a) they allow better control by European DPAs prior to transfer, at least in those Member States where they are subject to prior formalities, as they are in Belgium and France; (b) they allow better control by European DPAs after transfer as the clauses impose co-operational and audit duties on data

[574] Samuel Gibbs, 'Data Regulators Reject EU-US Privacy Shield safe harbour deal,' *The Guardian* 14 April 2016.

[575] Standard Contractual Clauses ensure that adequate safeguards are provided for the transfer of personal data from the EU to countries outside the EU and serve to minimise the potential of data being disclosed. Standard Contractual Clauses are not compulsory, but offer the advantage that recipients of personal data transferred from a third country outside the European Union/European Economic Area (EEA) is obligated to comply with data protection standards, while Member States' data protection authorities are required to ensure that such transfers conform to such standards, thus according adequate levels of data protection. The Council of the European Union mandates the European Commission, pursuant to Article 26(4) of the Data Protection Directive 95/46/EC, to determine whether Standard Contractual Clauses offer sufficient safeguards with regard to privacy protection, the safeguarding of fundamental rights and freedoms and the provision of corresponding rights relating to data transfers. Two sets of Contractual Clauses have been issued by the European Commission relating to data transfers from data controllers within the EU to data controllers outside the EU or EEA; (Decision 2001/497/EC and Decision 2004/915/EC) and one Decision dealing with data transfers to data processors outside the EU/EEA (Decision 2010/16/EC). On 28 September 2016 The Irish Data Protection Commissioner initiated proceedings seeking a reference to the CJEU to determine the validity of Standard Contractual Clauses relating to data transfers from the EU to the US. The proceedings, *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems* 2016/4890P, commenced on 7 February 2017 in the Commercial Court and ended on 15 March 2017. The judgment is awaited.

importers, and (c) they allow better control by the data-exporting party which has a contractual right to suspend the transfer or terminate the agreement.[576]

International data flows between Europe and the U.S.-EU Privacy Shield engagement, as well as the SCC Model Clauses, were called into question following an announcement by Maximilian Schrems that he had received the draft decision by the Irish Data Protection Commissioner on 25 May 2016 informing him that the Commissioner intended to file the necessary proceedings within days with the Irish Courts, challenging the validity of the Standard Contractual Clauses, on foot of a complaint by Schrems that under current EU case law it was 'highly unlikely that Facebook Ireland 'could continue sharing data with the U.S. authorities.' [577] In a statement provided to *The Privacy Advisor*, which reports on the latest privacy developments, the Irish D.P.C. said that having 'thoroughly and diligently' investigated the Schrems complaint, he had informed both Schrems and Facebook of 'our intention to seek declaratory relief in the Irish High Court and a referral to the CJEU to determine the legal status of data transfers under Standard Contractual Clauses.'[578] Schrems commented that he could see no way that the CJEU can say that SSCs are valid, 'if they liked Safe Harbour,' based on the existence of what he called 'far-reaching U.S. Surveillance'.[579]

Although the US has pledged to adhere to the EU's commitment for high standards of data protection, Lam predicts that this pledge is unlikely to be fulfilled, but does not foresee a suspension of EU-US data transfers on the initiative of the EU, due to what he refers to as the EU's economic dependence of the US.[580] Accordingly, it might be the case that the EU will ultimately not

[576] Tanguy Van Oversttaeten and Alexandre Entraygues, 'The European Court of Justice to rule on the validity of standard contractual clauses' *Linklaters* 30 May, 2016, 1,2. <http://www.linklaters.com/pdfs/mkt/brussels/160530_Alert_The_European_Court_of_Justice_to_rule_on-the_validity_of_standard_contractual_clauses.pdf.> accessed 29 September 2016.
[577] Europe v Facebook, Press Release of 26 May, 2016. Cited in: 'Europe vs. Facebook: Austrian activist wins another legal battle over data protection' *RT* (26 May, 2016) <https://www.rt.com/news/344519-europe-vs-facebook-austrian-activist/> accessed 28 August 2016.
[578] Jedidiah Bracy, 'Model clauses in jeopardy with Irish DPA referral to CJEU' *The Privacy Advisor*, 25.5.2016. <https://iapp.org/news/a/model-clauses-in-jeopardy-with-irish-dpa-referral-to-cjeu/> accessed 23 July 2016.
[579] ibid.
[580] Christina Lam, 'Unsafe Harbor: The European Union's Demand For Heightened Data Privacy Standards In Schrems v Irish Data Protection Commissioner' 40(3) (2017) *Boston College International and Comparative Law Review* 1, 13.

be able to ensure compliance with its data protection standards on a worldwide scale, [581] although such compliance might constitute the best approach to harmonising EU and US privacy protection regimes.[582]

13.0 Impact of the CJEU decisions in the *Digital Rights Ireland*, *Google Spain*, and *Schrems* cases on the data privacy/national security balance

As has been suggested above,[583] the Snowden revelations have been influential in encouraging the CJEU in its robust review of legislation governing the processing of personal data by private and public bodies. The decision in *Digital Rights Ireland* [584] has been of particular significance in this regard, in that it has facilitated the enhanced protection of data privacy in any future EU legislation involving data surveillance, and thus adjusted the data privacy/national security balance in favour of the former. Thus, the Snowden revelations, the *Google Spain* and the *Schrems* judgments, have helped to foster a growing demand in Europe for the effective protection of personal data. The *Digital Rights Ireland* [585] verdict has weakened the cause of those who had resisted legal reform of measures which the CJEU found were incompatible with the EU Charter of Fundamental Rights, a constitutional instrument which, in the hands of the CJEU, supports an advanced standard of protection for personal data throughout the EU. The data privacy/national security balancing paradigm will still remain, but given the increased protection available to data privacy since the Charter of Fundamental Rights became legally binding on Member States and institutions when acting within the scope of EU law, the balancing exercise will have to take due account of the centrality of data protection rights in the post-2009 legal order of the EU.[586]

14.0 The Alternative Data Privacy/National Security Balance: Circumventing Data Privacy Protections in the EU: The Mass Surveillance of Personal Data by Spy Agencies in some EU Member States

In his concurring opinion in *Roman Zaharov v Russia* (2015) Judge Dedov the Russian representative on the Court, echoed doubts expressed by the Russian

[581] ibid, 13.
[582] This point is developed in the Conclusion to the thesis.
[583] Nóra Ní Loideáin, 'EU Law and Mass Internet Surveillance in the post-Snowden Era' 3(2) (2015) *Media and Communication Data* 53.
[584] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others*. Grand Chamber CJEU, 8 April 2014.
[585] ibid.
[586] See Stefano Rodotà 'Data Protection as a Fundamental Right' in Serge Gutwith et al, (eds), *Reinventing Data Protection*? (Springer, New York, 2009) 77-82.

Government as to the competence of the ECtHR to examine the quality and effectiveness of the domestic law *in abstracto* without the applicant's victim status being established and without determining that there had been interference with his right to respect for his private life in practice, and not merely theoretically. He remarked that this approach had been used by the ECtHR in interception cases against two prominent democratic states: the United Kingdom and the Federal Republic of Germany. In these two cases - *Kennedy v United Kingdom* (2010) and *Klass and Others v Germany* (1978), the Court confirmed the effectiveness of the relevant domestic systems against arbitrariness. However, Judge Dedov found it regrettable that 'both of these States had recently been involved in major, well publicised surveillance scandals.[587] Firstly, the mobile telephone conversations of the Federal Chancellor of Germany were unlawfully intercepted by the National Secret Service, and secondly, the United Kingdom authorities provided a United States secret service agency with access to, and information about, the United Kingdom's entire communications database, with the result that the U.S. authorities were able to interpret the personal data of all United Kingdom citizens without any appropriate domestic safeguards at all.[588] Judge Dedov's conclusion was that his two examples, British and German, indicated that something was wrong with the approach of the ECtHR to breach of privacy cases from the very outset.

However, the two examples cited by Dedov were part of a much wider phenomenon: the freedom enjoyed by national secret service agencies throughout Europe to intercept the private communications of citizens, sometimes with, as in the case of the U.K. and sometimes without, as in the case of Germany, the connivance of state authorities. In 2016, the after *Zakharov* was decided, the United Kingdom Investigatory Powers Tribunal, the only Court that hears complaints against U.K. security agencies, such as MI5, MI6 and GCHQ, found that these had operated an illegal regime to collect vast amounts of communication data, tracking individual phone and web use and other confidential personal information, without adequate safeguards or

[587] *Roman Zakharov v Russia* Application No. 47143/06, 4 December 2015, 83-89.
[588] ibid.

supervision for 17 years.[589] When the Investigatory Powers Tribunal described the regime governing the collection of bulk communications data as illegal, it meant that it failed to comply with Article 8, ECHR which protected the right to the privacy of such data, and that it was in contravention of the terms of this Article between 1998, when this collection started, and 4 November 2015, when it was made public. The Tribunal also found that the retention of bulk person databases (BPD), which might include medical and tax records, individual biographical details, commercial and financial activities, communications and travel data, also failed to comply with Article 8 of the ECHR for the decade it was in operation until it was publicly acknowledged.

Information supplied by Edward Snowden from 2013 onwards, has indicated that the British Government Communications Headquarters (GCHQ) has been actively cooperating with the NSA in the exchange of data. The GCHQ has been accessing and processing its data under a programme named TEMPORA. Reports indicate that there is a further European dimension to U.S. surveillance activities. These reports implicate at least three other EU Member States: Sweden, France and Germany and suggest that these States may be operating their own large-scale Internet interception programmes and, like Great Britain through its GCHQ, exchanging the personal data of European citizens with the NSA.[590]

The *CEPS Report* of 2013, a study commissioned as a briefing paper by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, which examined the data surveillance activities in five EU States - the UK, France, Germany, Sweden and Holland, found that the evidence suggested that the U.K. government 'is engaged by far in the most extensive large-scale surveillance activities in the EU.' [591] The Report, relying on expert testimony, concludes that Sweden is becoming an increasingly important partner in the global intelligence network. Intelligence operations in Sweden are the responsibility of the National Defence Radio Establishment (FRA), which is

[589] Alan Travis, Home Affairs, *The Guardian* 17 October 2016.
[590] Adam Entous and Siobhan Gorman, 'Europeans Shared Spy Data With U.S.' *The Wall Street Journal* 29 October, 2013.
[591] Didier Bigo et al, 'Mass Surveillance of personal Data by EU Member States and its Compatibility with EU Law' 61 (2013) CEPS Paper in Liberty and Security 1 39. Henceforth cited as CEPS Paper.

reported to have engaged in operations and programmes for the mass collection of personal data, 'with features that resemble in part those pursued by the U.S. NSA and the UK GCHQ. However, Sweden's new Internet laws passed in 2008 (the FRA law) authorised the FRA to monitor all cable-bound communications traffic in and out of Sweden, including e-mails, text messages and telephone calls.[592] It is now believed that FRA is intercepting and storing communication data from fibre-optic cables crossing Swedish borders from the Baltic Sea.[593] Campbell also stated that the FRA had become a new and important member of the 'Five Eyes,' and is believed to be 'the biggest collaborating member of GCHQ outside the English-speaking countries,' having access to cables from the Baltic States and Russia, hitherto inaccessible to the 'Five Eyes' organisation.[594]

The evidence indicates that the FRA has been operating programmes for the 'upstream' collection of private data, 'collecting both the content of messages as well as metadata of communications crossing Swedish borders.' [595] The metadata are retained in bulk and stored in a database known as 'Titan' for a period of 18 months.[596] There is evidence that the FRA may be sharing substantial quantities of data it collects with foreign intelligence services, including the NSA: Swedish legislation allows for the bulk transfer of data to other states if authorised by the Government. Swedish authorities 'have made use of this possibility through the exchange of raw data with the U.S. as well as with the Baltic States.[597]

Experts consulted for the CEPS study claimed that France now ranks fifth in the world of metadata collection after the U.S., the U.K., Israel and China, and operates the second most important intelligence data collection processing centre in Europe after the U.K. This has been publicly acknowledged by the head of the main intelligence agency in France, the DGSE.[598] The metadata

[592] Ronald Deibert et al (eds), *Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace'* (Massachusetts Institute of Technology, 2010) 331-32.
[593] Statement by Duncan Campbell at the European Parliament's LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens, First Hearing, 5 September, 2013.
[594] Cited in CEPS Paper 47.
[595] CEPS Paper. The practice of 'upstreaming' involves tapping directly in the communications infrastructure as a means of intercepting data.
[596] ibid.
[597] ibid, 47
[598] ibid.

centre operated by the DGSE forms an 'intelligence platform' that feeds the six principal intelligence, defence and law enforcement bodies in France. The DGSE specialises in communication interception and cryptography to the benefit of the entire intelligence community. These bodies send their requests to the DGSE which, having searched its massive database, forwards intelligence reports on the basis of the data it has analysed. This work is, according to an expert informant of the CEPS, 'carried out routinely, discretely and without any form of parliamentary control.'[599]

The French intelligence services engage in cooperation with many foreign intelligence services. The Head of the DGSE told the French Parliament that his agency was working with more than 200 foreign services, in 'frequent' cooperation with 50 of these, and in 'intense' cooperation with 10. He added that, on the initiative of the U.S.A., Western intelligence services had set up a database allowing each nation to obtain immediate access to all the information gathered. These statements by the head of the DGSE supplement disclosures by *The Washington Post* in 2005 that France has been hosting a secret intelligence centre in Paris named 'Atlantic Base' where six countries, namely USA, U.K., France, Germany, Canada and Australia, routinely exchange information.[600]

France

While French law strictly regulates security intercepts authorised by the Prime Minister on the advice of the National Advisory Commission on Security Intercepts, there is a gap in the legal framework regarding the large-scale interception and storage of data, leaving a degree of legal uncertainty which the intelligence services appear to have exploited. [601] A senior member of the intelligence services interviewed by *Le Monde* journalists was reported as having claimed that collection of metadata by the DGSE is not illegal but 'alegal' - conducted outside the law. [602] The CEPS paper notes that two French NGOs, the International Federation of Human Rights and the League of Human Rights have jointly claimed that infringements of personal liberties have been perpetrated through automatic data processing. On the basis of the

[599] ibid, 50.
[600] Diana Priest, 'Help from France In Covert Operations' *The Washington Post* 3 July, 2005.
[601] CEPS Paper, 51.
[602] J. Follorou and F. Johannes, 'Révélations sur le Big Brother francais, *Le Monde*, 4 July, 2013. <www.lemonde.fr> accessed 28 August 2015.

French criminal code, they challenge 'the fraudulent access to an automated data processing system, collection of personal data by fraudulent means, wilful violation of the intimacy of private life and the use and conservation of recordings and documents obtained through such means.'[603] In response to these privacy concerns, the French prosecutor's office opened a preliminary inquiry.[604] As of May 2015, a determination in relation to the inquiry had not emerged.[605] However, in 2015, The Intelligence Act was passed, and according to the then French Premier Manuel Valls, it had 'nothing to do with the practices revealed by Edward Snowden.' [606] The Act widened the basis upon which surveillance can be undertaken in the public interest, and mandated a surveillance programme developed in 2008 to tap into international cables.[607] Moreover, an oversight commission comprising judges and members of parliament was established, with a deadline of twenty-four hours to give non-binding opinions in relation to authorisation requests.[608] Additionally, a redress procedure was also created. However, Tréguer comments that 'the procedure is veiled in secrecy' and 'fails to respect defence rights' and 'echoes the law of the US and the UK.'[609]

Germany

Evidence gathered for the CEPS Paper on the activities of the German Intelligence Services indicates that Germany has been engaging in large-scale surveillance of communications data. This activity is linked to a network of exchange and transfer of data to both domestic intelligence and law enforcement agencies and international partners, despite what the report calls 'the existence of a strong constitutional and legal framework for the protection of privacy.' [610] The three main German intelligence Agencies are legally authorised to search up to 20% of communications having a foreign element,

[603] CEPS Paper, at 52.
[604] C. Lable and N. Vincour, 'French Prosecutor Investigates U.S. Prism spying scheme' *Reuters* 28 August 2013. <http://www.reuters.com/article/2013/08/28/us-usa-security-france-idUSBRE97R0WE20130828> accessed 6 June 2015.
[605] (--------) 'NSA/Surveillance: Damning new revelations and still no judicial inquiry' *fidh Worldwide Movement For Human Rights* <https://www.fidh.org/en/region/europe-central-asia/france/nsa-surveillance-damning-new-revelations-and-still-no-judicial. accessed 16 June, 2017.
[606] Félix Tréguer, 'Intelligence Reform and the Snowden Paradox: The Case of France' *Media and Communication* 5(1) (2017) 17, 23.
[607] ibid.
[608] ibid.
[609] ibid.
[610] CEPS Paper, 52.

for a specific purpose, such as the fight against terrorism or the protection of the Constitution. Reports publishing the Snowden revelations indicate that the German Intelligence Service (BND):

> [D]ay after day and month after month, passes on to the NSA massive amounts of connection data relating to the communications it had placed under surveillance. The so-called metadata - telephone numbers, e-mail addresses, IP connections - then flow into the Americans' giant databases.[611]

The main federal law in Germany regulating communications surveillance is the G-10 law, which allows for specific limitations to the secrecy of communications as provided in Article 10 of the Constitution. Under the G-10 law, the intelligence services may operate warrantless automated wiretaps of domestic and international communications for purposes such as the fight against terrorism or the protection of the Constitution. The G-10 law was amended in 1994 and 2001 to add electronic and voice communications to the list of communications that intelligence agencies may monitor. However, two significant decisions of the German Federal Constitutional Court have limited the scope of the G-10 law. In March 2004, the Court ruled that the G-10 law regulating communications surveillance infringed the German Constitution, especially Article 1 on human dignity and Article 13 on the inviolability of private homes. The Court also heard that certain communications, such as the contacts with close family members, doctors, priests or lawyers are protected by an absolute area of intimacy that no government may infringe.[612] In February 2008, the Court ruled that certain provisions of the law of North-Rhine Westphalia were unconstitutional. This law allowed the regional office for the protection of the Constitution to gather data secretly on private computers. The Court interpreted Articles 1 and 2 of the German Constitution as containing a fundamental right for every citizen to have the integrity and confidentiality of IT systems guaranteed by the States.[613]

---

[611] Hubert Gude, Laura Poitras and Marcel Rosenbach, 'Mass Data: Transfers from Germany Aid U.S. Surveillance' *Spiegel Online*, 5 August, 2013. <http://www.spiegel.de/international/world/german-intelligence-sends-massive-amounts-of data-to-the-nsa-a-914821.html> accessed 5 June, 2015.
[612] Federal Constitutional Court, Decision of 3 March 2004, Reference No. 1 BVR, 2387/98.
[613] Federal Constitutional Court decision of 27 February, 2008. Reference No. 1 BVR. 370/07.

The German oversight system for controlling the activities of German Intelligence Services has elements of transparency and credibility lacking in the other countries so far mentioned. Two oversight bodies exist at Parliamentary level. The first, the G-10 Committee of the Bundestag, has the task of determining the necessity and legitimacy of the measures taken by the Intelligence Agencies which could infringe upon the fundamental rights enshrined in Article 10 of the German Constitution. The G-10 Committee, composed of 4 members of Parliament, is called upon to act when an Intelligence service makes an official request for a surveillance measure to the German Ministry of the Interior and this request is granted. The committee follows the entire procedure, including the collection of personal data, its analysis and use. It also checks whether fundamental rights of German citizens have been violated following individual complaints. Compared with oversight authorities in the USA, the U.K., Sweden and France, 'Germany is the only case in which the oversight body not only authorizes programmes but holds responsibility for their implementation and holds investigative powers.'[614] Another oversight body, the PKGr, is responsible for controlling the three federal intelligence services. The German Government is obliged to provide all relevant information on the activities of the Intelligence Agencies to the 11 members of the PKGr, who are all members of the Bundestag. A report on the 2011 activities of the BND, show, that more than 2.9 million e-mails and text messages have been the subject of surveillance measures.[615] Notwithstanding the relatively robust system of oversight operating in Germany, data protection bodies at federal and regional levels in a joint statement following the Snowden revelations,, called for the control powers of the oversight bodies, the G-10 Committee and PKGr, to be enhanced, and their links with data protection authorities strengthened.[616]

[614] Stefan Heuman and Ben Scott, 'Law and Policy in Internet Surveillance Programs: United States, Great Britain and Germany' *Impulse* September 2013, 15. <https://netzpolitik.org/wp-upload/Nr.25_Law_and_Policy_in_Internet_Surveillance_Programs.pdf> accessed June 7, 2015.

[615] 'The German PRISM: Berlin Wants to Spy Too' *Spiegel Online International* (17 June 2013). <http://www.spiegel.de/international/germany/berlin-profits-from-us-spying-program-and-is-planning-its-own-a-906129.html> accessed 6 June 2015.

[616] See <http://www.bfdi.bund.de/SharedDocs/Publikationen/Entschliessungssammlung/DSBundLaender/05092013_EntschliessungUeberwachungDurchNachrichtendienste.pdf?__blob=publicationFile> Cited in CEPS Paper, 72, fn 257.

The *CEPS Report* found that the surveillance programmes it examined in EU Member States were 'incompatible with minimum democratic rule of law standards derived from the EU Charter of Fundamental Rights and the European Convention on Human Rights,' adding that 'the principles enshrined in the Charter and the Convention are essential components of the Constitutional tradition of the States in question.'[617] Among other criticisms made in the report are that Member States' surveillance programmes jeopardise the privacy of EU nationals as data owners; that they jeopardise the EU principle of 'sincere cooperation' enshrined in Article 4.3 of the Treaty on the European Union; that large-scale electronic surveillance blurs the line between national sovereignty and matters of EU competence, and that the boundary between domestic and foreign interception is blurred by data exchange among intelligence services.[618]

One major problem arises from the transnational programmes linking the U.S. National Security Agency with a number of European Intelligence services and facilitating data exchange. Part of the problem stems from the fact that under European law, individuals have ownership of their data, while under U.S. law ownership rests with the company or service that assembled the data. Thus, transnational programmes facilitating the transmission of Europeans' data to the NSA, for example, could be deemed a theft of correspondence, in addition to involving potentially illegal access, collection and processing of data, if this has been done without the authorisation and/or knowledge of the national authorities in charge of the management of these electronic data. Only the national authorities may authorise derogations of national security on foot of existing bilateral, European and international agreements.

Edward Snowden's disclosures and subsequent and similar ones, have necessitated a new approach to the privacy/security balance in Europe [619] and raised a number of significant new questions. At this point, few doubt that the NSA, having direct access to the servers of U.S.-based Internet giants is able to read, record and store almost every type of digital communication worldwide.

[617] CEPS Paper, 19.
[618] ibid.
[619] Barney Henderson, (ed), 'Angela Merkel rebukes US and Britain over NSA surveillance' *The Telegraph* 29 January, 2014.

As Snowden disclosed this information from 2013 onwards, 'the public discovered that the Americans have a preference for spying on Germany - more so than any other country in Europe.'[620] Among the questions raised for EU citizens by the NSA's PRISM programme [621] and its employment of unprecedented technical expertise to compromise European privacy rights through secret surveillance, is how a country like Germany can permit its citizens to be spied on by an agency of another country. One answer to the question was that of Dieter Deiseroth, a judge at Germany's Federal Administrative Court, who contended that 'when foreign agencies infringe upon fundamental rights on Germany territory, the state cannot look away. Accepting the massive collection of private information would be a serious violation of the principle that every state has to defend such rights.' [622] An alternative view is that of Claus Arndt, a legal expert who served from 1968 to 1989 on the Bundestag's 9-10 Commission, a body charged with the oversight of intelligence measures taken by German security agencies. Arndt claimed that senior German politicians have never made an issue of surveillance by the Americans and that they all 'did their best to stick their heads in the sand.' [623]

German politicians were far from being the only Europeans to acquiesce in U.S. surveillance of the data of European citizens. In 2013, the year of the Snowden revelations, it became known that the Obama Administration had successfully lobbied the EU Commission to scrap a data-protection measure that would have substantially reduced the capacity of the NSA and other U.S. Intelligence agencies to obtain personal data on Europeans without their knowledge or consent. The measure was known within the EU as the 'anti-FISA clause.' This was in reference to the U.S. Foreign Intelligence Surveillance Act that authorises the U.S. Government to eavesdrop on

[620] 'The German PRISM: Berlin Wants to Spy Too' *Spiegel Online International* (17 June 2013) <http://www.spiegel.de/international/germany/berlin-profits-from-us-spying-program-and-is-planning-its-own-a-906129.html> accessed 6 June 2015.
[621] A classified programme which routes e-mails, instant messages and other digital communications to the NSA, which are obtained from nine online platforms; Microsoft, Google, Facebook, Yahoo, YouTube, Skype, AOL, Apple and PalTalk. PRIMS enables the NSA to obtain the content, in addition to the metadata attaching to such communications. See Barton Gellman and Laura Poitras, *'U.S., British intelligence mining data from nine U.S. Internet companies' The Washington Post* (June 7, 2013).
[622] 'The German PRISM: Berlin Wants to Spy Too' *Spiegel Online International* (17 June 2013) <http://www.spiegel.de/international/germany/berlin-profits-from-us-spying-program-and-is-planning-its-own-a-906129.html> accessed 6 June 2015.
[623] ibid.

international phone calls and e-mails. The proposed EU measure would have nullified any U.S. request for technology and telecoms companies to hand over data on EU citizens. Details of the proposed measure and of successful U.S. diplomatic and political campaign to abort it are disclosed in documents obtained by the *Financial Times*.[624] The documents reveal that leading U.S. technology companies,

> [W]ho had worked closely with the Obama administration in trying to weaken EU data protection legislation were also fearful of the measure, since it would have forced them to choose between two competing government mandates - the U.S. demand for data and the EU law forbidding it. [625]

The chief privacy officer of one of the largest U.S. technology groups foresaw a 'nightmare' for all of these groups if the EU legislation had been passed: 'There would have been a conflict with any FISA request made by the U.S. government.' [626] The U.S. diplomats and politicians who lobbied the EU authorities to abort the data-protection legislation deployed the argument, which the EU Commission found compelling, that dropping the legislation would smooth the way ahead of talks on the trans-Atlantic free trade agreement, since the EU 'didn't want any complications on that front.' [627]

A large majority of EU Commissioners opposed the data-privacy protection measure arguing that it would have little legal weight, since most data servers of large technology companies holding information on EU citizens are in the U.S. Another argument was that enhancing data protection in Europe meant 'needlessly antagonising Europe's most important ally.'[628] However, the decision of the EU Commission to discard the data protection measure, combined with the revelation that PRISM enables the NSA to access users'

---

[624] Jason Fontella-Khan and Peter Spiegel, 'Washington Pushed EU to dilute data protection' *Financial Times* June 12, 2013.
[625] ibid.
[626] ibid.
[627] 'EU Weakens Data Protection at U.S. Request' *Spiegel Online* 13 June, 2013) <http://www.spiegel.de/international/world/eu-weakened-data-protection-laws-ahead-of-prism-spy-program-a-905520.html> accessed 1 June 2015.
[628] Jason Fontella-Khan and Peter Spiegel, 'Washington Pushed EU to dilute data protection' *Financial Times* June 12, 2013.

data across the globe, has meant that European technology companies are concerned that without the kind of data protection measurers originally planned by the EU, 'technologies such as cloud computing - because most of the servers are in the U.S. - will not take off in Europe out of concern that Washington will have easy access to that information.' [629]

15.0 Two Parallel Systems of Surveillance

The information gleaned by the European Parliament's Committee on Civil Liberties and Home Affairs (LIBE), the work of investigative journalists published mainly in *The Guardian* newspaper and the post-2013 revelations of Edward Snowden, between them provide significant details about surveillance systems in a number of European countries, in which spy agencies and security services collect the communications data of citizens without regard to the legal constraints on this activity, and without knowledge of those whose data are being collected. In the context of the data privacy/national security balance, two parallel systems impacting on this balance are in operation in some major European States. One is a system of laws, governing the circumstances in which governments may legitimately interfere, in the interests of national security, with legally protected privacy rights, subject to the oversight of the European Courts, the CJEU and the ECtHR. Legal regulation of the communications surveillance conducted by the security services varies from one state to another, but in general, research has revealed that legal frameworks are characterised by ambiguity or loopholes when large-scale communications surveillance is in question, while national oversight lacks the capacity to monitor effectively the lawfulness of intelligence services' large-scale interception of data.

There can be little doubt that this interception was sometimes on a massive scale. For example, 'upstream' (tapping directly into the communications infrastructure as a means of intercepting data) featured in the surveillance programmes of all the states surveyed in the LIBE study: the United Kingdom, France and Germany. A report on the GCHQ's Tempora programme alleged that the United Kingdom intelligence service had placed interceptors on

[629] 'The German PRISM: Berlin Wants to Spy Too' *Spiegel Online International* (17 June 2013). <http://www.spiegel.de/international/germany/berlin-profits-from-us-spying-program-and-is-planning-its-own-a-906129.html> accessed 6 June 2015.

approximately 2,000 undersea fibre-optic cables close to the south-west coast of Britain.[630] The same report mentioned Sweden's operations for the 'upstream' collection of private data: this featured the interception of communications data and metadata from fibre-optic cables crossing Swedish borders from the Baltic Sea.

The consequences of these secret surveillances are considerable. They impact on the daily lives of all the individuals living in Europe when they use Internet services (e-mail, social networks via personal computers or mobile services. Some governments in the EU were kept unaware of the surveillance activities while their citizens were subject to them. They were also kept secret from companies and branches of government affected by them. In general, they are on a scale beyond what was previously called 'targeted surveillance'.

The LIBE study suggests that the controversy over large-scale harvesting of personal data has to be understood along a continuum of intelligence service activities. Three of the surveillance activities outlined in this continuum might be said to conform to the European legal norms governing the data privacy/national security balance: (a) Counter-terrorism activities that follow a criminal justice logic. (b) Counter-terrorism activities that try to monitor the future by profiling suspects. (c) Cyber activities that target specific groups in a militarily strategic approach.

The fourth surveillance activity falls outside the legal norms governing the privacy/security balance. This is electronic mass surveillance activities carried out without clear objectives, and thus distinct from selective, targeted surveillance. Activity that goes beyond targeted surveillance can lead to data mining and compromise the data privacy rights of entire populations. It is the purpose and scales of surveillance that differentiate democratic regimes from police states. A basic point made in the LIBE study is that an analysis of the surveillance programmes in its report to the European Parliament cannot be reduced to a question of a balance between data protection and national

[630] Ewan MacAskill et al, 'GCHQ taps fibre-optic cables for secret access to world's communications' *The Guardian* 21 June, 2013.

security (since the programmes are not designed to achieve such a balance), but this balance has to be framed in terms of collective freedoms and democracy.

The question then arises: what modalities of action are available to EU and COE institutions, which foster a democratic rule of law framework where fundamental human rights, including the data privacy of European citizens and judicial oversight constitute key norms to counter unlawful large-scale surveillance by member countries. One obstacle facing the EU and COE institutions in this regard is that activities of intelligence services in individual EU States are the sole responsibility of each state. They are covered by Articles 4(2) and 72 of the Treaty of the European Union which reserve intelligence activities to the Member States exclusively. This might suggest that those involved in mass surveillance are outside the remit of COE and EU intervention. However, the LIBE Report suggests that this is not necessarily the case, and that both the European Convention on Human Rights and the EU Charter of Fundamental Rights could play a significant role here, especially given the fact that from a legal point of view, some EU Member States' programmes are incompatible with minimum democratic standards and compromise the fundamental rights of citizens and residents of Europe.

16.0 The Council of Europe Versus The European Union: Which Regime Provides Greater Protection For Data Privacy Rights?

This is a complex question, mainly because the major instrument of Council of Europe primary law, from the perspective of the human right to privacy, and by extension to data privacy, the European Convention for the Protection of Human tights and Fundamental Freedoms (the ECHR), was to exert an influence on the most significant instrument of European Union primary law dealing with data privacy. This was the Charter of Fundamental Rights of the European Union (2000). This influence is acknowledged in the official journal of the European Communities, to which the European Union (EU) became the legal successor.[631] Thus, the human rights protected by the ECHR, including the right to the protection of personal data, were transposed into the primary

[631] 'The European Parliament, Council and Commission stress the prime importance they attach to the protection of fundamental rights, as derived in particular from the Constitution of Member States and the European Convention for the Protection of Human Rights and Fundamental Freedoms.' Official Journal of The European Communities, 103, 27 April, 1977, 1.

law of the EU, and mediated in the jurisprudence of the EU Court of Justice (the CJEU). This has been highlighted in the case-law of the CJEU.[632]

The right to privacy provisions in the EU Charter of Fundamental Rights mirror, and sometimes even copy, word for word, the equivalent provisions of the ECHR. Article 52 of the Charter stipulates that the meaning and scope of Charter Rights which correspond to ECHR rights are to be the same as those laid down by the ECHR. It is therefore not surprising that the Council of Europe Court, the ECtHR, has accommodated EU law and the jurisprudence of the CJEU in many of its judgments.[633] The proportionality principle, a key element of the ECtHR data privacy/national security balancing paradigm, appears throughout the EU Data Protection Directive (Directive 95/46/EC). It has been estimated that approximately half of the substantive provisions of the EU Charter find their equivalent in the ECHR, or the case law of the ECtHR.[634]

Given the profound influence of the privacy rights provisions of the ECHR on those of the European Union, it is reasonable to assert that the Council of Europe, through the ECHR initially at least, offered the greater protection to data privacy rights. However, from 2009 onwards, when the Treaty of Lisbon became the controlling instrument of EU primary law, the EU began to assert itself as the dominant advocate for European privacy rights. Article 6(1) of the Lisbon Treaty recognised the ECHR as having the same legal status as EU Treaties, thus making it an integral of EU primary law and giving it binding legal force, and thereby colonising the ECHR. However, at the same time, Article 6(2) of the Lisbon Treaty declared that the EU 'shall accede to the ECHR.'

A plausible interpretation of this colonising process is that it was part of a long-term project by EU agencies to bring about the emergence of the CJEU as the major European human rights Court. After the EU Charter of Fundamental

[632] See, for example, the reference to the 'special significance' of the ECHR in Case C-305/05 *Ordre des Barreaux Francophones and Germanophone And Others v Council of Ministers* Grand Chamber 26 June, 2007, at para 29.
[633] Paul Craig and Gráinne de Búrca, *EU Law: Texts, Cases and Materials* (Sixth edn, Oxford University Press, 2001) 386, fn 30.
[634] Marie-Luce Paris, 'Paving the Way: Adjustment of Systems and Mutual Influences Between the European Court of Human Rights and European Law Before Accession' 51(1) (2014) *The Irish Jurist* 1, 10.

Rights became part of primary EU law in 2009, the CJEU, in its jurisprudence, moderated its deference to the provisions of the ECHR, as it strove for greater autonomy as a specifically EU Court. The CJEU indicated its reluctance to embrace the project decreed in Article 6(2) of the Lisbon Treaty that the EU should accede to the ECHR, which would mean that individuals whose ECHR rights had been breached by acts of the EU would be able to seek redress before the ECtHR, thus making EU legal acts subject to review under the ECHR system. As a token of this reluctance, the CJEU tended to rely increasingly on the Charter of Fundamental Rights without reference to the ECHR.[635]

These developments must be viewed against the background of a long-standing debate since the 1970s. This debate centred on a vision of an integrated pan-European system of human rights protection, embracing the Council of Europe and the European Union. This system would have involved the ECtHR, with its record of expertise and stature as a human rights Court, exercising this function for all of Europe. The CJEU would not act as a parallel or rival human rights court, thus leaving the sphere of human rights to the exclusive jurisdiction of the ECtHR.[636]

This scheme was endorsed by the European Commission on the basis that it would help to develop a common culture of fundamental rights in the EU, and reinforce the credibility of the human rights system of the EU. A Draft Agreement on the accession of the EU to the ECHR took three years to complete. However, the CJEU asserted itself, and in a December 2014 opinion on the Draft Agreement, it decided that it was incompatible with the EU Treaties.[637] This Opinion, binding on EU Member States and EU institutions, represents a further step by the CJEU in its project of preserving and furthering

[635] Gráinne de Búrca 'After the EU Charter of Fundamental Rights: The Court of Justice as a Human Rights Adjudicator?' 20(2) (2013) *Maastricht Journal of European and Comparative Law* 168, 175.

[636] Oddný Mjöll Arnardóttir and Antoine Buyse - *Shifting centres of gravity in human rights protection : rethinking relations between the ECHR, EU, and national legal orders* (Routledge, 2016) 5. See also Paul Craig and Gráinne de Búrca, *EU Law: Texts, Cases and Materials* (Sixth edn, Oxford University Press, 2011), 419-420.

[637] Opinion Pursuant to Article 218 (11) TFEU, C-2/13. December 18 2014 <http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d5498e825298f346e99568a78451b88b99.e34KaxiLc3eQc40LaxqMbN4Pa3mSe0?text=&docid=160882&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=432736> accessed 7 September 2016.

its privileged position as the primary defender of human rights, including data privacy rights, in Europe. Its engagement with the *Digital Rights Ireland* case, and its groundbreaking decision of April 2014[638] in this case, represents its growing dominance as a defender of human rights in Europe. This dominance has been reinstated in the verdict of the CJEU in Tele2/Watson.[639]

However, while the CJEU was consolidating its position as the primary defender of the data privacy rights of European citizens, the ECtHR engaged in restricting the freedom exercised by European State agencies to intercept the private communications of citizens. One interesting line of ECHR case law arises from the interference with an individual's private life by State authorities in the interest of national security. The cases in this category involved applicants who did not have concrete proof that they had been subject to surveillance, but who claimed that the mere existence of a secret system of surveillance, as distinct from its use in respect of them, violated their rights under article 8 of the ECHR. In *Klass and Others v Federal Republic of Germany*,[640] the ECtHR held that in the very existence of secret surveillance legislation, which was involved for all those to whom it could be applied, represented an abuse of their right to respect from their private and family life under Article 8 (1) ECHR.

The ECtHR, in a number of similar cases, gave individuals the opportunity to challenge secret surveillance laws *in abstracto*: in other words, when such individuals could not furnish any proof that they had been targets of such surveillance. The Court's departure from its customary procedure and for considering some cases *in abstracto* is explained in its decision in *Kennedy v The United Kingdom.*[641] Here, the Court held that an Applicant could challenge secret surveillance legislation on the basis that, at the material time, he was potentially at risk of being subjected to such measures and that remedies against abuse provided by domestic law are inadequate.[642] The ECtHR wanted to ensure that the secrecy of surveillance measures did not result in their being

[638] Joined Cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others*. Grand Chamber CJEU, 8 April 2014.
[639] Case C-203/15 *Tele 2 Severige and Watson* (Grand Chamber) 21 December, 2016.
[640] 2 E.H.R.R., 214 (1979-80), at para 41.
[641] Application No. 26859/05 (2010).
[642] ibid, at para 128.

unchallengeable and outside the supervision of national judicial authorities as well as that of the ECtHR.

The case of *Zakharov v Russia* [643] provides a good illustration of the primary protection afforded by the ECtHR. The applicant, Zakharov, was a campaigner for media freedom and the rights of journalists. In Russia, a system of secret surveillance required operators to intercept mobile telephone communications. Following unsuccessful attempts to challenge this practice at local level, the matter was brought before the ECtHR. Zakharov argued that the laws governing the monitoring of mobile phones infringed his right to private life guaranteed by Article 8(1) ECHR, that the elements of these laws were not accessible and that contrary to Article 13, ECHR, no effective remedies were available under Russian law.[644]

Although the Russian authorities gave evidence that Zakharov had not been subjected to surveillance, the Court found a wide range of defects in the Russian regulatory framework, following its exhaustive investigation of every robust provision of Russian surveillance law, and how these provisions had been applied in practice. The more significant of the defects in Russian surveillance practices identified by the Court invite comparison with U.S. surveillance practices: the breadth of discretion granted to the Executive when dealing with the protection of national security, the emergency procedure provided for in Russian law which enables interception of data without judicial authorisation and without sufficient safeguards against abuse, and the total absence of any notification requirement with regard to the subject of surveillance.[645]

The approach of the ECtHR to the standing of the applicant in *Zakharov* is similar to that taken in *Klass* and *Esbester v the United Kingdom*[646] This is a two-strand approach. Should an applicant claim that he has been subjected to surveillance, he has to furnish conclusive proof. However, given the nature of secret surveillance, this would be difficult, if not impossible. Alternatively,

[643] Application No. 47143/06 (2015).
[644] ibid, at paras 180 and 217.
[645] See details surveillance practices in Chapter Two and Three of this thesis.
[646] (1994) 18 EHRR, CD, 72.

applicants to the ECtHR can challenge the surveillance regulation framework *in abstracto*, without having to furnish proof that they have been spied upon. This abstract review standard, upheld by the Court in *Kennedy*, is likely to be a feature of ECtHR cases involving secret surveillance.

The recent case of *Szabo and Vissy v Hungary* [647] suggests that this may be the case. The circumstances leading to the application were similar to those surrounding *Klass*, *Kennedy* and *Zakharov*. In 2011, the Hungarian government established an Anti-Terrorism Task Force. Under the legislation governing this, the Task Force engaged in secret house searches, surveillance recording of electronic and computerised communications and the opening of letters and parcels. These activities were not subject to judicial review. Two residents of Budapest filed a complaint to the Hungarian Constitutional Court claiming that the sweeping prerogatives of secret intelligence-gathering for national security purposes breached their right to privacy. The Hungarian Constitutional Court dismissed most of these complaints.

The complainants brought an application before the ECtHR, relying on Article 8 of the ECHR. They did not claim that they had been subjected to surveillance, but that they could be subjected to disproportionately intrusive measures. The ECtHR accepted that there had been a violation of the applicants' right to respect for private and family life, and that they could be subjected to intrusive measures without being able to avail of adequate remedies at national level. The series of cases heard *in abstracto* discussed above, culminating in *Sazbo and Vissy v Hungary* [648] parallels the privacy-protective path marked out by the CJEU.

17.0 Contrasting the European and U.S. positions on the Balancing of Data Privacy Rights against National Security Interests

There are significant differences between the U.S. and the countries of western Europe on the question of what privacy means and should mean, in attitudes to data privacy protection and its relative importance in relation to other social goods such as national security, and the laws regulating government uses of personal data as well as laws protecting national security. These differences

[647] Application no. 37138/14 (12 January 2016).
[648] ibid.

have their origin in contrasting ideological and socio-political approaches to the question of what ought to be kept private, what kinds of privacy deserve to be protected in legislation and what criteria should apply in determining the kind and degree of this protection. One broad distinction, based on two contrasting sets of values, is that while in the U.S. the emphasis is on freedom to do something, the jurisprudence of the ECtHR offers freedom from having something done. Laws in the two different jurisdictions may be explained by reference to differing attitudes to privacy. In the U.S., privacy has traditionally been understood as autonomy, the right to do what one wants without state interference, as opposed to privacy being viewed as a form of property, the right to be preserved from surveillance. Whereas the two European systems, the Council of Europe and the European Union, have proactively regulated uses of personal data, the U.S. has refrained from regulation to protect personal data.[649]

Differing models of government as between Europe and the U.S. help to account for contrasting treatments of privacy over time. Europeans have adopted a social-democratic form of government. Fundamental rights such privacy are dynamic and evolving. Government assumes an 'affirmative duty' to the public:

> [T]o foster this evolution through the positive operation of law, bolstering and expanding individual autonomy. Law advances policy choices that are distributive, or allocative, of societal resources, in accordance with the normative choices of democratic bodies. Individuals owe a duty to one another in an interdependent system of social responsibility.[650]

On the other hand, the United States embraces a libertarian model of government, under which fundamental rights and liberties, including the right of privacy, derive from a relatively static Constitution: living constitutionalism

[649] Paul M. Schwartz and Joel Reidenberg, 'Data Privacy Law: A Study of United States Data Protection' (Charlottesville, Virginia, Michie 1996): Julia .M Fromholz, 'The European Union Data Privacy Directive.' 15 (2000) *Berkeley Technology Law Journal* 461.
[650] Richard J. Peltz-Steele, 'The Pond Between: Differences In The US-EU Data Protection/Safe Harbour Negotiation' *Journal of Internet Law* 19(1) (2015) 14, 20.

or constitutional evolution or constitutional reform although possible, is not in favour. As Peltz-Steele puts it

> Government is best that governs least, so the operation of law is largely negative, to ensure that social and economic liberties are protected from interference Individual autonomy flourishes on liberty, rendering persons responsible for their own choices, whether successful or unsuccessful.[651]

While the EU approach to data protection is comprehensive, the U.S. approach is sectoral, or *ad hoc*, with a limited constitutional foundation. Europeans consider privacy a fundamental human right, for which government is responsible for providing to its citizens. The right to privacy is explicitly mentioned in the Constitutions of many European countries, in the Council of Europe Convention for Human Rights and Fundamental Freedoms, and the European Charter of Fundamental Rights. Historically, data protection is grounded in the post-1945 attempts of European countries to control improper use of personal data.[652] While the right to privacy is heavily regulated in Europe, privacy protection through statutory law in the U.S. is not well developed and has been characterised as 'at best a thin patchwork.' [653]

A further significant contrast between the U.S. and Europe in the context of the data privacy/national security balance is evident in the differing responses of the judicial systems in the two jurisdictions when data privacy is compromised by the demands of national security. In Europe, the two major Courts, the Council of Europe ECtHR (Human Rights Court) and the European Court of Justice (CJEU) have been notably proactive in the protection of data privacy rights when these are subjected to interference by overbroad surveillance measures mandated by legislation enacted by individual states or by the European Union.[654] The EU Data Retention Directive of 2006 was struck down by the CJEU for being excessively privacy-invasive. In the U.S., by contrast,

---

[651] ibid.
[652] Lauren B. Movius and Nathalia Krup, 'U.S. and E.U. Privacy Policy: Comparison of Regulatory Approaches' 3 (2009) *International Journal of Communication* 169.
[653] A. Michael Froomkin, "The Death of Privacy?" 52 (2000) *Stanford Law Review* 1461, 1539.
[654] See for example, the case of *Zakharov v Russia* Application no. 47143/06 (2015).

the Courts, especially the Supreme Court, have been reluctant to intervene when State security is at issue.

It is, as Whitman points out, common for Europeans to maintain that they respect 'a fundamental right to privacy' that is either weak or wholly absent in the cultural context of the United States.[655] In this context, Europeans point to Article 8 of the ECHR, which protects the right to 'respect for private and family life' and the EU Charter of Fundamental Rights, which mandates both 'respect for private and Family Life' and 'Protection of personal data.'[656] By the standards of these two groundbreaking documents, American law seems, from the European point of view, simply to have 'failed.' [657] However, as Whitman points out, 'it is not just that Europeans resent and distrust the American approach to privacy. The reverse is also true.' [658] For example, anyone who has lived in the United States can be just as obsessively attached to their privacy as Europeans are to theirs, except that the two versions of privacy are different. For example, Americans defend their privacy by resorting to firearms, while some of the most contentious American social issues are conceived as privacy matters, examples being abortion and sodomy.[659]

18.0 Conclusion

Recent developments, both judicial and legislative, have further shifted the balance away from data retention and towards privacy considerations. The first of these concerns the recent CJEU verdict in *Tele 2 and Watson* [660] which marks a significant consolidation of privacy protective principles following from the verdict in *Digital Rights Ireland*.[661] In relation to *Tele 2 and Watson*,[662] the question posed by the Swedish referring court in relation to the first element of the case, which asked that 'an unequivocal ruling on whether… the general and indiscriminate retention of electronic data is *per se*

[655] James Q. Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' 113 (2004) *The Yale Law Journal* 1151, 1157.
[656] Ken Gormley, 'Long Live the Constitution,' (November 17, 2002) *Pittsburgh Post-Gazette* <http://old.post-gazette.com/forum/comm/20021117edgorm1117p1.asp> accessed 7 January 2017.
[657] See David A. Anderson, *The Failure of American Privacy Law, in* Protecting Privacy 139 (Basil S. Markesinis ed., 1999) 139.
[658] James Q. Whitman, 'The Two Western Cultures of Privacy: Dignity versus Liberty' 113 (2004) *The Yale Law Journal* 1151, 1157.
[659] ibid, 1158.
[660] Case C-203/15 *Tele 2 Severige and Watson* (Grand Chamber) 21 December, 2016.
[661] Case C-293/12.
[662] Case C-203/15 *Tele 2 Severige and Watson* (Grand Chamber) 21 December, 2016

incompatible with Articles 7 and 8 and 52(1) of the Charter.'[663] The Court considered the second element of the reference (*Watson*) in relation to the Data Retention and Investigatory Powers Act (2014) and in the context of judicial review proceedings which came before the Court of Appeal of the United Kingdom. The key point to be adjudicated upon was whether the provisions of the Act were incompatible with the EU Charter of Fundamental Rights and the ECHR.

The Court's salient finding is that notwithstanding Article 15(1) of the e-Privacy Directive providing for exceptions with regard to the confidentiality of communications captured by Article 5(1) of the Directive and safeguards regarding traffic and location data as enshrined in Articles 6 and 9 of the Directive respectively, it is not permissible that such exceptions would serve to render nugatory the principle of confidentiality, which represents one of the Directive's key objectives.[664]

The CJEU's judgment is significant for reiterating a number of critical normative principles which play a key role in the data privacy/national security balancing paradigm. Of particular significance is the confirmation of the finding in *Digital Rights Ireland* that data retention legislation which interferes with 'the fundamental rights enshrined in Articles 7 and 8 of the Charter is very far-reaching and must be considered to be particularly serious.' [665] Most significantly, the CJEU held that in instances where 'data is retained without the subscriber or registered user being informed is likely to cause the persons concerned to feel that their private lives are the subject of constant surveillance.' [666] Further, even with reference to legislation which 'does not permit retention of the content of a communication and is not, therefore, such as to affect adversely the essence of those rights,' [667] the Court held that notwithstanding such provisions, 'the retention of traffic and location data could nonetheless have an effect on the use of means of electronic

[663] ibid, at para 50.
[664] ibid, at para 89.
[665] ibid, at para 100.
[666] ibid. The court referred to para 37 of the *Digital Rights Ireland* judgment in support of its finding in this regard.
[667] ibid, at para 101.

communication and, consequently, on the exercise by the users thereof of their freedom of expression, guaranteed in Article 11 of the Charter.'[668]

Crucially, in relation to the aim of combating serious crime and by extension terrorism, by means of privacy-invasive data retention methods, the CJEU held that by virtue of

> [T]he seriousness of the interference in the fundamental rights concerned represented by national legislation which, for the purpose of fighting crime, provides for the retention of traffic and location data, only the objective of fighting serious crime is capable of justifying such a measure.[669]

However, the Court noted that although

> [T]he effectiveness of the fight against serious crime, in particular organised crime and terrorism, may depend to a great extent on the use of modern investigation techniques, such an objective of general interest, however fundamental it may be, cannot in itself justify that national legislation providing for the general and indiscriminate retention of all traffic and location data should be considered to be necessary for the purposes of that fight. [670]

From the standpoint of the data privacy/national security balancing paradigm, this element of the CJEU judgment is of paramount significance and indicates jurisprudential emphasis on data privacy rights. The CJEU noted the undesirability of legislation which is silent in relation to the 'any relationship between the data which must be retained and a threat to public security.' [671] As a consequence of these considerations the CJEU held that national data retention legislation, such as the Swedish legislation referred to by the CJEU:

[668] ibid.
[669] ibid, at para 102.
[670] ibid, at para 103.
[671] ibid, at para 106.

> Therefore exceeds the limits of what is strictly necessary and cannot be considered to be justified, within a democratic society, as required by Article 15(1) of Directive 2002/58, read in the light of Articles 7, 8 and 11 and Article 52(1) of the Charter.[672]

Lynskey comments that the *Tele2/Watson* judgment given by the CJEU is a 'radical' one, on the basis of the degree of protection it offers in relation to data protection and privacy, and its finding that by 'providing for general and indiscriminate data retention is incompatible with the e-Privacy Directive, as read in light of the relevant EU Charter rights.' [673] However, it is significant that the judgment does not prohibit data retention *per se*. The Court held that when Article 15(1) of the e-Privacy Directive is read in tandem with the provisions of Articles 7, 8 and 11:

> [I]t does not prevent a Member State from adopting legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime, provided that the retention of data is limited, with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period adopted, to what is strictly necessary.[674]

The import of this latter finding by the CJEU relates to the distinction between blanket data retention and targeted data retention, with the latter passing muster on the basis of its necessity and as an essential tool in the fight to combat crime and terrorism. From the perspective of the data privacy/national security balancing paradigm, the CJEU verdict maintains a clear jurisprudential emphasis on data privacy rights and safeguards taking precedence over national security objectives. Lynskey comments that the judgment 'will be a game-changer for state surveillance in Europe' and although 'it offered an early

[672] ibid, at para 107.
[673] Orla Lynskey, 'Tele2 Sverige AB and Watson et al: Continuity and Radical Change' (January 12, 2017) *European Law Blog* <http://europeanlawblog.eu/2017/01/12/tele2-sverige-ab-and-watson-et-al-continuity-and-radical-change/> accessed 12 January 2017.
[674] Case C-203/15 Tele 2 Severige and Watson (Grand Chamber) 21 December, 2016, at para 108.

Christmas gift to privacy campaigners, it is likely to receive a very mixed reaction from EU Member States as such.' [675]

With regard to the second element of the case, the UK Court of Appeal's referencing of the question concerning the nexus between Article 8 ECHR and the EU Charter of Fundamental Rights in relation to data protection and privacy, the Court deemed that 'the question whether the protection conferred by Articles 7 and 8 of the Charter is wider than that guaranteed in Article 8 of the ECHR is not such as to affect the interpretation of Directive 2002/58, read in the light of the Charter.'[676]

The second development within the ambit of the EU is the proposed Regulation on Privacy and Electronic Communications.[677] The proposed Regulation firmly seeks to bolster levels of data privacy and privacy protection to 'data processed in relation with electronic communications in accordance with Articles 7 and 8 of the Charter and ensure greater legal certainty.' [678] The proposals further seek to particularise the provisions of the General Data Protection Regulation and clearly place significant normative emphasis on the importance of the confidentiality attaching to communications which is deemed 'essential for exercising the freedom of expression and information and other related rights, such as the right to personal data protection or the freedom of thought, conscience and religion.'[679]

Additionally, the proposals recognise and enshrine 'the essence of the fundamental right to respect for private and family life, home and communications' as captured by Article 7 of the Charter of Fundamental Rights.[680] They also provide that in instances where the content of electronic communications is interfered with this 'should be allowed only under very clear

[675] Orla Lynskey, 'Tele2 Sverige AB and Watson et al: Continuity and Radical Change' (January 12, 2017) *European Law Blog* <http://europeanlawblog.eu/2017/01/12/tele2-sverige-ab-and-watson-et-al-continuity-and-radical-change/> accessed 12 January 2017.
[676] Case C-203/15 Tele 2 Severige and Watson (Grand Chamber) 21 December, 2016, at para 131.
[677] Proposal for a Regulation Of The European Parliament And Of The Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) European Commission (Brussels, 10.1.2017) COM(2017) 10 final 2017/0003 (COD).
[678] ibid, 9, para 3.6.
[679] ibid.
[680] ibid, 16, para 19.

defined conditions, for specific purposes and be subject to adequate safeguards against abuse.' [681] The proposed measures are predicated on the principle of subsidiarity and with this in mind, they encompass a review of the E-Privacy Directive 'to maintain consistency with the GDPR,' and to adopt 'measures to bring the two instruments in line.'[682] This aim appears particularly necessary, as the General Data Protection Regulation does not capture the processing of data in instances involving the 'prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties,' which include 'the safeguarding against and the prevention of threats to public security and the free movement of such data,' and it is noted that the GDPR 'should not, therefore, apply to processing activities for those purposes.' [683]

It seems reasonably settled that from the EU perspective, both jurisprudentially and legislatively, the balancing paradigm in the ambit of the European Union is firmly pointing towards privacy protective measures as opposed to data retention objectives, while seeking to accommodate both normative standpoints in the most inclusive fashion. The *Tele 2 and Watson* judgment, however, does give rise to the question of a potential conflict of laws in terms of those emanating from the EU and those attaching to the ECHR. White postulates the concern that in arriving at its judgment, the CJEU, although ruling out any form of blanket data retention, has not ruled out 'targeted indiscriminate data retention' and considers this proposition in the context of the concurring opinion of Judge De Albuquerque in the *Szabó And Vissy v Hungary* verdict of the ECtHR,[684] who contended that the salient difficulty regarding the Court's reasoning, with regard to the application of the necessity, rested in the 'degree of suspicion of involvement in the offences or activities being monitored.'[685] Moreover, Judge De Albuquerque expressed his concern that in arriving at its verdict, it deployed the minimal standard of adjudication by reference to the

[681] ibid.
[682] ibid, 4, para 2.2.
[683] Regulation (EU) 2016/679 Of THE European Parliament And Of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (4.5.2016) O.J. L 119/1, para 19.
[684] Matthew White, 'A Threat to Human Rights? The new e-Privacy Regulation and some thoughts of Tele2 and Watson' (10 January, 2017) *EU Law Analysis* <http://eulawanalysis.blogspot.ie/2017/01/a-threat-to-human-rights-new-e-privacy.html> accessed 17 January 2017.
[685] *Szabo and Vissy v Hungary* (Application No 37138/14) Fourth Chamber, January 12 2016. at para 21.

concept of 'individual suspicion,' [686] as opposed to the previous concept of 'reasonable suspicion,' as deployed by the Grand Chamber[687] and further expressed his concern that by having recourse to the former, as opposed to the latter concept, the Court was engaging in assumptative reasoning, on the basis that 'national security protection is not limited to the investigation of past, ongoing or future offences and therefore the "reasonable suspicion" criterion should be dispensed with.'[688]

Judge De Albuquerque emphasised his concerns by noting that:

> The real reason why the Chamber's reasoning does not remain faithful to the Grand Chamber's criterion of "reasonable suspicion" is because it assumes that the fight against terrorism requires a "pool of information retrievable by the authorities applying highly efficient methods and processing masses of data, potentially about each person, should he be, one way or another, connected to suspected subjects or objects of planned terrorist attacks.[689]

From Judge De Albuquerque's perspective, such adjudicative reasoning seems to afford the possibility that mass data retention could be permissible, in order to investigate an instance of terrorism or crime, thus casting an invigilatory eye over many people in the quest to identify those responsible. In addition, Judge De Albuquerque was possibly expressing trepidation at the import of the Court's declaration that:

> [I]t is a natural consequence of the forms taken by present-day terrorism that governments resort to cutting-edge technologies in pre-empting such attacks, including the massive monitoring of communications susceptible to containing indications of impending incidents.[690]

In this regard, a situation might transpire whereby EU law could be in violation of the ECHR. Although the CJEU has ruled out blanket telecommunications

[686] ibid, at para 21.
[687] ibid, at para 35.
[688] ibid, at para 19.
[689] ibid, at para 20.
[690] ibid, at para 68.

and Internet data retention collection, it has not conclusively prohibited selective or targeted telecommunications and Internet data retention. White speculates that should the ECtHR issue a ruling on data retention, in the vein of Judge De Albuquerque's verdict, such a verdict could 'put EU law in violation of the ECHR,' with Member States being placed in an invidious position whereby complying with EU law could result in violating the European Convention on Human Rights and similarly, compliance with the European Convention on Human Rights could result in violating EU Law.[691] Moreover, White suggests that in instances where 'minimum standards of human rights protection' are not complied with due to EU Law requirements, ECHR provisions 'should prevail' adding that 'anything less is a threat to human rights, meaning that (even if well intentioned) the CJUE can also be.'[692]

White's concerns notwithstanding, both the verdict in *Tele 2 and Watson* and the Regulation on Privacy and Electronic Communications, indicate a normative continuum of the privacy protective principles enshrined in the CJEU's verdict in *Digital Rights Ireland*.[693] It seems likely that future European legal instruments, whether promulgated by the EU or by individual Member States, will necessarily be premised on the *Digital Rights Ireland* judgment, but more significantly, will need to be formulated with the legal and normative principles, in addition to the data retention limitations attaching to the provisions of the EU Charter of Fundamental Rights. Formulating a legislative instrument which could balance privacy rights against national security concerns in the context of the *Digital Rights Ireland* judgment might seem to present challenges. However, such a balance is promoted by reference to the judgment, which acknowledges the need for and the role of data retention in the fight against serious crime and terrorism, but rules out blanket retention. This element of the judgment offers legislators and Courts the opportunity to engage in a workable balancing exercise, with neither element of the balancing paradigm being supplanted by the other.

---

[691] Matthew White, 'A Threat to Human Rights? The new e-Privacy Regulation and some thoughts of Tele2 and Watson' (10 January, 2017) *EU Law Analysis* <http://eulawanalysis.blogspot.ie/2017/01/a-threat-to-human-rights-new-e-privacy.html> accessed 17 January 2017.

[692] ibid.

[693] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others*. Grand Chamber CJEU, 8 April 2014.

Chapter Two

The Privacy/Security Balance in the U.S. pre-9/11

1.0 Introduction

In the context of the data privacy/national security balance, it is necessary to distinguish between the pre-9/11 and post-9/11 periods. In the former, concerns over national security did not involve responding to organised terrorist attacks by external agencies on the U.S. mainland, involving a considerable loss of American lives, and the understandable anticipation of further, similar attacks in the immediate future, which marked the opening of the latter period. However, this is not to say that during the pre-9/11 period, particularly from 1945 to the end of the twentieth century, successive Administrations were exempt from national security concerns. Between the end of World War Two and the formal ending of the Cold War in December 1989,[1] there was a general sense that war might easily break out between the U.S. and the U.S.S.R. or China, and that international Communism posed an ever-present threat to the security of the U.S. and its institutions. This helps to explain why U.S. Administrations and their intelligence agencies - the NSA, the FBI and the CIA - were actively infringing the data privacy of U.S. citizens, with the actual, or ostensible purpose of protecting the security of the state and the integrity of its value systems.

As this chapter will demonstrate, the period under review was marked by the institution by State authorities of secret domestic surveillance programmes involving the collection and retention of millions of items of citizen-to-citizen correspondence sent by Americans to other Americans, involving co-operation between the surveillance agencies and telegraph and postal services. A problem associated with these surveillance programmes is the difficulty of distinguishing between interference with the objective of protecting national security and interference involving domestic surveillance of persons and groups who were engaged in political activities: anti-war groups, people demonstrating in favour of equal rights for coloured people, or people

[1] Peter Stothard and Mary Dejevsky, 'Malta summit declares: Cold War is over' *The Times* (December 4, 1989).

suspected by the government and some of its agencies of being linked with communist subversion and Russian espionage activities in the United States.

While some privacy-invasive surveillance measures during the period may have been undertaken *bona fide* for national security purposes, there were times when surveillance was undertaken for purposes having little, if any, relevance to national security protection, but was motivated instead by a desire to promote the purely political interests of the Party in power, or, alternatively, to facilitate the agenda of the Director of the F.B.I., one of whose preoccupations was to damage the reputations of individuals he did not approve of. These aspects of pre-9/11 surveillance, which involved gross breaches of law will be dealt with in a separate section of this chapter.

Consideration will first be given to U.S. understandings of the right to privacy, and in particular the right to data privacy. Separate consideration will be given to the legal right of government and its law enforcement and security agencies (F.B.I., the C.I.A. and the N.S.A.) to access communications data in the interest of public safety, while at the same time narrowing the scope of privacy protections. In the United States, particularly, though not exclusively, since the beginning of the twenty-first century, the various branches of law have made it easier for public authorities to obtain voluminous quantities of communications data to the detriment of privacy.[2]

The branches of law in question here are statutory law, Supreme Court Jurisprudence, and the Constitutional underpinning of the prerogative power of the President to deal with perceived threats to public safety in times of crisis. This prerogative power is generally understood to be derived from a wide interpretation of Clause 1 of Article 2 of the U.S. Constitution: 'The executive power shall be vested in the President of the United States of America.' The theory of prerogative power holds that the President must have whatever authority is necessary to resolve a crisis that confronts the State, 'even if this

[2] See Joel R. Reidenberg, 'The Data Surveillance State in the United States and Europe,' *Wake Forest Law Review* 49 (2014), 583; Paul M. Schwartz, 'German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance,' *Hastings Law Review* 54 (2002) 751; Jack M. Balkin, 'The Constitution in the National Surveillance State, *Minnesota Law Review* 93 (2008) 1; Jed Rubenfeld, 'The End of Privacy,' *Stanford Law Review* 61 (2008) 101.

means that he or she must go against the laws'.[3] This view of the scope of Presidential power enjoys the support of long-standing jurisprudential tradition, reaching back to the eighteenth century. Alexander Hamilton, in Federalist 41, argued that the President's emergency powers 'ought to exist without limitation.'[4]

Attention will then focus on major scandals relating to data retention activities during the 1960s and 1970s, when data privacy rights were illegally infringed by the Executive and the CIA for reasons not relevant to national security. Widespread hostility to these practices resulted in the establishment of a Senate investigation. The Report of the group conducting the investigations (the Church Committee Report) will be analysed, and the implications of its findings discussed.

The chapter will then deal with the passage of the Foreign Intelligence Surveillance Act (FISA) signed into law in 1978, in response to recurring reports of overbroad surveillance practices in the context of national security involving the indiscriminate collection and storage of the personal data of millions of citizens who posed no demonstrable threat to the security of the State. The consequent demand for the statutory regulation of the surveillance activities of U.S. Intelligence agencies was met by FISA. The provisions of FISA will be analysed in the context of its creation in 1978 as part of a regime designed to impose limits on, and oversight of, the domestic use of warrantless surveillance by government for the collection of foreign intelligence, and to bring to an end the practice of electronic surveillance by the executive branch without a court order: hence the establishment of the FISA Court (the FISC) to adjudicate on government applications for intelligence collection. The chapter will examine the ways in which FISA and its Court impacted on the data privacy/national security balance, and the extent to which it fulfilled the tasks assigned to it by Congress in 1978.

A major issue considered is whether State authorities, operating through their intelligence agencies, induced these agencies, particularly the NSA, to engage

[3] Arthur M. Schlessinger, Jr., *The Imperial Presidency* (New York 1973) 17.
[4] Cited in Donald P. Kommers and John E. Finn, 'American Constitutional Law, Essays, Cases and Comparative Notes (Wardsworth Publishing Company 1998) 486.

in privacy-invasive and disproportionate surveillance practices. In this context, ascertaining the role of the NSA, in these practices, presents a significant problem, given the peculiar circumstances surrounding its establishment and its immunity from public scrutiny of its activities between 1952 and 1976. The chapter will address these matters in detail, as well as the detailed investigation by a Senate Select Committee of the surveillance activities of the NSA and other Agencies, and the negative consequences of these activities for the data privacy rights of U.S. citizens. The chapter will further examine the findings and the revelations of the Senate Select Committee and its recommendations for the reform of surveillance practices. This process will involve a detailed analysis of both FISA and the FISC in the context of the establishment of an appropriate data privacy/national security balancing paradigm, in addition to offering an analysis of the shortcomings and dubious assumptions associated with FISA and the FISC.

The problematic nature of carrying out a balancing exercise between rights which are qualitatively different (the right to data privacy and the interests of national security) is examined in detail. Finally, the Chapter reflects on the idea that two parallel data privacy/national security balancing systems operated in the US pre-9/11, one of them legally mandated, the other resulting from the secret, unsupervised activities of the NSA.

2.0 U.S. Understandings of the Right to Privacy and Particularly Data Privacy

Privacy means something radically different in the U.S. constitutional rubric than simply the notion of having one's private life protected, or having one's online data secured from unwarranted intrusion by State agencies or private individuals. In the pre-9/11 era, the focus of this chapter, when State security was a less pressing concern of U.S. governments that it later became, the equilibrium between State security requirements and privacy protection imperatives tended to feature less on the agenda of the Supreme Court than did issues of State regulation of individual freedom and autonomy and the privacy/free speech balance.

It is true that State interference with privacy for reasons of national security and domestic crime prevention, and particularly the latter, was the subject of

Supreme Court consideration before 9/11, and will be examined in this chapter. However, when attacks on material, personal and State security in general were made easier by the rapid development of new communication and information technologies, the privacy/security balance became the main focus of U.S. jurisprudence and government action through legislation. This will be dealt with in the next chapter which deals with the situation post-9/11.

2.1 The Emergence of a Constitutional Right to Privacy in U.S. Supreme Court Jurisprudence

The text of the U.S. Constitution contains no explicit provision that protects a comprehensive right to privacy, nor do any of the Amendments to the Constitution. While the Constitutional text acknowledges a right to property, the sources for a Constitutional right to privacy are more obscure. However, some of the Amendments, particularly the First, Fourth, Fifth and Fourteenth, implicate some aspects of privacy. For the purposes of the present discussion, the Fourth Amendment has a particular relevance. It provides that 'The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated.' A reasonable interpretation of this Amendment is that it postulates an intimate relation of property to privacy, in that it visualises privacy as a right to exclude others from one's property. In 1928, in *Olmstead v The United States*,[5] the Supreme Court ruled that the Fourth Amendment did not prohibit the government's use of wiretaps of private telephone conversations, secured without physical trespass on to Olmstead's property, thus implying the need for a property interest in cases involving claims to privacy rights. The significant feature of this case was not the judgment, but the dissenting opinion of Judge Brandeis, who argued for a broader conception of the right guaranteed by the Fourth Amendment, and in effect for a constitutional right to privacy disjoined from property. He made the case that the makers of the Constitution, in formulating the Fourth Amendment, had conferred, 'as against the government, the right to be let alone- the most comprehensive of rights and the right most valued by civilised men.'[6] The view of privacy advanced by Brandeis did not become influential in U.S. jurisprudence until the mid-nineteen sixties.

[5] 277 U.S., 438 (1928).
[6] ibid, at 478.

In the nineteen sixties, liberation from various kinds of moral and societal restraints became a popular cause, and the discourse of rights began to achieve an ascendancy over the discourse of correlative duties. The same tendency began to prevail in U.S. jurisprudence. Judicial conservatism gave way to judicial activism, as judges sought to discover or discern in the text of the Constitution rights hitherto not brought to light. The era of judicial activism was regarded by those who ushered it in as part of a modernising project. This ultimately led to the emergence of privacy as a Constitutional right. Already in 1890, Warren and Brandeis, invoking the Common Law principle that a man's home was his castle, used this principle as a basis for implying a right to personal privacy. Starting from the premise that the Common Law has always recognised that a man's house is impregnable even to officers of the law 'engaged in the execution of its commands,' they asked rhetorically: 'Shall the Courts now close the front entrance to constituted authority, and open the back door to prurient curiosity.'[7]

In 1950, Edward Griswold, Dean of the Harvard Law School, in a speech which he titled, 'The Right to be let alone,' reaffirmed the principle advocated by Brandeis in his 1928 dissent in *Olmstead*. Griswold went even further than Brandeis in wishing to extend the scope of constitutional rights in the service of privacy. Brandeis had claimed that the Fourth Amendment together with the Fifth (which provided that no person 'shall be compelled in any criminal case to be a witness against himself'), should be understood as implicitly securing 'a more general right to be let alone.' Griswold claimed that 'the right to be let alone' was nothing less than 'the underlying theme of the Bill of Rights,' essential to the autonomy of the individual and to the life of 'the inner man.'[8]

Griswold's account of the scope of 'the right to be let alone' is questionable, if it seems to suggest, as it does in its reference to 'the autonomy of the individual,' that such a right can be absolute. When Brandeis, to whom Griswold owed his use of the term, employed it in his dissent in *Olmstead v United States*,[9] he was careful to qualify it. While he did call it 'the most comprehensive of rights,' he

[7] Samuel Warren and Louis Brandeis, 'The Right to Privacy,' (1890) 4 *Harvard Law Review*. 193.
[8] Erwin Griswold, 'The Right to be let alone,' *Northwestern Law Review* 55 (May-June 1960), 216, 217, 224.
[9] 277 U.S., 438 (1928).

went on to remark that '[t]o protect that right, every unjustified intrusion by the government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.'[10] The phrase 'unjustified intrusion upon the privacy of the individual' indicates a recognition by Brandeis that some form of forms of intrusion upon individual privacy are justified, as the Fourth Amendment makes clear in its account of the circumstances in which 'searches and seizures' can take place: 'no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons and things to be seized.'

2.2 Privacy as Autonomy

A little over two decades after Griswold's affirmation of the right to be let alone, privacy emerged in U.S. Supreme Court jurisprudence as primarily a set of fundamental interests 'that run against the state, rather than [as] a proprietary control over important personal information.'[11] Throughout the nineteen sixties and nineteen seventies, consistent majorities on the U.S. Supreme Court dedicated themselves to the task of exploiting the rights-creating potential of the Constitution, with particular emphasis on specific rights, for example, to privacy and autonomy, and thence to abortion and the use of narcotics.

In the U.S. Supreme Court, only a small number of justices adopted the historical approach and construed the Constitution by trying to interpret the framers' intentions. Examples include Justices White and Rehnquist, the two dissenters in *Roe v Wade*.[12] White based his dissent on his failure to find anything 'in the language or history of the Constitution to support the Court's judgement', while Rehnquist argued that 'To reach its result, the Court necessarily has had to find within the scope of the Fourteenth Amendment a right that was completely unknown to the drafters of the Amendment [in 1868]'. White spoke for many critics of the *Roe* judgment when he described it as a raw, unprincipled exercise of judicial power.'[13] However, since the nineteen sixties, the majority of the Court adopted the 'present-tense' approach

[10] ibid, at 478-79.
[11] Ronald J. Krotszynski, 'The Polysemy of Privacy,' 88 (2013) *Indiana Law Journal* 881, 916.
[12] 410 U.S. 113 (1973).
[13] The opinion of the Court in *Roe v Wade*, and the dissenting opinions of Rehnquist and White are recorded in Donald P. Kommers and John E. Finn, *American Constitutional Law, Essays, Cases and Comparative Notes.* (Wadsworth Publishing Company 1998) 477-86.

as being more appropriate in cases where standards and values, such as personal rights including privacy, equality and so forth, were in question. The basis of this approach was that such values can be interpreted only in accordance with present-day views of them, as these views are held and endorsed by judges. The modern U.S. Supreme Court has thus regarded the Constitution as a living, developing organism, whose elements, for example, the standard for measuring what is an inherent personal right, change with the passage of time, and as social attitudes and values change and develop.

A parallel to this trend in the U.S. Supreme Court jurisprudence may be found in the jurisprudence of the European Court of Human Rights (ECtHR). This Court has frequently emphasised that the European Convention of Human Rights, the 'Constitution' under which it operates, is a 'living instrument which should be interpreted according to present-day conditions.'[14] In 1995, the Court held that the Convention cannot be interpreted 'solely in accordance with the intentions of [its] authors as expressed more than forty years ago.'[15] As De Hert points out, 'although the Convention does not speak to us about modern means of communication,' the Court has brought these under the scope of Article 8, ECHR.[16]

2.3 Evolving Jurisprudential Understandings of Privacy

A key moment in U.S. jurisprudence for the emergence of privacy as a Constitutional right was the case of *Griswold v Connecticut*.[17] Connecticut, one of the last States with a statute restricting the use of contraceptives, was obliged to defend the constitutionality of its law before the U.S. Supreme Court. Three Justices, Goldberg, Brennan and Warren, argued that there was a 'right of marital privacy'[18]

The judgment in *Griswold* remains controversial. It contains six opinions, two of which are dissenting, and incorporates at least six interpretative approaches. Of greater concern is the fact that, as Kommers and Finn point out, 'the seven judges in the majority could not agree on the constitutional basis for the right to

[14] *Tyrer v The United Kingdom*, judgment of 25 April, 1978, 31, E.C.t.H.R.
[15] *Laizdou v Turkey*, judgment of 23 March, 1995, 71. E.C.t.H.R.
[16] Paul J.A. de Hert, 'Balancing security and liberty within the European human rights framework,' (2005) 1 *Utrecht Law Review* 68,74.
[17] 331, U.S., 479 (1965).
[18] ibid, 486-7.

marital privacy they voted to uphold.' [19] Despite reservations about *Griswold* as a credible example of Constitutional interpretation, it is important as a stage in the emancipation of privacy from property.[20]

In *Eisenstaedt v Baird*,[21] a groundbreaking case, the Supreme Court disjoined the privacy right enunciated in *Griswold v Connecticut* (the 'right of marital privacy') from its attachment to marriage and the family, and declared it a free-standing individual right. *Eisenstadt* marked an important step from a number of perspectives. It gave the right to privacy an individual basis, and liberated it from dependence on other rights or values. More significantly, in the context of the security/privacy debate, the case represented a shift from privacy as 'freedom to engage in certain activities,' and to make 'certain sorts of choices without governmental interference.' [22]

The line of Supreme Court cases dealing with lifestyle choices from *Griswold* and *Eisenstadt* exhibited the working of the wedge principle, in that one expansion of the right to privacy was followed by a further one, until limited privacy finally emerged as personal autonomy. However, in none of these cases purporting to establish and protect various zones of privacy (including Griswold and *Eisenstadt*), was the Court talking about citizens' freedom from official intrusion into their homes, their persons, their papers, their telephones; their right to be free from official surveillance or accosting, from having to file, with governmental bodies, forms and returns containing information of varying degrees of privateness, from having data about them collected by official bodies.[23] Instead, the decisions in these cases vindicates freedom from official regulation.

2.4 The Privacy/Security Balance pre-9/11

In the context of the privacy/security balance before 9/11, the main focus is not on maintaining the security of the State against external threats, but on upholding the rule of law within the U.S. This mainly involves wiretapping and

[19] ibid, 41-2.
[20] See Mary Ann Glendon, *Rights Talk. The Impoverishment of Political Discourse*, (New York 1991), 57.
[21] 405 U.S. 438 (1972).
[22] Michael J. Sandel, 'Moral Argument and Liberal Toleration: Abortion and Homosexuality.' 77(3) (1989) *California Law Review* 521, 527-8.
[23] Louis Henkin, 'Privacy and Autonomy' 74(7) (1974) *Colombia Law Review* 1410, 1425.

bugging of telephones by federal agents with the purpose of obtaining evidence where criminal activity of criminal intent were suspected. Two subsequent Supreme Court cases, *Berger v New York* [24] and *Katz v United States* [25] marked a significant change in the Court's view of the balance between individual privacy and State surveillance. In its opinion, the Court held that the Fourth Amendment protects people, as distinct from places. It then held that 'what [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.' [26]

A fundamental principle underlying the judgment in *Katz* was enunciated by Justice Stewart, speaking for the Court: 'Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures.'[27] The new understanding of how the Fourth Amendment should be applied in wiretapping and bugging cases, whatever the level of sophistication in the technology involved, is conveyed in the following:

> Once it is recognised that the Fourth Amendment protects people- and not simply 'areas' - against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure.[28]

The government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment. The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance.[29]

In *Lopez v U.S.* decided four years before *Katz*, Justice Brennan, dissenting in *Lopez*, anticipated the judgment in *Katz*, and enlarged upon the serious threats to privacy posed by developing surveillance technologies. He stressed 'the

[24] 388 U.S. 41 (1967).
[25] 389 U.S. 347 (1967).
[26] *Katz v United States* 389 U.S.347 (1967), 351-2.
[27] ibid, at 359.
[28] ibid, at 353.
[29] ibid.

qualitative difference' between electronic surveillance technologies and conventional stratagems such as eavesdropping and disguise. While the latter do not so seriously intrude upon the right of privacy, as soon as electronic surveillance comes into play, the risk to privacy changes radically. Brennan struck a menacing, and prophetic, note when he warned that '[t]here is no security from [electronic] eavesdropping, no way of mitigating the risk, and so not even a residuum of true privacy.' He further claimed that electronic aids make eavesdropping 'more penetrating, more indiscriminate, more truly obnoxious to a free society. Electronic surveillance, in fact, makes the police omniscient,' and police omniscience is one of the most effective tools of tyranny.'[30] This kind of rhetoric anticipates the tone and content of much of the commentary on the radically more invasive surveillance techniques employed in the U.S.A. and Great Britain in response to the events of 9/11.

It is fair to say that prior to its decisions in *Berger* and *Katz*, the Supreme Court had not fully come to terms with the realities of modern advances in the techniques of electronic surveillance. In particular, it had failed to recognise that the privacy protections offered by the Fourth Amendment needed to be interpreted more expansively in the light of the realities of the technological age. It was not until 1967, when, in *Berger* [31] and *Katz*, [32] the Court declared that wiretapping and bugging violated Fourth Amendment guarantees of freedom from unreasonable searches and seizures, that criteria were available to legislators which would need to be embodied in any statute authorising the use of electronic surveillance techniques.

The decision in *Katz* reversed the traditional Supreme Court view that the Fourth Amendment right to privacy could not be violated without a physical trespass. The essence of the *Katz* judgment was that the Fourth Amendment protects people, as distinct from places. It further held that 'what [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.'[33] A fundamental principle underlying the judgment in *Katz* was enunciated by Justice Stewart, speaking for the Court: 'Wherever a

[30] 373 U.S. 427 (1963), at 465-66.
[31] *Berger v New York* 388 U.S. 41 (1967).
[32] *Katz v United States* 389 U.S. 347 (1967).
[33] ibid, at 351 -2.

man may be, he is entitled to know that he will remain free from unreasonable searches and seizures.'[34]

In 1968, a year after *Katz,* Congress enacted a law, *Title III of the Omnibus Crime Control and Safe Streets Act*[35] for the better regulation of electronic surveillance. This law provided for strict controls on government wiretapping and bugging. Thus, through the combined efforts of the Supreme Court and Congress, legal regulation of government intelligence-gathering expanded significantly in the 1960s.[36] Prior to its decisions in *Berger* and *Katz*, the Supreme Court had not fully come to terms with the realities of modern advances in the techniques of electronic surveillance. In particular, it had failed to recognise that the privacy protections offered by the Fourth Amendment needed to be interpreted more expansively in the light of the realities of the technological age. It was not until 1967, when, in *Berger* and *Katz*, the Court declared that wiretapping and bugging violated Fourth Amendment guarantees of freedom from unreasonable searches and seizures, that criteria were available to legislators which would need to be embodied in any statute authorising the use of electronic surveillance techniques.

On 19 June, 1968, Congress enacted the Omnibus Crime Control and Safe Streets Act.[37] Title III of the Act sets out the conditions and circumstances under which the interception of both wire and oral communications may occur. It prohibits all wiretapping and bugging by private parties without first securing the consent of a participant in the conversation. Certain persons and agencies are exempted from the operation of the Act. These include the President of the U.S.A. acting in National security cases, and telephone, telegraph and Federal Communications Commission employees acting in the normal course of their employment. State and Federal law enforcement officials, in the performance of their duties, may apply for court authorisation to engage in eavesdropping in carefully delimited circumstances. With the prior consent of a party to a conversation, these officials are given an

[34] ibid, at 359.
[35] Public Law 90-351, 802, Stat. 197.
[36] Daniel J. Solove, *Nothing to Hide, The False Tradeoff between Privacy and Security* (Yale University Press, 2011) 9.
[37] Details of these provisions of Title III of the Crime Control Act are set out in U.S.C., 2511 and 2516.

unqualified privilege to intercept the communication without securing Court approval. Under the Act, the various states are left free to enact their own legislation, the only limitation on this being that they do not set standards below those enumerated in Title III. The states are also left free to impose a total ban on all eavesdropping. At a practical level, the Act attempts to curtail the availability of eavesdropping devices by banning the manufacture, distribution, sale, possession and advertising such eavesdropping devices as are useful for surreptitious electronic surveillance. In the context of the role of President Bush in security matters post-9/11, it is interesting that Title III of the Crime Control Act emphasises its intention not to 'limit the Constitutional power of the President in national security matters [38] or the Presidential power to protect national security.[39]

Four years after the passage of the Omnibus Crime Control and Safe Streets Act, the Supreme Court in *United States v U.S. District Court (Keith)* [40], tested the National Security exception in a case in which the defendants, U.S. citizens, were charged with destroying government property and one of them was charged with the bombing of a Michigan C.I.A. office.[41] The defendants moved to compel the government to reveal whether a warrantless wiretap of any of the defendants' conversations had taken place. In an affidavit, the Attorney-General acknowledged that he had approved warrantless wiretaps in this case, but argued that the wiretaps had been employed to gather intelligence information 'deemed necessary to protect the nation from attempts of domestic organisations to attack and subvert the existing structure of the Government'.[42] The Attorney-General also certified that the disclosure of the recorded conversations could also harm national security.[43] The Government provided the District Court, under seal, with the transcripts of the recorded conversations and records showing that the Attorney-General had approved the wiretaps.[44] The District Court ruled in favour of the defendants and the Court of Appeal affirmed on a writ of Mandamus.

[38] 18 U.S.C., 2514.
[39] ibid, 2511 (3).
[40] 407 U.S. 297 (1972).
[41] ibid, at 299.
[42] ibid, at 300, fn 2.
[43] ibid.
[44] ibid, at 300-01.

The Supreme Court dismissed the Government's contention that the Crime Control Act recognised the President's ability to conduct national security surveillance without a warrant. The Court based its judgments on three considerations. The first of these was that the national security exception mentioned in the Act was worded negatively: it did not grant the President the authority to obtain foreign intelligence information but simply ensured that whatever inherent authority he possessed in this regard would not be interfered with. This meant that in passing the Act, Congress had left presidential powers where it found them.[45] The second ground for the Court's dismissal of the government's case was that it did not concern the authority of the President to engage in surveillance of foreign activities, since there was no evidence of any direct or indirect involvement of a foreign power.[46] The third ground was that the government had not shown a sufficient reason to carve a domestic national security exception into the Fourth Amendment.[47]

In an appendix to his dissenting opinion in *United States v White* (1971),[48] Justice Douglas included a Memorandum from President Johnson, dated 30 June 1965: 'For the Heads of Executive Departments and Agencies.' [49] Johnson then laid down basic guidelines to be followed by all government Agencies. These included the stipulation that no Federal agent was to intercept telephone conversations within the U.S. by any mechanical or electronic device, without the consent of the parties involved, 'except in connection with investigations related to the national security.' Furthermore, no interception was to be undertaken without the 'prior approval of the Attorney General.'[50] The national security exception, however, gave scope to the Executive Branch of the government to relax Constitutional safeguards in relation to privacy, a situation that prevailed pre-9/11 and more openly so post-9/11.

The absence of an overarching comprehensive U.S. privacy law appears to be the principal reason that the EU concluded that the U.S. did not provide adequate privacy protection as this was defined in the EU Directive on the

[45] ibid, at 303.
[46] ibid, at 309.
[47] ibid, at 320-21.
[48] 401 U.S. 745 (1971).
[49] ibid, 767
[50] 401 U.S. 767-8.

Privacy of Personal Data, 95/44/EC. This Directive created a Working Party, known as the Article 29 Working Party, named after the Article of the Directive which enacted it, while Article 30 authorised this Working Party to advise the European Commission on matters related to the implementation of the Directive including data protection practices in third countries. In an Opinion on U.S. data protection practices, the Working Party took the view that 'the current patchwork of narrowly-focused sectoral laws and voluntary self-regulation cannot at present be relied upon to provide adequate protection in all cases for personal data transferred from the European Union.'[51]

3.0 Major Interferences with data privacy for national security reasons pre-9/11 in the context of the data privacy/national security balance, with emphasis on the background and role of the NSA.

Before considering interferences with data privacy during the period under review, it will be necessary to outline the circumstances surrounding the establishment of the National Security Agency (The NSA). This Agency was to play the major role in compromising the data privacy rights of U.S. citizens in the pre-9/11 era. One of the key legal enactments of the period under review was a Memorandum from President Truman to the Secretaries of State and Defence, of October 24, 1952.[52] The significance of the Truman Memorandum is that it was a Presidential Order mandating the establishment of the NSA.

James Bamford describes the Truman Memorandum as 'the birth certificate of America's newest and most secret agency, so secret in fact that only a handful in the government would be permitted to know of its existence.'[53] The establishment of the NSA 'received no news coverage, no congressional debate, no press announcement, not even the whisper of a rumour.'[54] There was no mention of the new organisation in *The Government Organisation Manual*, *The Federal Register* or *The Congressional Record*. As Bamford Remarks,

[51] Opinion 1/99 concerning the level of data protection in the United States and the ongoing discussions between the European Commission and the US Government. Available at: <http://ec.europa.eu/justice/dataprotection/article29/documentation/opinionrecommendation/files/1999/wp15_en.pdf> Accessed 30 September 2014.
[52] Available at <http://www.nsa.gov/docs/efoia/released/truman.truman.tif> accessed 20 June 2017.
[53] James Bamford, *The Puzzle Palace: A Report on America's Most Secret Agency* (Penguin 1983). Cited in Robert N. Davis, 'Striking the Balance: National Security vs. Civil Liberties' *Brooklyn Journal of International Law* 29 (1) (2003-04) 175, 182.
[54] ibid, fn 44.

'[e]qually invisible were the new agency's director, its numerous buildings and its ten thousand employees.'[55] The fact that the NSA was created by Presidential Order rather than by statute law helped to shield it from scrutiny. The extent of the latitude enjoyed by the NSA is indicated in a 1976 Report by a Congressional Committee which revealed that the agency maintained that 'no existing statutes control, limit, or define the signals intelligence activities of NSA.'[56]

The NSA's General Counsel further claimed that the Fourth Amendment of the U.S. Constitution did not apply to the NSA when it intercepted international communications by U.S. citizens.[57] If by Presidential fiat, the NSA had the freedom to disregard the provisions of the Fourth Amendment when intercepting the communications of U.S. citizens, its activities were rendering its telecommunications surveillance activities largely free from constitutional restrictions, and violating the privacy rights of U.S. citizens at a fundamental level by denying them their constitutional rights. In U.S. law, the Fourth Amendment 'is the critical constitutional provision regarding telecommunications surveillance.' [58] This Amendment provided that:

> The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[59]

The view taken by those who directed the surveillance activities of NSA was that the Cold War, or a serious threat to national security, suspends the

[55] ibid.
[56] Supplementary Detailed Staff Reports On Intelligence Activities And The Rights Of Americans, Book Three, Final Report Of The Select Committee To Study Governmental Operations With Respect To Intelligence Activities, S. Rep No. 94-755, at 736. (9th Congress Second Session 1976), The Assassination Archives and Research Centre, available at <http://www.aarclibrary.org/publib/contents/church/contents_church_reports_book3.htm.> accessed 20 March 2015. Henceforth cited as Church Report.
[57] ibid.
[58] Paul M. Schwartz, 'Germany and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance' *Hastings Law Journal* 54 (2003) 751, 764.
[59] For background to the Amendment, see Anthony G. Amsterdam, 'Perspectives on the Fourth Amendment' 58 (1973-1974) *Minnesota Law Review* 349-477; Silas J. Wasserstorm and Louis Michael Seidman, 'The Fourth Amendment as Constitutional Theory' *Georgetown Law Journal* 77 (1988-89) 19-112.

protection from unfounded interference with liberty furnished by the Fourth Amendment. This view implies the claim that the Fourth Amendment bans only 'unreasonable' searches or seizures and that in wartime 'what is reasonable is essentially unfettered presidential discretion to wield every tool available to respond to the enemy.'[60]

If one were undertaking an assessment of the data privacy/national security balance prevailing at any stage before 1976, one would have been facing a formidable, if not insuperable, obstacle: the veil of secrecy surrounding the surveillance programmes pursued by intelligence agencies for national security reasons which impinged on the data privacy of U.S. citizens. The extent of these surveillance programmes and the degree to which they compromised the privacy rights of citizens did not become matters of public knowledge until 1976, with the publication of a voluminous report of a lengthy U.S. Senate Investigation of government-sponsored surveillance operations conducted by intelligence agencies between 1945 and 1975 involving the privacy rights of Americans.[61]

In this section, two of the more controversial secret surveillance programmes undertaken for security reasons will be considered: Project *Shamrock* and the CIA mail opening programme. These have been chosen because of the scale of the surveillance involved in each and the effect of their activities on the data privacy/national security balance. The national security dimension of Project *Shamrock* was made clear by a former NSA senior executive who pointed out that the project was developed 'because it could provide foreign intelligence information concerning a number of foreign intelligence requirements,

[60] John Yoo, 'The Terrorist Surveillance Program and the Constitution' *Georgia Mason Law Review* 14 (2007) 565, 586-87. See also Jed Rubenfeld, 'The End of Privacy' *Stanford Law Review* 61 (2008) 101 and Joseph D. Mornin, 'NSA Metadata Collection and the Fourth Amendment' *Berkley Technology Law Journal* 29 (2006) 985.

[61] The Report, was popularly known as *The Church Report*, after the Chairman of the Senate Select Committee, Frank Church, is based on the testimony of many people who were involved in surveillance programmes and of public figures who were familiar with the nature of these programmes. The Committee engaged in the most 'thorough investigation ever made of United States intelligence.' It consisted of a staff of 100, which conducted over 800 interviews, 250 executive hearings and compiled over 110,000 pages of documentaries. Church Committee Report, Book 1, Note 1, 7.

particularly those related to foreign affairs, terrorism, and espionage.'[62] The Senate Select Committee found that 'millions of private telegrams sent from, to, or through the United States' were obtained by the NSA from 1947 to 1975 under a secret arrangement with three United States telegram companies'[63] as part of Project *Shamrock*. In this context, the Church Report also revealed that some operatives in the intelligence community contended that questionable and illegal acts, such as those perpetrated in the *Shamrock* project, were justified by a law higher than statutory law or the Constitution: if national security required such acts, they were acceptable. In this way when intelligence officials secured the cooperation of telegraph company executives for Project *Shamrock* in which the NSA received millions of copies of international telegraph messages without the senders' knowledge, they assured the executives that they would not be subjected to criminal liability because the project was 'in the highest interests of the nation.'[64]

Such practices and the attitudes underlying them raise issues relevant to the data privacy/national security balance. One of these is that the more technology advances, 'the more difficult it is to control its privacy-intrusive use.'[65] During the pre-9/11 era, technology was developing at such a fast rate, and in a more pervasive form, without regard to its implications for privacy, while at the same time technological privacy-protective measures were not keeping pace with invasive technological surveillance measures. In this connection, it is necessary to take account of a problem confronting security intelligence generally: the perceived vulnerability of democratic societies in face of the diffuse nature of the threats posed to their security. This means that intelligence is regarded as necessary in relation to everything which is, or can potentially become, a danger to state security. In turn, it also means that when external limits are imposed on intelligence gathering in the form of robust judicial or legislative oversight, than, as Campbell observes, 'the natural tendency on the

[62] James G. Hudec, 'Unlucky *Shamrock* - The View From the Other Side' 44 (5) (2000) Central Intelligence Agency Library <https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol44no5/html/v44i5a12p.htm> accessed 21 November 2016. See also Schneier on Security 29 December 2005 <https://www.schneier.com/blog/archives/2005/12/project_shamroc.html> accessed 22 November 2016.
[63] Church Committee Report, Book 2, 6.
[64] Church Committee Report, Book 2, 145.
[65] Kevin Aquilina, 'Public security versus privacy in technology law: A balancing act?' 26(2) (2010) *Computer Law and Security Review* 130.

part of all security and intelligence agencies is to over-collect information,' [66] that is, to engage in overbroad surveillance measures which infringe citizens' rights to data privacy insofar as these are enshrined in the Fourth Amendment.[67] Campbell points out that internal limits will not suffice, because, 'while the staff of a security agency should set limits on the collection of data, it is not primarily their job to think about the damage which over-collection can do to the vital values of democratic societies.' [68] In this context, the pre-9/11 period had two phases: the first, from the early 1950s to 1978, the second from 1978 to 2001. In the first, because intelligence gathering was subject to minimal judicial or legislative oversight, the intelligence agencies, as the Church Committee found, engaged in overbroad surveillance, which encompassed the private data of Americans in addition to data relevant to state security, thereby adjusting the privacy/security balance in favour of security. Post-1978, the passage of FISA, with its provision for judicial review of government requests for surveillance warrants, should, at least in theory, have adjusted the balance in the opposite direction. Whether it did so in fact will be considered elsewhere in this chapter.[69]

Among the recommendations made in the Church Committee Report was that the NSA should not request from any commercial carrier any communication which it could not otherwise obtain: this recommendation was to ensure that the NSA would not resume an operation such as *Shamrock*.[70] Operation *Shamrock* became illegal, both as a violation of the Fourth Amendment of the Constitution, and as argued at the Church Committee, in violation of the Communication Act of 1934, once it began to target United States citizens and domestic terminals. Operation *Shamrock* as Bloom and Dunn point out, 'expanded beyond its initial scope and initial justification.' [71] At a public hearing of the Senate Select Committee on 6 November 1976, Senator Church

[66] Professor Iain Campbell, Venice Commission, Speaking Notes, European Parliament Hearing on Mass Surveillance, 7th November 2013. <http://www.europarl.europa.eu/document/activities/cont/201311/20131114ATT74429/20131114ATT74429EN.pdf> accessed 23 December 2016, 16.
[67] ibid.
[68] ibid.
[69] See section dealing with FISA and the FISC.
[70] Church Committee Report, Book 2, 310.
[71] Robert Bloom and William J. Dunn, 'The Constitutional Infirmity of Warrantless NSA Surveillance: The Abuse of Presidential Power and the Injury to the Fourth Amendment' 15 (2006) *William and Mary Bill of Rights Journal* 147, 158.

read the Committee's Report on the *Shamrock* programme, detailing how the NSA's agreements with private companies provided them with Americans' international telegrams from 1947 until May 15, 1975, when NSA Director General Allen terminated the programme.[72]

A parallel programme to Project *Shamrock*, the CIA mail-opening programme, was examined by the Church Committee under the heading *Illegal or Improper Means*. This kind of surveillance was described in the Church Report as 'not only vastly excessive in breadth and a basis for degrading counterintelligence actions, but was often conducted by illegal or improper means'.[73] The Report reveals that over a period of approximately twenty years, the CIA carried out a programme of indiscriminately opening citizens' first-class mail. [74] Between 1940 and 1973, the CIA and FBI secretly and illegally opened and photographed letter mail within the U.S.[75] with the purpose of collecting 'foreign intelligence' and 'counterintelligence' information.[76] Over that period, the two agencies, the CIA and FBI, implemented twelve separate programmes 'which involved the illegal opening of hundreds of thousands of first class letters'.[77] The longest-running CIA Mail opening programme from 1953 to 1973, which operated in New York City, involved the screening of in excess of 28 million letters, with 'the exteriors of 2.7 million' photographed while '214,820 letters were opened'.[78] The collective scope of these programmes is difficult to ascertain, but it appears that just one of these programmes operated by the CIA, involved the opening of more than 215,000 letters between the United States and the Soviet Union over a twenty-year period.[79]

In its assessment of the number of Americans affected by domestic intelligence activity, the Church Report revealed that U.S. Intelligence agencies 'investigated a vast number of American citizens and domestic organisations'.[80] In its memorandum to the Church Committee of 10 June 1975, the FBI

[72] See *Schneier on Security* (29 December 2005). <https://www.schneier.com/blog/archives/2005/12/project_shamroc.html> accessed 22 November 2016.
[73] Church Committee Report, Book 2, 12.
[74] ibid.
[75] ibid, 168.
[76] ibid, 208.
[77] ibid, 168.
[78] ibid.
[79] ibid, 184.
[80] ibid, 6.

acknowledged that it had developed over 500,000 intelligence files, and that it had opened 65,000 of these files in 1972 alone.[81] Each of these files contain information on more than one individual or group. In addition to at least 130,000 first class letters opened and photocopied by the FBI between 1940 and 1966 in eight U.S. cities, some 300,000 individuals were indexed in a CIA computer system, and separate files were created on approximately 72,000 Americans and 100 domestic groups during the course of Operation *Chaos* from 1967 to 1973.[82] An estimated 100,000 Americans were the subjects of surveillance by U.S. Army Intelligence between the 1960s and 1971, while Intelligence files on more than 11,000 individuals and groups were created by the Inland Revenue Service.[83]

The two most significant findings of the Church Committee were, firstly, that most basic harm caused by the 'illegal and improper' surveillance programmes 'was to the values of privacy and freedom which our Constitution seeks to protect and which intelligence activity infringed on a broad scale'.[84] The second significant finding was that the Committee had seen 'segments of our Government, in their attitudes and action, adopt tactics unworthy of a democracy, and occasionally reminiscent of the tactics of totalitarian regimes'.[85] This latter finding echoes a warning by Attorney General, Harlan Fiske Stone in 1924 that Federal Agencies should not investigate political or other opinions as opposed to 'conduct forbidden by the laws' because:

> When a police system passes beyond these limits, it is dangerous to the proper administration of justice and to human liberty, which it should be our first concern to cherish…..There is also a possibility that a secret police may become a menace to free government and free institutions, because it carries with it the possibility of abuses of power.[86]

---

[81] ibid.
[82] ibid.
[83] ibid.
[84] Church Committee Report, Book 2, 15.
[85] ibid, 3.
[86] *New York Times* 13 May, 1924. See also a similar comment in the Church Report: 'Secrecy, even what would be agreed by responsible men to be necessary secrecy, has, by a subtle and barely perceptible accretive process, placed constraints upon the liberties of the American people.'

A similar comment was made in the Church Report: '[s]ecrecy, even what would be agreed by responsible men to be necessary secrecy, has, by a subtle and barely perceptible accretive process, placed constraints upon the liberties of the American people.' [87]

4.0 Major Scandals Relating to Data Retention: Privacy Rights Illegally Infringed by the Executive and its Agencies

For a considerable period in the nineteen sixties and nineteen seventies, law enforcement agencies, notably the F.B.I., whose normal function was to deal with domestic criminal activities, was employed by the government to spy, for bogus security reasons, on those citizens who were suspected, not of criminal intent or criminal acts, but of posing a threat to the political or ideological interests of the party in power. In 1963, Allen Dulles, Director General of the Central Intelligence Agency, assured Americans that 'Our government in its very nature - and our open society in all its instincts, under the Constitution and the Bill of Rights automatically outlaws intelligence organisations of the kind that have developed in police states.' [88] However, despite such expressions of confidence that the U.S. Constitution and the Amendments in the Bill of Rights would protect citizens against secret police activities, 'evidence continues to accumulate that the Constitutional safeguards developed by the Supreme Court are inadequate to control clandestine police investigative methods.' [89] For example, in the late nineteen sixties, various instances were reported of undercover investigators being employed against political or quasi-political groups within the United States. Groups being spied on included members of the Conference on New Politics in Chicago who reported that they were being infiltrated by agents who were reporting to the F.B.I. [90] In 1968, a policeman testified before a Congressional Committee that he infiltrated protest groups in Chicago who had gathered to demonstrate during the Democratic National Convention.[91] Civil Rights campaigners were a common target: in 1964, the

[87] Church Committee Report, Book 1, 9.
[88] Allen Dulles, *The Craft of Intelligence* (1968), cited in Joseph R. Lundy, 'Police Undercover Agents: New Threat to First Amendment Freedoms.' *The George Washington Law Review* 37(2) (1968-69) 634.
[89] ibid.
[90] *New York Times*, 7 September, 1967.
[91] *Chicago Daily News*, 4 October, 1968.

subversives unit of the Alabama Department of Public Safety was secretly compiling data on the activities of these campaigners.[92]

J. Edgar Hoover was Director of the F.B.I. from 1935 until his death in 1972. During the period, he used the considerable surveillance resources of the F.B.I. to compile secret files on political leaders, and to collect data on civil rights groups and their leaders, using illegal methods.[93] The most notable victim of Hoover's violation of privacy norms was Martin Luther King. From 1963 to 1965, the F.B.I. maintained taps on King's home telephone, and, at Hoover's direction, installed listening devices in King's hotel and motel rooms.[94] Dean Rusk was U.S. Secretary of State under Presidents Kennedy and Johnson. In testimony before the Senate Foreign Intelligence Relations Committee, in July 1974, he helped to explain why the Constitutional protections afforded to privacy, the safeguards developed by the Supreme Court in combination with legislation such as the Crime Control Act, proved insufficient to protect the privacy rights of many individuals against the frequently unauthorised investigative methods employed by law enforcement agencies such as the F.B.I. under Hoover's direction. Rusk gave evidence to the Foreign Relations Committee which suggested that the F.B.I. up to the time of Hoover's death was never fully answerable to the rule of law. It had developed, as Rusk put it:

> [I]nto an extraordinarily independent agency within our government….Mr Hoover, in effect, took orders only from himself…He had created a kind of kingdom…almost unparalleled in the administrative branch of our government, a combination of professional performance on the job, some element of fear, very astute relations with the Congress, and very effective public relations.[95]

At the same time that Hoover's F.B.I. was freely engaging in the interception of telephone conversations involving people of whom he disapproved, and who posed no demonstrable threat to the security of the State, President Johnson

[92] *New York Times*, 17 February, 1964.
[93] Hoover's Illegal surveillance methods are documented in Athan G. Theoharis and John Stuart Cox, *The Boss: J. Edgar Hoover and the Great American Inquisition*. (Temple University Press 1988).
[94] Arthur M. Schlesinger, Jr., *Robert Kennedy and His Times* (Andre Deutsch, 1978) 360.
[95] ibid, at 250.

was telling the heads of Agencies, which included the F.B.I., that he was strongly opposed to such interception as a general investigative technique.[96] The telephone taps on Martin Luther King's home, the hotels in which he stayed and the offices of the Civil Rights movement in New York and Atlanta, demanded by Hoover, were authorised by President Kennedy and his brother Robert, the U.S. Attorney-General, after some vacillation.[97] The latter, having insisted that the taps be evaluated at the end of thirty days, failed to enforce this demand, and the F.B.I. maintained taps on King's home for two more years.[98] This Executive sanction of serious breaches of individual rights was part of a larger picture, involving high politics and Hoover's determination to destroy King's credibility and that of the Civil Rights movement. The readiest way to achieve this aim was to establish a link in the public mind between King and Communist subversion and Russian espionage in the United States. Hoover convinced President Kennedy that some of King's close associates were agents of a Soviet conspiracy,[99] while the F.B.I. issued a report on King's 'Affiliations with the Communist Movement.' For his part, King suspected that the President was himself afraid of Hoover, because the latter had amassed secret files on all major political figures, including the Kennedys, and was consequently in a position to intimidate and threaten sitting Presidents.[100] It is reasonable to assume that the Kennedys authorised the taps on King partly to find out the truth about Hoover's accusations that he had Communist links, and partly to protect themselves from what Hoover might do with the compromising secret files he had compiled on them, particularly on the President.[101]

The Nixon presidency, beginning in 1969, and ending prematurely in disgrace in 1974, featured the most egregious use so far of Executive power to override Constitutional and legislative instruments of privacy protection. In the early days of the Nixon term, the National Security Agency implemented Project Minaret, which tightened the surveillance of the 'watch lists' of American

[96] For details of President Johnson's instructions to the Intelligence Agencies, see Section 2.4 The Privacy/Security Balance pre-9/11.
[97] Arthur M. Schlesinger, Jr., *Robert Kennedy and His Times* (Andre Deutsch, 1978) 360.
[98] ibid.
[99] ibid, 358. For a detailed discussion of this aspect of Hoover's ongoing secret surveillance of King with the aim of discrediting him, see *Let the Trumpet Sound. The life of Martin Luther King, Jr.* Stephen B. Oates (Search Press, London) 1982 pp 265-334.
[100] Ovid Demaris, *The Director* (New York, 1975). 210.
[101] See David Wise, *The American Police State* (New York, 1976) and Arthur M. Schlesinger, Jr., *Robert Kennedy and His Times* (Andre Deutsch, 1978) 359 'The still sacrosanct Hoover had vast power to do damage to King, to the Civil Rights Bill, and to the Kennerdys.'

citizens which the Agency had begun to assemble in the early 1960s. These citizens included those travelling to Cuba in addition to those who were deemed to pose a danger to the President, and those involved in civil disturbances, with a specific focus on civil rights and anti-Vietnam War groups. Under Nixon, MINARET grew to approximately 300,000 surveillance targets.[102] At the White House, Nixon acted on the principle that he had enemies everywhere and that these enemies must be dealt with. His senior administrative staff members collaborated with him in the compilation of an 'enemies list,' consisting of Democratic politicians, journalists and major contributors to the Democratic Party. Potential Democratic opponents in the subsequent Presidential Election were identified, and Nixon suggested to an enthusiastic aide that surveillance should be carried out on these, remarking: 'Maybe we can get a scandal on any one of the leading Democrats.'[103]

A significant feature of this surveillance was that it was not motivated by concerns about the internal security of the U.S., about criminal activity or external threats to the security of the State. Its goals were expressed in a document drawn up by John Dean, Presidential Legal Counsel, headed 'Dealing with Our Political Enemies.' This document addressed 'the matter of how we can maximise the fact of our incumbency in dealing with persons known to be active in their opposition to our administration.'[104] One way of dealing with political opponents, whether politicians or supporters, was to suborn compliant officials in the Internal Revenue Service into handing over the tax returns of these political enemies, with a view to finding irregularities. When senior Revenue officials failed to comply, Nixon suggested that some of his agents could 'sneak' into the IRS offices 'in the middle of the night' and purloin the necessary information. Nixon wanted this kind of surveillance

[102] Gabriel Schoenfeld, *Necessary Secrets: National Security, The Media, and the Rule of Law* (Norton and Company 2010); U.S. Senate Committee on Intelligence Activities Within the United States, Intelligence Activities and the Rights of Americans. 1976 US Senate report on Illegal Wiretaps and Domestic Spying by the FBI, CIA and NSA 16 (1976) - the Church Committee Report, which noted that warrantless wiretapping began to occur frequently in the 1930s.
[103] Nixon speaking to R.H. Haldermanm, White House Chief of Staff. Cited in Anthony Summers, *The Arrogance of Power. The Secret World of Richard Nixon.* (Gollancz, 2000). 377.
[104] ibid, 375.

pursued energetically, but he cautioned his White House collaborators that covert activities must not be traceable to him.[105]

Among the illegal activities sanctioned by the White House were a hundred 'political' break-ins, targeting financial records, tapes, correspondence and even medical records. Others included wiretaps and the warrantless interception of telephone calls. These attacks on privacy followed a consistent pattern: all the victims were of political concern to the Nixon Administration. It is one of the grotesque ironies of Nixon's use of technology for surveillance purposes that a taping system he ordered to be installed in the Oval Office was destined to yield much of the evidence that established beyond doubt that Nixon and senior members of his staff had been engaged from the beginning of his Presidency in gross violations of privacy law and of the rule of law in general. Speaking of the wiretaps and break-ins, a Republican Senator, Lowell Weicker, observed that the Fourth Amendment guarantee of the right of the people to be secure on their persons, houses papers and effects, against unreasonable searches and seizures, 'was expressly violated' and that these violations by Nixon's White House had been its 'greatest distortion of the political system.' [106] On March 8, 1971, several Vietnam protestors broke into an FBI field office in Pennsylvania in search of proof that the agency was illegally monitoring left-wing activists. They stole hundreds of documents, some of which substantiated the concerns which motivated their break-in. Over the following months, the burglars mailed documents from the stolen cache to several journalists, including Betty Medsger at *The Washington Post*. *The Post* published a series of articles based on the documents, revealing how 'the FBI was spying on political activists, and actively trying to disrupt their activities'.[107]

In the summer of 1971, Nixon established a secret investigative unit that would respond directly to the Oval Office. This group consisted of five men, who soon became known as the 'Plumbers' who, on 16/17 June 1973, broke into the Democratic National Committee office in the Watergate Building in Washington. They had been in the building for about an hour when police caught them in the act, and arrested them. They had electronic equipment,

[105] ibid, 377.
[106] ibid, 393.
[107] Betty Medsger, *The Burglary - the Discovery of J. Edgar Hoover's Secret FBI*. (Alfred Knopf, 2014).

cameras and dozens of rolls of film. One of them was identified as James McCord, a member of the 'Committee to Re-Elect the President.' Another was Howard Hunt, holder of a White House Pass, and reportedly used by the White House 'as a consultant on a highly confidential matter.' It soon emerged that four of the five burglars were veterans of CIA operations. When the F.B.I. began trying to discover who had been involved in the planning of the break-in, the White House began trying to prevent them from finding out, and went into cover-up mode with the clear intent of obstructing justice.[108] By joining the cover-up and by asking the C.I.A. to remove the F.B.I. from the investigation, Nixon was threatening to corrupt important agencies of government. Further, in approving of, and even suggesting, burglaries without Court warrants against political adversaries, Nixon was usurping the historic role of the judicial branch of government. Nixon's standpoint, almost to the end, was based on an exaggerated estimate of the scope of Presidential privilege: 'If the President does it, that means it's not illegal.'[109] When Gerald Ford succeeded Nixon as president, he appeared to herald an end to the illegal privacy-invasive practices of his predecessor: 'Our great Republic is [now] a government of laws, not of men'.[110]

5.0 Church Committee Report and the Balance Between National Security and Personal Liberties Pre-9/11

In the light of the multiple revelations by the Church Committee of illegal privacy-invasive surveillance programmes conducted by U.S. Intelligence agencies, at the cost of fundamental constitutional liberties, the source of many of those revelations being those who participated in these programmes, there can be little doubt that privacy/security balance veered strongly towards national security until the enactment of the Foreign Intelligence Surveillance Act of 1978 [FISA] provided a legal framework capable of limiting and guiding intelligence agencies. This was the model recommended by the Church Committee.

[108] David Frost *Frost/Nixon* (London, 2007), pp xi-xii.
[109] ibid, xii and 207ff. See Jim McGee, 'The Rise of the F.B.I.,' *The Washington Post Magazine* 20 July, 1997.; F.B.I.'s 'Political Abuses.' *U.S. News and World Report* (December 15, 1975). 61.; Amitai Etzioni, 'Implications of Select New Technologies for individual Rights and Public Safety.' (2002) 15 (2) *Harvard Journal of Law and Technology* 257, 287 onwards.
[110] Andrew Rudalevige, 'The New Imperial Presidency' (University of Michigan Press, 2005) 100-1.

The nature of the balance, or imbalance, between national security and data privacy prevailing up to the passage of FISA can be attributed to a number of factors. One of these, identified in the Church Committee Report, was that the FBI, CIA and NSA escaped meaningful Congressional oversight and scrutiny. The Church Committee found that there was 'a clear and sustained failure by those responsible [the legislators] to control the intelligence community and to ensure its accountability.'[111] In its Report, the Church Committee drew attention to a number of fundamental institutional flaws that allowed intelligence agencies to subvert such personal liberties as the privacy of personal data in the name of national security. Malleable terms such as 'subversion', 'national security' and 'foreign intelligence' provided intelligence agencies with opportunities to collect information. The Church Committee Report draws attention to the ambiguity of the term 'subversive'. The Report also observes that where statutes do exist, as with the CIA, they are vague and fail to provide the necessary guidelines defining missions and institutions.[112] The Report also points out that '[t]he absence of precise standards for intelligence investigations of Americans contributed to over-breadth [of surveillance]'.[113] Another contributing factor to the distortion of the privacy/national security balance was that senior executive intelligence officials furthered a culture of impunity by giving implicit directions to operatives to violate the law.[114] A third contributing factor was that the intelligence community presumed, with some show of reason over a long period, absolute and permanent secrecy of their operations.[115] It was natural that not anticipating testing of their activities by Congress or public opinion, these agencies should have acted with greater impunity and less adherence to reasonable interpretations of whatever law, however exiguous, applied in relation to their activities. Fourthly, in the absence of Congressional oversight, intelligence agencies felt themselves able

[111] Church Committee Report, Book 2, 15.
[112] Church Committee Report, Book 1, 4.
[113] Church Committee Report, Book 2, 165.
[114] Church Committee Report, Book 1, 11.
[115] ibid.

to act like a 'monarchical executive', unaccountable to any coequal branch of government.[116]

The evidence outlined above indicates that the data privacy/national security balance was determined, during the period prior to the passage of FISA, largely by excessive surveillance measures undertaken by U.S. Intelligence agencies. As the Church Committee discovered, the overwhelming number of excesses continuing over a prolonged period of time was due in large measure to the fact that the system of checks and balances created in the U.S. Constitution to limit abuse of governmental power was seldom applied to the intelligence community. Guidance and regulation from outside the Intelligence agencies, where it was imposed at all, had been vague. The Church Committee enquiry found that '[p]residents and other senior Executive officials, particularly the Attorney General, have virtually abdicated their Constitutional responsibility to oversee and set standards for intelligence activity'.[117] Another finding was that senior government officials generally gave the intelligence agencies 'broad, general mandates for immediate results on pressing problems', and in neither case 'did they provide guidance to prevent excess.'[118] Furthermore, 'their broad mandates often resulted in excessive or improper intelligence activity'.[119] As for Congress, as well as declining to exercise effective oversight, it passed laws or made statements which were interpreted by Intelligence agencies as supporting overly-broad investigations.[120]

There is an explanation for the failure of Congress to exercise any but minimal oversight of intelligence activities for nearly thirty years. The National Security Act of 1947, which created the CIA, did not include statutory Congressional oversight provisions. This position changed following revelations in 1974 by the then New York Times from Seymour Hersh that U.S. Intelligence agencies

[116] Frederick A.O. Schwartz and Aziz Huq, *Unchecked and Unbalanced: Presidential Power in a Time of Terror* (The New Press, 2007), 2; see Church Committee Report, 'unchecked power is prone to unwise, inefficient application and ….leads inescapably to abuse,' Church Committee Report, Book 1, 50; Walter F. Mondale, Robert A. Stein and Monica C. Fahnhorst, 'National Security and the Constitution: A Conversation Between Wallter F. Mondale and Robert A. Stein' 98 (2014) *Minnesota Law Review* 2011.
[117] Church Committee Report, Book 2, 14.
[118] ibid.
[119] ibid.
[120] ibid.

engaged in domestic spying.[121] As a consequence, the Church Committee's subsequent investigation, as Johnson points out, 'did nothing less than revolutionize America's attitudes towards intelligence supervision'[122] and then, as a consequence, helped to tilt the privacy/national security balance in favour of privacy.

6.0 Judicial Oversight of Surveillance in the name of National Security: Implications for the Data Privacy/National Security Balance.

Until the mid-1970s, judges had relatively little to say about intelligence activities undertaken in the interest of national security. Since such activities are almost always related to foreign affairs, judges avoided jurisdiction over most intelligence controversies under the 'political question' doctrine, which 'allocates the resolution of national security disputes to the two political branches of government: the executive and legislative branches.[123] However, by 1980, the then Attorney General, Benjamin Civiletti could write that '[a]lthough there may continue to be some confusion about how the law applies to a particular matter, there is no longer any doubt that intelligence activities are subject to definable legal standards'.[124]

With the development of sophisticated forms of surveillance technology, which enabled intelligence agencies to collect data without physical searches, and intelligence agencies choosing Constitutional boundaries, the Supreme Court intervened to restrict domestic surveillance activities, at the same time redefining the scope of the Fourth Amendment to curb overreach by intelligence agencies. Under the Fourth Amendment, an impartial magistrate

[121] Seymore Hersh, 'Huge CIA Operation Reported in U.S. Against AntiWar Forces, Other Dissidents in Nixon Years' *New York Times*, December 22, 1974.

[122] Loch K. Johnson, 'The Church Committee Investigation of 1975 and the Evolution of Modern Intelligence Accountability' 23 (2008) *Intelligence and National Security* 198, 199; see also Johnson's book *America's Secret Power: the CIA in a Democratic Society* (Oxford University Press, New York, 1989) in which Johnson characterises the first phase of modern intelligence in the U.S. from 1947 to 1974 as 'the Era of Trust…a time when the intelligence agencies were permitted almost complete discretion to chart their own courses.' 9. William Colby, Director of the CIA from 1973 to 1976 concurs: 'The old tradition was that you don't ask: It was a consensus that intelligence was apart from the rules……that was the reason that we did step over the line in a few cases, largely because no one was watching. No one was there to say don't do that.' Cited in Genevieve Lester, 'External Accountability: Congress, Opposition, and Oversight Development,' unpublished Ph.D Dissertation, U.C. Berkley, 2012.

[123] Frederic F. Manget, 'Intelligence and the Rise of Judicial Intervention' 15(2) (1995) *The Journal of Conflict Studies* 43, 44.

[124] Benjami Civiletti, 'Intelligence Gathering and the Law: Conflict or Compatibility?' 48(6) (1980) *Fordham Law Review* 883, 891.

had to rule on the validity of a search before it could be conducted. The Amendment provided that:

> The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[125]

In *Katz v United States*[126] the Court overruled a prior decision[127] and held that the Fourth Amendment prohibits warrantless electronic surveillance, recognising that electronic surveillance can be just as invasive as physical entry of a private space.[128] *Katz* was not relevant in the context of the data privacy/national security balance, since it did not involve national security. Furthermore, the Court did not consider the scope of the Fourth Amendment in the national security context. However, the majority in *Katz* inserted a footnote to the judgment to the effect that there was possibly an exception from the warrant requirement in cases involving national security.[129] The contents of the footnote was challenged by one of the concurring Justices, Justice Douglas, who argued that the President (or his agent) could not be 'detached, disinterested and neutral'[130] in cases involving national security, on the basis that the Fourth Amendment did not permit the executive branch to fulfil the inherently incompatible positions of adversary, prosecutor and neutral, disinterested magistrate.[131] In response to *Katz*, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968, to govern wiretapping and electronic surveillance, in addition to codifying the dicta in *Katz* and explicitly exempting any surveillance relating to national security

[125] For a background to the Fourth Amendment see Anthony G. Amsterdam, 'Perspectives on the Fourth Amendment' 58 (1973-74) *Minnesota Law Review* 349; Silas J Wasserstorm and Louis Michael Seidman, 'The Fourth Amendment as Constitutional Theory' 77 (1988-89) *Georgetown Law Journal* 19-112.
[126] 389, U.S. 347 (1967).
[127] In *Olmstead v United States*, 277 U.S. 438 (1928).
[128] This holding was codified in the Omnibus Crime Control and Safe Streets Act of 1968 42 U.S.C. § 3789d.
[129] *Katz v United States* 389 U.S. 358, fn 23. The footnote reads: 'Whether safeguards other than prior authorisation by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case.'
[130] ibid, at 347.
[131] ibid, at 360.

information from procedural requirements in Title III. Title III of the Act provided that:

> Nothing shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect security information against foreign intelligence activities.[132]

Congress, in enacting Title III, in effect facilitated a change in the balance between data privacy and national security, helping to tip the balance in favour of national security at the expense of data privacy. The principle enunciated in Title III, namely that the President enjoyed unlimited constitutional power to obtain, necessarily as a result of surveillance conducted by intelligence agencies, foreign intelligence information deemed [by him] to be essential to the security of the United States and to protect national security information against foreign intelligence activities, incentivised intelligence agencies to conduct excessive secret surveillance of citizens' data in the name of national security. This overboard secret surveillance by NSA, CIA and FBI operatives was conducted in the knowledge that statute law, as exemplified in Title II, did not provide that whatever secret intelligence activities they were engaged in, overbroad or otherwise, in the name of national security were subject to constitutional processes.

In *United States District Court for the Eastern District of Michigan* (*Keith*), while the Court was conscious of the risk of executive overreach in the name of national security, it stressed that its decision was limited to domestic security, and expressed no opinion on warrantless surveillance of 'foreign powers or their agents'.[133] The Supreme Court's dealings with executive overreach in the name of domestic security did not come to terms with executive overreach in national security cases. Following *Keith*, the U.S. Department of Justice limited warrantless wiretapping to cases involving 'a significant connection with a

[132] Omnibus Crime Control And Safe Streets Act Of 1968 42 U.S.C. § 3789d.
[133] 407 U.S., (1972), at paras 321-22.

foreign power, its agents or agencies,' but, significantly, did not apply that limitation to the NSA's electronic programmes.[134]

7.0 FISA: Adjusting the Data Privacy/National Security Balance? Restricting the Interpretation of Personal Data in the Context of Intelligence Surveillance by the Executive Branch in the name of National Security

The enactment of FISA was a response by Congress to the findings of the Church Committee that the privacy rights of U.S. citizens had been consistently and intensively violated by the Executive branch of government and its intelligence agencies over a long period in the name of national security. The privacy rights in question involve the protection of individuals from unwanted or harmful uses of their personal data. In the United States, the protection of these rights is mandated by the Fourth Amendment to the U.S. Constitution, which guarantees 'the right of the people to be secure in their persons, houses, papers and effects.' A Senate Report stated that Congress enacted FISA 'in large measure [as] a response to the revelations that warrantless electronic surveillance in the name of national security had been seriously abused,'[135] and that the changes embodied in FISA were intended to strike 'a fair and just balance between protection of national security and protection of personal liberties.'[136] Another response was the creation by Congress of the Senate and House Select Committees on Intelligence to 'provide the requisite oversight of intelligence agencies.'[137] The purpose of these Intelligence Committees was to 'serve as a permanent check on executive authority, deterring intelligence agencies from engaging in the overreach that led to the formation of the Church Committee.'[138]

The fundamental task facing Congress was to find an appropriate balance between security and liberty. FISA was also a response to the reluctance of the Supreme Court to decide on an issue central to the data privacy/national security balance: whether the traditional assertion by the Executive of a power

[134] Church Committee Report, Book 2, 189.
[135] Senate Report. No. 95-604 (1977). Reprinted in 1978 U.S.C.C.A.N. at 3905-06, 7.
[136] ibid, 9.
[137] Senate Resolution 400, 94th Congress (1976).
[138] Walter F. Mondale, Robert A. Stein and Caitlinrose Fisher, 'No Longer a Neutral Magistrate: The Foreign Intelligence Surveillance Court in the Wake of the War on Terror' (2016) 100 *Minnesota Law Review* 2251, 2262. Senator Walter F. Mondale, elected U.S. Vice-President in 1976, was an instrumental members of the Church Committee.

to search and seize outside the Fourth Amendment's ordinary requirements when acting to obtain intelligence for national security purposes.[139]

The official, positive view of FISA was that it created a framework of checks and balances in which the Executive could continue 'to wield extensive intelligence, but must comply with numerous substantive and procedural requirements when exercising this power.' [140] This optimistic trend was reflected in President Carter's signing statement on 25 October 1978. The President expressed confidence that the FISA legislation had struck a balance between adequate intelligence to guarantee the security of the U.S., on the one hand, and the preservation of basic human rights on the other. He suggested that FISA would assure that intelligence officials would act 'lawfully' and would 'remove any doubt about the legality of those surveillances which are conducted to protect our country against espionage and international terrorism.'[141] Brand points out that President Carter's optimistic signing statement 'gave no hint of the complexity of the statutory framework on which the legislation rested and the tensions in the Act that would help to undo it.'[142] However, as Brand also remarks:

> It is difficult to chide the President for the hopes he expressed for FISA. The legislation was, in retrospect, a bold first effort. At the time, the need for a search warrant to engage in foreign intelligence had yet to be resolved, and Congress had never enacted legislation in the area.[143]

It is worth noting, in this context, that prior to the passage of FISA:

---

[139] Jed Rubenfeld, 'The End of Privacy: Presidential Power and the Fourth Amendment' 61 (2008) *Stanford Law Review* 101,158; Kim L. Kelley, 'The Foreign Intelligence Surveillance Act of 1978' 13 (1980) *Vanderbilt Journal of Transnational Law* 719-760; Christine A. Burke, 'Foreign Intelligence Surveillance: Intelligence Gathering of Persecution?' 6(3) (1982) *Fordham International Law Journal* 501-529; Robert Bloom and William J. Dunn, 'The Constitutional Infirmity of Warrantless N..S.A. Surveillance: The Abuse of presidential Power and the Injury to the Fourth Amendment' 15 (2006) *William and Mary Bill of Rights Journal* 147-202.

[140] Jed Rubenfeld, 'The End of Privacy: Presidential Power and the Fourth Amendment' 61 (2008) *Stanford Law Review* 101, 158.

[141] Foreign Intelligence Surveillance Act 1978. Statement on signing S. 1566 Into Law. October 25, 1978. The American Presidency Project, <http://www.presidency.ucsb.edu/ws/?pid=30048> accessed 27 November 2016.

[142] Jeffrey S. Brand, 'Eavesdropping on our Founding Fathers: How a Return to the Republic's Core Democratic Values Can Help Us Resolve the Surveillance Crisis' 6(1) (2015) *Harvard National Security Journal* 1 7.

[143] ibid.

> [H]istory had suggested that warrantless searches for foreign intelligence purposes were lawful. For example, in 1940, President Roosevelt stated his view that electronic surveillance was appropriate where "grave matters involving defense of the nation" were involved.' President Truman took a similar position.' Warrantless surveillance for foreign intelligence was pervasive by the time of the Kennedy Administration.[144]

7.1 Provisions of FISA

FISA embodies a system which provides for two kinds of checking mechanisms upon the implementation of foreign intelligence electronic surveillance if this surveillance is to be deemed permissible. In chronological order, the first system of checks is internal, and involves the Executive; the second is external and judicial, involving a Secret Court, the Foreign Intelligence Surveillance Court, (FISC), which is required to authorise such warrants where there is 'probable cause to believe that the target of surveillance is a foreign power, an agent of a foreign power or a terrorist group,' [145] and that each of the facilities or places at which the surveillance is directed, is being used, or is about to be used, by a foreign power or an agent of a foreign power. Under the FISA statute, 'agents of a foreign power' include persons who knowingly engage in, or aid and abet, or conspire to commit sabotage for or on behalf of a foreign power (including al Qaeda), in addition to other non-U.S. persons who act in the United States as officers of a foreign power.[146] FISA provides for the possibility that urgent circumstances might require the government to undertake surveillance for up to seventy-two hours before there is time to secure the authorisation of the FISC.[147]

FISA was intended to be a prophylactic against the recurrence of the endemic misuse of intelligence agencies for purely political purposes which prevailed before the introduction of FISA. There was no effective limitation on wiretaps

[144] ibid. For background to this see Kim L. Kelley, 'The Foreign Intelligence Surveillance Act of 1978' 13 (1980) *Vanderbilt Journal of Transnational Law* 719, 720-731.
[145] 50 U.S.C.A., Section 1805(a) (3). The standard of proof here appears to be lower than that applied in criminal proceedings. See James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts, New York Times*, Dec. 16, 2005. <http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all> accessed 3 December 2016. Cited in Sinha Alex G., 'NSA Surveillance Since 9/11 and the Human Right to Privacy' (2013) 59 *Loyola Law Review* 861, 864, fn 4.
[146] 50 U.S.C. 1801 (b).
[147] 50 U.S.C.A, Section 1805(f).

for national security reasons until the passage of FISA. The policy of the Executive during the pre-FISA period, as Birkenstock points out, 'was demonstrated by Attorney General Brownell's 1954 Directive for the FBI to conduct warrantless searches and seizures, by surreptitious means if necessary whenever the Bureau determined that the interests of national security required the search.'[148]

FISA, by introducing a measure of judicial review, created the potential to screen for such misuse. As a further means of achieving this purpose, FISA built in severe criminal penalties for anybody violating its provisions, mandating up to five years' imprisonment and 10,000 Dollars in fines for any government official who 'engages in electronic surveillance under color of law except as authorised.' [under FISA] [149] These provisions, at any rate, in the context of the data privacy/national security balance, represented a gesture towards striking a fair and just balance between the protection of national security and the protection of personal liberties including data privacy. On the one hand, while FISA, in its initial form, provided for a limited range of surveillance activities, authorising only wiretaps and bugs, it was subsequently amended pre-9/11 to sanction a wider range of such activities: physical searches, pen registers, trap and trace devices and business records.[150] It may be significant that the official title of the FISA Act does not make mention of the privacy it was designed to protect: 'An Act to authorize Electronic Surveillance to obtain Foreign Intelligence Information.'[151]

The substantive provisions of FISA deal with the procedures to be followed for security approval from the judiciary in the form of FISC or the Attorney General, to conduct electronic surveillance. The application of these procedures is not always predictable. For example, the Attorney General may authorise immediate surveillance in times of emergency without having recourse to the FISC [152] and electronic surveillance may be conducted without a

[148] Gregory E. Birkenstock, 'The Foreign Intelligence Surveillance Act and Standards of Probable Cause: An Alternative Analysis' 80 (1992) *Georgetown Law Journal* 843, 846-49.
[149] 50 U.S.C., Section 1809 (a) (c).
[150] Intelligence Authorisation Act for the Fiscal Year 1999, Public Law No. 105-272, Section 601(2), 112 Stat. 2396, 2405-5.
[151] Foreign Intelligence Surveillance Act 1978, Pub.L. 95–511, 92 Stat. 1783, 50 U.S.C.
[152] Notwithstanding any other law, the President through the Attorney General, may authorise surveillance without a Court order.' 1802 (a) (1).

warrant from the FISC that government will comply with statutory 'minimization procedures' and that there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a 'United States person is a party.'[153] 'Minimisation procedures' are defined as 'specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light if the purpose and technique of the particular surveillance, to minimise the acquisition and retention of data.'[154] Judicial review by the FISC applies to all other circumstances in which the government wants to conduct electronic surveillance. The government application for a search order must be made to the FISC with the written approval of the Attorney General, contain a description of the target of the surveillance and the proposed minimisation procedures.[155] The application must also certify that the information targeted by the proposed foreign surveillance is foreign intelligence information and that 'normal' techniques could not obtain the desired information, and contain evidence in support of these certificates.[156] These complex procedures having been completed, the task of the FISC is to review each application with a view to approving or rejecting it.[157]

7.2 The Problems with FISA

It is instructive to study the findings and recommendations of the Church Committee Report in conjunction with the provisions of FISA. FISA was framed as a legislative response to the Church Committee report and a corrective to government surveillance systems which facilitated the subversion of civil liberties, including data privacy, in the name of defending national security. Engaging in a comparison between the Church Committee Report and the provisions of FISA had led many commentators to conclude that its structure and its agenda for shared responsibility among the branches of government did not provide a credible basis for finding an appropriate balance between national security and data privacy. One of the leading commentators

[153] ibid, at 1801(1).
[154] ibid, at 1801(h).
[155] 1804 (a) (1) - (b).
[156] ibid.
[157] What Brand describes as 'the tangled web of provisions' embodied in FISA is subjected to detailed analysis. See Jeffrey S. Brand, 'Eavesdropping on our Founding Fathers: How a Return to the Republic's Core Democratic Values Can Help Us Resolve the Surveillance Crisis' 6(1) (2015) *Harvard National Security Journal* 1.

in this field, Brand, identifies the structure of the FISC as FISA's 'Achilles heel.'[158]

In its preoccupation with preserving the secrecy of FISC, FISA resorted to creating a non-adversarial process in which warrants are issued by FISC on the basis of information provided almost exclusively by the Executive Branch of government, the party which is seeking the warrants. As Brand points out: '[f]or the most part, opposition parties, cross-examination of government witnesses, and opposing arguments - the staples of the American justice system- are absent. The proceedings are conducted entirely in secret.'[159]

From the Government's point of view, it is because the FISC deals with ongoing and sensitive national security issues, the inner workings of the FISC are largely kept secret.[160] Vladeck points out that the secrecy dimension of the FISC originated in a compromise between Congress and the Executive following the Church Committee's findings of intelligence abuses in the 1970s. This compromise involved an agreement on the part of the Executive 'to have many of its foreign intelligence surveillance activities subjected to greater legal oversight and accountability, in exchange for which Congress and the Courts agreed to provide such oversight and accountability in secret.'[161] Squitieri argues that 'it is precisely because the FISC operates under a layer of secrecy that a special advocate is desirable.' [162] Benkler points out that the secretive nature of national security law can result in an 'echo chamber,' [163] with Squitieri contending that when this arises, 'similarly situated and isolated actors have a reduced opportunity to have their presumptions and conclusions tested by "outside" opinions,'[164] and cites an example highlighting this point. The leaks by Edward Snowden revealed that the FISC was interpreting Section 215 of the Patriot Act broadly, authorising the government's bulk telephone

[158] ibid.
[159] ibid.
[160] Joel Samaha, *Criminal Procedure* (Cengage Learning 9th edition 2015) 584.
[161] Stephen J. Vladeck, 'The FISA Court and Article III' 72(3) (2015) *Washington and Lee Law Review* 1161, 1164.
[162] Chad Squitieri, 'The Limits Of The Freedom Act's Amicus Curiae' 11(3) (2015) *Washington Journal Of Law, Technology and Arts* 197, 201.
[163] Yochai Benkler, 'A Public Accountability Defence for National Security Leakers and Whistelblowers' 8 (2014) *Harvard Law and Policy Review* 281, 285.
[164] Chad Squitieri, 'The Limits Of The Freedom Act's Amicus Curiae' 11(3) (2015) *Washington Journal Of Law, Technology and Arts* 197, 201.

metadata collection programme.[165] However, the United States Court of Appeals for the Second Circuit came to a different conclusion, holding that Section 215 of the Patriot Act did not authorise such a widespread collection programme.[166] While acknowledging that the Second Circuit's opinion represents just one decision, Squitieri observes that 'it is revealing that two Courts interpreting the same law came to such drastically different outcomes, with the FISC operating on an *ex parte* basis, and the Second Circuit operating within a traditional adversarial setting.[167]

Although these two conflicting judgments, involving the FISC and the Second Circuit, cover a period later than that covered in the present chapter, the secrecy of the FISC Court remains a constant, as do the issues this secrecy gives rise to. In relation to the fact that the FISC deemed that Section 215 of the Patriot Act authorised mass surveillance and the Second Circuit concluded that it did not, one legal scholar observed that '[t]he Patriot Act didn't authorise bulk surveillance; the FISC did, based on a major misreading of the Patriot Act.'[168] The 'major misreading' of the Patriot Act referred to by Kerr is better described as a major redaction of that Act brought about by the intervention of the Department of Justice, whose lawyers persuaded the secret FISA Court (the FISC) to change a law that was intended to facilitate targeted surveillance, was never intended to authorise mass surveillance, and to agree that the law could be stretched to authorise mass surveillance.[169]

A further departure from U.S. Constitutional judicial structure was exemplified in the selection of FISC judges, who are handpicked by the Chief Justice of the U.S. Supreme Court. What Brand calls 'FISA's precarious balancing act' relied on a number of dubious assumptions. One of these was that the Foreign intelligence Surveillance Court (FISC) and the Foreign Intelligence Surveillance Court of Review (FISCR) could oversee the maintenance of the

---

[165] ibid.
[166] *ACLU v Clapper*, 785 F. 3d 787, 826 (2nd Circuit) 2015.
[167] Chad Squitieri, 'The Limits Of The Freedom Act's Amicus Curiae' 11(3) (2015) *Washington Journal Of Law, Technology and Arts* 197, 202.
[168] Orin Kerr, 'How much has Congress changed on surveillance?' (2 June 2015) *The Washington Post* <https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/06/02/how-much-has-congress-changed-on surveillance/?utm_term=.d75a549c11e0> Accessed 29 December 2016.
[169] See Bruce Schneier, *Data And Goliath: The Hidden Battles to Collect Your Data and Control Your World* (W.W. Norton and Company, New York and London, 2015) 173-74.

delicate balance between privacy and national security 'in non-adversarial, closed proceedings where deliberations were limited to remain secret.' [170] FISA created a FISA Court of Review, made up of three federal district or appeals court judges on the FISA Court.[171]

Another problem was that the success of FISA depended on the good faith of the Executive Branch in the execution of its duties and the expectation of effective Congressional oversight. FISA required the FISC to report to the House and Senate Intelligence Committees regarding its overall activities.[172] Brand remarks that each of these assumptions would prove flawed.[173] One reservation about the FISA Court's procedures was that no institutionalised means existed of challenging a FISA judge's initial analysis. Another is that during the period up to 9/11 the provisions of FISA meant that only the Government had the authority to appeal most FISC decisions, hence those decisions were seldom subject to the normal judicial process of collaborative review. The result as Berman points out, was that:

> Novel and complex legal questions have therefore been left in the hands of the one man or woman who happened to be on duty the week that they arose. This system compounded the FISA Court's failure to fully analyze the government's justification for the bulk-collection programs **by** providing that one FISA judge's decision was in essence the final word on the subject.[174]

Since these bulk collection programmes have the capacity to compromise the data privacy of untold numbers of Americans, they therefore have the capacity to tilt the data privacy/national security balance in favour of the latter, and so frustrate the original purpose of the FISA legislation which was enacted by Congress to restrict the ability of Government to engage in the overbroad collection of citizens' data.

---

[170] ibid.
[171] 50 U.S.C.A. Section 1803(b).
[172] 50 U.S.C. Section 1802(a).
[173] Jeffrey S. Brand, 'Eavesdropping on our Founding Fathers: How a Return to the Republic's Core Democratic Values Can Help Us Resolve the Surveillance Crisis' 6(1) (2015) *Harvard National Security Journal* 1, 12.
[174] See Emily Berman, 'The Two Faces of the Foreign Intelligence Surveillance Court' 91 (2016) *Indiana Law Journal* 1191, 1193.

Other reservations commonly expressed concern about the secrecy, and hence the lack of transparency, surrounding the proceedings of the FISC. These reservations are based on the premise that transparency of judicial action, like adversarial proceedings, should constitute an exemplary norm for all Courts. Proponents of this point of view have argued that 'exposing judicial proceedings to public scrutiny draws attention to flawed or unresponsive rulings, as well as potentially undesirable developments in the law.'[175] Other arguments for the transparency of the FISC are that 'when a judge's work will not be subject to public scrutiny and critique, it becomes easier for the judge to engage in incomplete, unconvincing or otherwise flawed analysis.'[176] Berman makes the point that 'citizens are more likely to trust in their government's good faith when a full account of its activities is available.'[177]

The original role of the FISC, and the one it was mandated to play under the provisions of FISA was that of a gatekeeper. This continued to be its role from the passage of FISA in 1978 until post-9/11, when it was given an additional and entirely different role: that of rule-maker.[178] When the FISC operates as a gatekeeper it is acting as a watchdog. Prior to the passage of the USA Patriot Act of 2001, the nature of FISA's statutory requirements for intelligence collection necessitated a narrow scope for the Court's operations. Its role was confined to evaluating ex parte applications for intelligence collection directed at specific, individual targets. These applications, requiring the Attorney General's approval, are generated in the National Security Division of the Department of Justice, on behalf of a National Intelligence Agency, whether it be the CIA, FBI or the NSA, requesting surveillance authority. Under the terms of FISA, the FISC judge must make an independent determination of whether the government has met the necessary standard.

The requirement that the FISC must make an independent determination in the case of each application is relevant in the context of a curious feature of the FISC's treatment of government requests for surveillance approval. Statistical

[175] See Alan Butler, 'Standing Up to Clapper: How to Increase Transparency and Oversight of FISA Surveillance' 45 (2013) *New England Law Review* 55, 86-88.
[176] Oren Bar-Gill and Barry Friedman, 'Taking Warrants Seriously' 106(4) (2012) *Northwestern Law Review* 1609, 1640.
[177] Emily Berman, 'The Two Faces of the Foreign Intelligence Surveillance Court' 91 (2016) *Indiana Law Journal* 1191,1204.
[178] ibid, at 1245.

records show that the FISC, during the pre-9/11 period, almost invariably acceded to government requests for warrants to conduct surveillance on American citizens and permanent residents. According to statistics compiled by The Electronic Privacy Information Centre, between 1978 and 2011, there were only eleven rejected applications out of thousands submitted with all the rejections occurring in 2003 or later.[179] Between 1978 and 2001, when President Bush ordered the NSA to begin surveillance operations outside the FISA framework, the government submitted a total of 13,102 requests to eavesdrop on Americans, the FISC requested modifications to only two of these requests, and ultimately approved all of them.[180] A number of explanations for these statistics might be offered. One is that the FISC Court is meant to approve all wiretaps placed inside America for intelligence gathering purposes. Another is that the terms of FISA provide that the FISC must authorise warrants where there is probable cause to believe that the target of surveillance is an agent of a foreign State or a terrorist group,'[181] the standard of providing 'probable cause' is lower than the standards applied in typical criminal proceedings.[182] It is also possible that the government agencies, when applying for warrants, were meticulous in ensuring that their applications conformed to the terms of FISA and that the most rigorous scrutiny of FISA requests is done within the Justice Department. Whatever explanation may be offered, it can only amount to speculation, since we are dealing with the deliberations of a secret court. When it comes to determining the influence of FISA on the data privacy/national security balance, similar difficulties prevail. If the FISC has been functioning, in effect, not as a watchdog protecting data privacy interests from overbroad government surveillance of personal data, but instead as a facilitatory rubber stamp for such surveillance, FISA can scarcely be regarded as the kind of corrective response advocated in the Church Committee Report to government surveillance systems which had been subverting data privacy rights in the name of defending national security.

[179] 'Foreign Intelligence Surveillance Act Court Orders, 1979-2015.' *Electronic Privacy Information Centre* <https://www.epic.org/privacy/surveillance/fisa/stats/> accessed 3 December 2016.
[180] Alex G Sinah. 'NSA Surveillance Since 9/11 and the Human Right to Privacy' 59 (2013) *Loyola Law Review* 861, 874.
[181] 50 U.S.C.A. Section 1805(a).
[182] Alex G Sinah. 'NSA Surveillance Since 9/11 and the Human Right to Privacy' 59 (2013) *Loyola Law Review* 861, 874.

As Breglio points out, some have argued that if more people knew about FISC, 'there would be an uproar about its seemingly undemocratic procedures.'[183] As an explanation of the fact that the FISC denied just four out of thirteen thousand wiretap applications it received between 1992 and 2002, a former Chief Judge of the FISC, Lamberth, attributed the government's almost perfect record in that Court to the 'superb internal review process created within the Department of Justice.' [184] This process requires personal approval of the Attorney General and the head of the requesting intelligence agency on each FISA application. However, notwithstanding Lamberth's claim, it remains true that the FISC's secret procedures rendered it virtually impossible to appeal a surveillance order since 'the defendant might never know that such an order had existed in his case or what proof the government had submitted in respect of it.'[185]

The above considerations suggest that the effect of FISA in adjusting the data privacy/national security balance was at best neutral. However, it has been argued that, far from functioning as a facilitator for government surveillance, the requirements of FISA constitute an unnecessary obstacle to the efficient operation of the surveillance process. In support of this argument, Sievert [186] points out that FISA requires that the federal government prove to a designated federal judge that there is 'probable cause' that a person present in the U.S. is 'an agent of a foreign power' before conducting electronic surveillance to obtain the content of their communications, despite the fact that the criminal law probable cause standard is not constitutionally required for searches conducted to obtain intelligence information in national security cases. This is the position established by the U.S. Supreme Court.[187]

---

[183] Nola K. Breglio, 'Leaving FISA behind: The Need To return to Warrantless Surveillance' 113 (1) (2013) *Yale Law Journal* 179, 190. For negative views of the FISC, see Gerald H Robinson, 'We're Listening! Electronic Eavesdropping, FISA and the Secret Court' 36 (2000) *Williamette Law Review* 51-81.

[184] Benjamin Wittes, 'The FISA Court Speaks' *Legal Times* 19 February 1996, 1 21.

[185] Nola K. Breglio, 'Leaving FISA behind: The Need To return to Warrantless Surveillance' 113 (1) (2013) *Yale Law Journal* 179, 189.

[186] Ronald Sievert, 'The Foreign Intelligence Surveillance Act of 1978 Compared with the Law of Electronic Surveillance in Europe' 43(2) (2016) *American Journal of Criminal Law* 125, 128.

[187] For example, *United States v U.S. District Court* (Keith), 407 U.S. 297 (1972); *Katz v United States*, 389 U.S. 347 (1967).

This exacting standard, Sievert argues, not mandated by the Constitution, has, along with other requirements of FISA, 'created an unnecessarily protracted risk-averse process that is dominated by lawyers, not investigators and intelligence collectors, that have arguably already endangered the safety of U.S. citizens in numerous reported terrorist cases.[188] Sievert's disparaging reference to FISA's insertion of judges into the adjudication of the intelligence collection process in the U.S., has its basis in the not uncommon view that the 'highly technical and nuanced nature of intelligence matters…….. is beyond the scope of most judges.' [189] Similar comments were made by Chief Justice Burger in *CIA v Sims*,[190] who noted that 'judges have little or no background in the delicate business of intelligence gathering,' adding that 'what may seem trivial to the uninformed [i.e. judges] may appear of great moment to one who [presumably investigators and intelligence collectors] has a broad view of the scene and who may put…..information in its proper context.' [191] Sievert refers approvingly to a response by a British Home Secretary to civil liberties organisations that interceptions of communications and such intrusions of privacy should be authorised by the Executive as someone who is responsible by election directly to the British people, and who has a greater understanding of the wider context.[192]

Writing with hindsight of the 9/11 experience, Sievert concluded that FISA was 'an unnecessary obstacle placed upon the government by the 1978 Congress before the advent of Al-Quaeda and ISIS. In matters involving members of these organisations, who are by any definition at war with the U.S., or cases involving a potential weapon of mass destruction, Congress should lower the standard of surveillance in line with the standards followed by our European allies.' [193] It is worth noting, in the context of these remarks that

[188] Ronald Sievert, 'The Foreign Intelligence Surveillance Act of 1978 Compared with the Law of Electronic Surveillance in Europe' 43(2) (2016) *American Journal of Criminal Law* 125, 128. See Also Ronald J. Sievert, 'Time to Rewrite the Ill-Conceived and Dangerous Foreign Intelligence Surveillance Act of 1978' 3(1) (2014) *National Security Law Journal* 47, 82-92.
[189] Ronald Sievert, 'The Foreign Intelligence Surveillance Act of 1978 Compared with the Law of Electronic Surveillance in Europe' 43(2) (2016) *American Journal of Criminal Law* 125, 153.
[190] 471 U.S., 159 (1984) at para 176.
[191] ibid, at para 178.
[192] Ronald Sievert, 'The Foreign Intelligence Surveillance Act of 1978 Compared with the Law of Electronic Surveillance in Europe' 43(2) (2016) *American Journal of Criminal Law* 125, 153.
[193] ibid, at 155.

Sievert is Professor at the George H.W. Bush School of Government, Texas A and M University.

8.0 Balancing Rights which are Qualitatively Different: Philosophical Issues Underlying the Data Privacy/National Security Balancing Paradigm

A basic philosophical question is whether it is reasonable to interfere with data privacy in order to address national security concerns. One approach to this question is to devise a system of national security legislation to protect privacy rights, while achieving national security objectives. To espouse this approach is to believe that national security and civil liberty interests are not mutually exclusive and to contest the position that any increase in security requires a decrease in liberty and that every gain in privacy must be at the cost of security.[194] Also associated with this approach is the view that sacrificing privacy does not automatically make a community more secure, a view that seems to have been vindicated in the case of the U.S. Terrorist Surveillance Programme.[195]

Particularly in times of national emergency, the most compelling point made by national security advocates in favour of even the most extreme data retention measures is that, in the final analysis, if the security of the nation has to be maintained, even at the expense of data privacy, civil liberties will mean very little, and it becomes extremely difficult to preserve civil liberties if the survival of the nations is in the balance. In other words, the protection of data privacy must yield to the larger national interest.[196] On the other hand, civil liberties advocates will suggest that privacy is to be regarded as a cornerstone of democracy, at the heart of liberty in a modern state, essential to the well-being of the individual. Hence, sacrificing privacy in the name of security undermines democracy itself, posing the question: Do we want to be completely secure in a police state?

To return to the original question whether it is reasonable to interfere with data privacy in order to address national security concerns, one answer is that this

[194] This case is argued by Daniel J. Solove, *Northing to Hide: The false Tradeoff Between Privacy and National Security* (Yale University Press, 2001) 34.
[195] See the section headed 'The Consequentialist Defence of the Terrorist Surveillance Programme, 241-252.
[196] See generally, Robert N. Davis, 'Striking the Balance: National Security vs. Civil Liberties,' 29(1) (2003-04) *Brooklyn Journal of International Law* 178-238.

kind of interference is not reasonable if a method can be devised to enforce national security and data privacy without loss on either side. Another answer is that although privacy and national security are both social values, they are different values, and it is not reasonable to trade one value against another. There are at least two grounds for doubting the commensurability of security and liberty interests. The first is that we are weighing collective interests (national security) against the privacy interests of relatively small numbers of individuals: thus the purported balance between data privacy and national security is in reality a proposal to trade off the liberties of the few against the security of the many. The second is that the balancing involves seeking to weigh known present interests (in data privacy) against future uncertainties (in respect of security risk).[197]

A somewhat similar position on the notion of commensurability of security and liberty is that the idea of balancing human rights such as data privacy against national security interests is dangerous and deeply misleading, because it assumes that we should decide which human rights to recognise through a kind of cost-benefit analysis. Those who advance such views reject the idea that even in times of emergency, the demands of the greater good of society must prevail against an individual human right. Those who argue that with regard to non-derogable rights, such as data privacy, there is no scope for balancing rights and interests. This point of view is influenced by the history of the relatively recent past: twentieth-century tyrannies have taught Europeans in particular that protecting the dignity of individual human beings is worth the increased discomfort and risk that respecting human beings may cost the public at large.[198]

However, even Dworkin, the social philosopher most frequently associated with the doctrine that it was not appropriate to try to attempt to balance a human right such as data privacy and a state interest such as national security, also argued that someone who claims that citizens have a right against the government need not go so far as to claim that the state is never justified in

[197] See Lucia Zedner, *Security: Key Ideas in Criminology* (London, Routledge, 2009), 135-6.
[198] See Ronald Dworkin, *Taking Rights Seriously* (Harvard University Press, 1977) 191. Dworkin regarded individual persons' rights as 'trumps.' See also Jeremy Waldron, ed., *Theories of Rights* (Oxford University Press, 1984) 153-167.

overriding that right. Dworkin suggested that the state may override that right when this is necessary to protect the interests of others. This is a common move in popular discussion of these matters: when someone complains about the etiolation of civil liberties in the wake of the response of government to terrorist attacks as was the case post-9/11, someone else responds on behalf of the government: 'Have you considered the rights of those who are blown up by terrorists?' It may be necessary to distinguish between two balancing paradigms: rights versus rights and rights versus social utility. It is not incoherent to argue that the security of the public is also a matter of rights. Consequently, rights are at stake on both sides of the equation, so that some adjustment to the existing balance may be justified to meet a radically new situation.

Reasons other than those already considered might be advanced for regarding balancing as an inadequate normative conception. One is that balancing is time-conditioned and socially conditioned and constitutes an inherently subjective process, depending on who is determining the balance and in what context it is being determined. Data users and data subjects might disagree profoundly on whether a particular compromise constitutes an appropriate balance between their points of view. Furthermore, technological changes often render old balances obsolete. It may also be argued that if 'balancing' is taken literally, this would mean that there is some way of ascertaining whether there is parity between the items being weighed in the balance. The problem here is that there is no method available for doing this. It therefore becomes a question of judgment, and that judgment may be open to dispute about the weights that were deemed to attach to the competing claims.[199]

In relation to the concept of trade-offs in the context of achieving a balance, this concept might be regarded as problematic on the ground that it does not discriminate between divergent conceptions of what it means *to balance*, nor does it provide criteria for judging when a balance has been achieved. Thus, it is not very informative to be told that a balance must be struck between privacy and data retention for security reasons, or that the right balance has been found

[199] Charles D. Raab, 'From Balancing to Steering: New Directions for Data Protections' in Colin J. Bennett and Rebecca Grant (eds.) *Visions of Privacy for the Digital Age* (University of Toronto Press, 1999) 68-93, 69.

between one and the other. Although the balancing paradigm is related to judicial decision, the achievement of a balance may ultimately be a matter of political negotiation, political consensus, or as was the case in the United States post-9/11, authoritative assertion.[200]

Despite the reservations outlined above the balancing paradigm, academic and journalistic discourse tends to be preoccupied with the notion of trade-offs and balancing between privacy and other social values, mainly national security. Bennett and Raab observe that the conception of privacy 'as a value to be balanced against competing values…….has become securely entrenched in data-protection policy and its practical implementation,' with result that 'the issue of trade-offs or balancing not only dominates discussion [of] the social dimension of privacy but is inherent to it.'[201] Such terms as 'trade-off' and 'balancing' have problematic conceptual implications. Undertaking a trade-off implies that one value must be upheld at the expense of the other: data privacy at the expense of security or vice versa. Such an approach by-passes the challenge to reconcile the two values without undermining either, on the basis that what are often regarded as antagonistic or irreconcilable values - for example, privacy and national security - are both indispensable to society.

Whatever reservations scholars may entertain about the conceptual limitations of the data privacy/national security balancing paradigm, the operation of a balancing process involving these two values is an essential component of international law and institutional practice. Under international law, states are obliged to serve as guarantors of human rights such as the right to data privacy on the grounds of general welfare, the protection of other rights, public morality or national security.[202] In doing so, states must balance an individual's right to privacy (including data privacy) against the general welfare of society.[203] It is also worth noting that the definition of public order and morals and the general welfare of society, which the state wants to maintain, varies depending on the given circumstances, so that the views on the privacy-invasive measures deemed necessary for the protection of public security and

[200] Colin J Bennett and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (MIT Press, Cambridge Massachusetts, 2007) 13.
[201] ibid, 19.
[202] Article 29(2) Universal Declaration of Human Rights.
[203] Alexandra Rengel, *Privacy in the 21st Century* (Hotei Publishing, Leiden, 2014) 88.

the justifications for these differ substantially from jurisdiction to jurisdiction. The views and individual circumstances may differ from country to country, but the International Covenant on Civil and Political Rights (ICCPR) makes it clear that individual rights (data privacy, for example) can be infringed by laws which are deemed necessary for the protection of public order and national security.[204] The materials reviewed in this thesis will demonstrate that the degree of such infringement can vary substantially from jurisdiction to jurisdiction, being more extreme in the U.S. for example, than in Europe, and be more extreme in the wake of terrorist threats to national security.

If one considers rights from the standpoint of the liberal idea of rights-based justice, one view is that rights trump absolutely all competing considerations. If we espouse this view, we are forced to conclude that an act that violates the scope of this right is, *ipso facto* unjustifiable. If we place data privacy in this category, and think of it as a right that trumps all competing rights or values, for example, national security, we may well wonder what right could plausibly deserve this degree of protection. Reflection would suggest that the class of absolute rights that would be involved here would most probably be empty, and would exclude the list of rights guaranteed by constitutions. Thus, we must conclude that the idea of rights as trumps enjoying absolute protection is untenable. An alternative account of rights such as data privacy is more plausible. According to this account, only reasons, national security exceptions, for example, that have a special kind of force are sufficient to override the position protected by the right.[205] The structure of rights finds expression in the U.S. Constitutional Rights doctrine: that once an interest has been identified as enjoying protection as a right, actions that infringe upon it are justified by compelling interests. Only reasons that are proportional, under the circumstances, can properly be classified as 'compelling.'[206] The nett point here is that no right is absolute and immune from infringement in any circumstances. This accounts for the use of a balancing process when data privacy rights clash with national security interests.

---

[204] Article 19 para 3, ICCPR, United Nations 1966.
[205] See Frederick Schauer, 'A Comment on the Structure of Rights,' 27 (1993) *Georgia Law Review* 415-34.
[206] See Mattias Kumm, 'Constitutional Rights as Principles. On the Structure and domain of Constitutional Justice. A review essay on A Theory of Constitutional Rights' 2(3) (2004) *International Journal of Constitutional Law* 574, 595.

A number of legal scholars, accepting the notion of a balancing paradigm when the relationship between a human right such as data privacy and societal interests such as national security is in question, have devised what may be described as principled balancing approaches. One of these is Barak,[207] who advocates an approach that translates the basic balancing paradigm into a series of balancing tests, taking into account the importance of the rights and the type of restriction. The point of this approach is that it restricts wide discretion in the balancing, makes the act of balancing more transparent, more structured and more foreseeable. Proportionality is a key component of Barak's 'principled balancing.' The emphasis is on the need always to look for a justification of a limit on human rights and to create a proper dialogue between the judiciary and the political branches of government, thus adding to the objectivity of judicial discretion. Barak describes proportionality as, *stricto sensu*, a consequential test [208] and requires 'an appropriate relationship between the benefit gained by the law limiting a human right (such as privacy) and the harm caused to the right by its limitation. On the 'goal' side of the balancing scale, the evaluation should take into account the importance of the goal (national security, for example) in view of its content, the urgency of its realisation reflected in the harm that would be caused without the restriction, and the probability of that harm.[209]

Aquilina, accepting the appropriateness of the data privacy/national security balancing paradigm in the context of the protection of communities from terrorist violence, also advocates a principled balancing approach as he outlines principles and procedures that might facilitate the achievement of such a balance. These principles include the use by government of the least privacy-

[207] Ahraon Barak, 'Proportionality and Principled Balancing' 4(1) (2010) *Law and Ethics of Human Rights* 1-18.

[208] Moral philosophers may be divided into absolutists and consequentialists. Absolutists hold that there are some kinds of action that are intrinsically wrong and should never be undertaken, irrespective of any consideration of the consequences. Consequentialists, on the other hand, believe that the morality of actions should be judged by their consequences, and that there is no category of act that may not, in special circumstances, be justified by its consequences, a position close to that encapsulated in the doctrine that the end justifies the means. In the context of the data privacy/national security balance a consequentialist might say: The morality of data retention should be judged by its consequences, and there is no category of act, including data retention for state security purposes that may not, in special circumstances, be justified by its consequences (i.e. keeping countries safe from terrorist attacks).

[209] Ahraon Barak, 'Proportionality and Principled Balancing' 4(1) (2010) *Law and Ethics of Human Rights* 1, 2. What Barak is advocating here is a process of 'cost benefit analysis,' which Dworkin condemned.

invasive technology, accountability, transparency, proportionality, fairness, purpose specification, informed consent, legality, purpose limitation, non-retention of data beyond a given timeframe, the right of access by the subject of surveillance to material concerning him or her, and the right of rectification where necessary.[210] Aquilana also argues that without such limitations on government surveillance in the defence of national security, in particular, transparency, proportionality and accountability, the rule of law within a democratic society would be jeopardised. In the light of what is now known about the secret warrantless surveillance activities of the NSA, Aquilina's warning is appropriate:

> The scales of the balance, if no preventive measures are put in place on the State's law enforcement agencies, would tilt in favour of the creation of a police state, to the detriment of democracy. Moreover, 'public security' should be more narrowly defined with more precision in national, regional and international law whilst the threats to public security should be statutorily identified.[211]

The proposition that value judgments cannot be divorced from the balancing process and that balancing is an inherently subjective process, has numerous advantages. To the questions 'What is the proper relationship between human rights and society's interests, and when is the state justified in restricting human rights,?' there is no universally accepted answer, since responses tend to vary from society to society and from one era to another.[212]

The variety of responses in the present era to the above questions reveals several extreme variations within a given era, ranging as they do from outright opposition to any restriction of human rights to a rejection of any restriction of state interference with human rights such as data privacy when the security of the State is in question. It is possible to identify several reasons for the latter

[210] Kevin Aquilina, 'Public security versus privacy in technology law: A balancing act?' 26(2) (2010) *Computer Law and Security Review* 130, 140-142.
[211] ibid, 142.
[212] See Ahron Barack, 'Proportionality and Principled Balancing,' 4(1) (2010) *Law and Ethics of Human Rights* 1, 8.

view, and why the human desire for security is so powerful that it seems easy to trump competing values such as data privacy.[213]

The first reason for the rhetorical power of security is that security in the sense of physical survival is a prerequisite for the enjoyment of other values such as privacy.[214] The second reason is that human risk perception may cause us to overestimate the risk of terrorism and cause us to have difficulty perceiving the harm of reduced privacy.[215] Thirdly, people are apt to think that it is better to have more rather than less security, while this is not the case with privacy. Fourthly, to the extent that national security is obtained at the expense of the privacy of a minority, the majority is more likely not to perceive or care about the privacy costs, and thus regard the security measures as reasonable.[216] Fifthly, social-psychological reactions of solidarity following a terrorist attack 'may cause people to be more willing to set aside individual rights claims such as privacy for a perceived collective benefit in terms of national security.[217] Finally, the Courts tend to defer to governments on matters of national security.[218] In support of this argument, Rivkin, defending the Bush administration response to the September 11 2001 attacks, commented: '[i]n principle, I trust we all agree that liberty and public safety are balanced differently in peacetime than in wartime.'[219]

However, although numerous commentators have raised the objection that balancing is both irrational and subjective, the legal scholar and philosopher, Alexy, has argued that a balancing exercise in relation to the weighing of rights such as data privacy and interests such as national security can be carried out in an effective manner, and that the objection that balancing is inherently irrational and subjective is unjustified.[220] In Alexy's balancing framework, constitutional rights such as data privacy are considered as principles at first

[213] See Jennifer Chandler, 'Privacy Versus National Security: Clarifying the Trade-Off' in Ian Kerr, Valerie Stevens and Carole Lucock (eds)., *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (Oxford University Press, 2009) 131-138.
[214] ibid.
[215] ibid.
[216] ibid.
[217] ibid.
[218] ibid.
[219] David B. Rivkin Jr., 'Answering the Critics of the Legal Case for the War on Terror' 32(2) (2009) *Harvard Journal of Law and Public Policy* 485, 486.
[220] Alexy's approach to balancing is outlined in Robert Alexy, *A Theory of Constitutional Rights* (Oxford University Press, 2002).

sight, but following the consideration of the legal and factual circumstances and the competing principles, such as national security, a principle will be transformed into a rule valid in that particular case through proportionality analysis.[221] Alexy recognises that decision-makers enjoy what he calls 'structural discretion' when addressing competing interests that are crudely of equal weight and where a single answer is unlikely to be inferred from a balancing appraisal.[222] Alexy argues that the exercise of judgment in the adjudication of conflicts between rights, and between rights and collective interests, is inescapable, and that balancing, properly understood and applied, is both rational and legitimate. He bases this conclusion on a detailed analysis of the jurisprudence of the German Federal Constitutional Court, a feature of which is that both constitutional rights and collective goals have the character of principles and that the objectives that these principles enshrine should be realised to the greatest extent possible, given the legal and factual constraints.

According to Alexy, while optimising any given constitutional principle entails its full implementation while no other countervailing principle pulls in a different direction, conflicts between principles can be rationally resolved by balancing each against the other according to the principle of proportionality. The principle of proportionality embodies three sub-principles: 'suitability,' 'necessity,' and 'proportionality in the narrowest sense.' The principle of suitability excludes the use of means to realise any given principle when such means are factually incapable of doing so where realising the given principle would interfere with the fulfilment of any other principle. The principle of necessity requires that if there are several suitable means of realising a given principle, some of which may, as a matter of fact and causation, interfere with the realisation of another principle, the means which least interfered with the other principle should be chosen. The principle of 'proportionality in the narrow sense' (otherwise known as the 'Law of Balancing') requires that, where the fulfilment of a given principle interferes with the realisation of a second one, the extent of the interference must be justified by the importance of satisfying the given one. Alexy's 'Laws of Balancing' are designed to provide a basis on which a number of equally acceptable resolutions of the tension

[221] ibid, 402.
[222] ibid, 414.

between two competing principles may be found. Alexy maintains his theory of principles has always emphasised that balancing is not a procedure which leads necessarily to precisely one outcome in every case, but merely that one outcome can be rationally established in enough cases 'to justify balancing as a method.'[223]

The balancing method has also been used by the European Court of Human Rights, (the ECtHR) which, however, follows a formal sequence of questions different from that discerned by Alexy in the jurisprudence of the German Federal Constitutional Court. In the context of Articles 8 to 11 of the ECHR, interference with a human right such as data privacy must be prescribed by law, necessary in a democratic society in pursuit of one or more specified interests, and proportionate to a pressing social need. However, in most of the cases which reach the ECtHR, Alexy's principles of 'stability' and 'necessity' will already have been answered in the affirmative and Alexy's neat tripartite test will, therefore, have collapsed into a single 'balancing question' : Are the means employed to a given principle factually capable of implementing this principle, while in the circumstances only infringing the competing principle to the maximum degree tolerable by reference to the broader considerations? While Alexy treats constitutional rights and collective goods as competing principles capable of being balanced according to his formula, the ECtHR formally assigns priority to the rights specified in the ECHR, and has the ultimate constitutional responsibility for determining what Convention rights mean.[224] A decision by the Grand Chamber of the ECtHR in 2003 illustrates the approach of that Court to the balancing process. The Court affirmed that

> [P]luralism and democracy are based on a compromise that requires various concessions by individuals or groups of individuals who must sometimes agree to limit some of the freedoms they enjoy in order to guarantee the stability of the country as a whole.[225]

[223] ibid, 402.
[224] See Steven Greer, "Balancing" and the European Court of Human Rights: a contribution to the Habermas-Aleexy Debate' 63(2) (2004) *Cambridge Law Journal* 2-3.
[225] *Refah Partisi (the Welfare Party) and Others v Turkey [GC]* - 41340/98, 41342/98, 41343/98 et al. Judgment 13.2.2003, at para 99.

It can be discerned from the jurisprudence of the ECtHR that the principle of fair balance has long been a feature of its decisions. This arises from the fact that the search for a fair balance between the demands of the general interest of a community and the requirements of the protection of the individual's human rights is inherent in the whole of the ECHR. In the jurisprudence if the ECtHR, at least two discrete functions have been performed by the fair balancing principle. Under the ECHR, two types of proportionality evaluation have been emphasised by the ECtHR. Firstly, the Court has asserted that a 'fair balance must be struck between the right of individual applicants and the general interests of the public.' The second meaning of proportionality is a modified and more specific version of the first and is defined as a reasonable relationship between the means employed, including their severity and duration, and the public objective to be sought.[226] A typical instance of the application of the 'fair balance' principle by the ECtHR is found in the judgment of the Grand Chamber in *Silvenko v Latvia*,[227] in which a mother and daughter complained of breaches of the rights to respect for their private lives and home, under Article 8 of the ECHR, as a result of their removal from Latvia as part of an agreed withdrawal of former USSR military personnel and their families following the collapse of the USSR. The Latvian government contended that the action taken against the applicants, a daughter and granddaughter of a former USSR military officer based in Latvia, was justified under Article 8(2) ECHR as being necessary to protect Latvian national security. The Grand Chamber held that its task consisted in ascertaining whether the impugned measures struck a fair balance between the relevant interests, namely the individual's rights protected by the ECHR on the one hand and the community's interests on the other. A majority of the Grand Chamber determined that the removal of the applicants did not strike a fair balance because the applicants had been integrated into Latvian society, and their relationship to a former USSR military officer did not constitute a real danger to Latvian security.

In the context of the data privacy/national security paradigm, there is one school of thought, the 'privacy is dead' school, which holds that the struggle to

[226] See Alistair Mowbray, 'A Study of the Principle of Fair Balance in the Jurisprudence of the European Court of Human Rights' 10(2) (2010) *Human Rights Law Review* 289-317; Arai-Takatiashi, *The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECtHR* (Intersentia, Antwerp, 2002) 193.
[227] *Slivenko v Latvia* (2004) 39 EHRR 24.

protect data privacy in a modern surveillance society is a futile exercise. An extreme manifestation of this outlook is the warning issued in 1999, by Scott McNealy, CEO of Microsystems: 'You have zero privacy anyway. Get over it.'[228] The founder of Facebook, Mark Zukerberg, has been reported as claiming that the rise of social networking means that people have no expectation of privacy and that privacy was no longer a social norm.[229] Donald Kerr, Deputy Director of the U.S. Office of National Intelligence remarked that:

> Too often, privacy has been equated with anonymity; and it's an idea that is deeply rooted in American culture.... But in our interconnected and wireless world, anonymity-or the appearance of anonymity-is quickly becoming a thing of the past .... Protecting anonymity isn't a fight that can be won. Anyone that's typed in their name on Google understands that. Instead of privacy, what I would offer, is a system of laws, rules, and customs with an infrastructure of Inspectors General, oversight committees, and privacy boards on which our intelligence community commitment is based and measured.[230]

9.0 Two Data Privacy/National Security Balancing Systems Pre-9/11:The Influence of NSA Surveillance Activity. The Legal and the Actual Balances

The legislative provisions for the data privacy/national security paradigm pre-9/11 are those set out in the Foreign intelligence Surveillance Act (FISA), discussed above. However, the fact that application of these provisions is overseen by a secret court (the FISC) and that this secret court almost invariably accedes to government data surveillance requests, means that we cannot be sure whether or not the balance is being tilted in favour of government surveillance of personal data. Thus, the complicating factor here is the lack of transparency in the application of the law, and the failure to provide for the supervision of the application of this law by a demonstrably independent external authority not subject to government influence. This kind

[228] See Polly Springer, 'Sun on Privacy. 'Get over It' (26 January 1999) *Wired* <http://archive.wired.com/politics/law/news/1999/01/17538.> accessed 24 November 2016.
[229] Bobbie Johnson, 'Privacy no longer a social norm, says Facebook founder' *The Guardian* 11 January, 2010.
[230] Speech of Dr. Donald Kerr, Principal Deputy Director of National Intelligence, Remarks and Questions and Answers at the 2007 Geospatial Intelligence (GEOINT) Symposium held on 23 October 2007. Cited in Jim Harper, 'Reforming Fourth Amendment Privacy Doctrine' 57 (2008) *American University Law Review* 1381, 1392-93, fn 46.

of supervision would seem necessary in respect of a law designed to curb the long-established practice of overboard surveillance of personal data to the detriment of privacy.

In the context of overbroad surveillance, secrecy and lack of transparency, the NSA has a unique role and a unique provenance. As The Church Committee Report indicated, its potential 'to violate the privacy of American citizens is unmatched by any other intelligence agency. The same Report, on the basis of expert evidence given during the Church Committee hearings, revealed that from the early 1960s until 1973, the NSA intercepted 'the international communications of American citizens, without a warrant, at the request of other federal agencies.'[231] The origin of the NSA, the nature of its original mandate, the secrecy surrounding its activities from the beginning and its enormous technological capacities which enable it to collect, retain and redistribute personal data, help to account for the mainly secret influence it exerts on the data privacy/national security balance.

In the period between its creation by Executive Order in 1952 and the establishment of FISA in 1978, there was no statute which either authorised, or specifically restricted, the electronic surveillance activities of the NSA insofar as these involved, or potentially involved, Americans. This was at a time when the NSA had the capacity to monitor almost any electronic communication which was transmitted through the air, and this included telephone calls and telegrams. A distinguishing feature of the NSA is that it owed its establishment to a memorandum from President Truman to the Secretaries of State and Defence in October 24, 1952.[232] The Truman Memorandum was a Presidential

[231] Church Committee Report, Book 2, 201-02.
[232] See Stephanie A. DeVos, 'The Google-NSA Alliance: Developing Cybersecurity at Internet Speed" 21(1) (2010) *Fordham Intellectual Property, Media and Entertainment Law Journal* 173, 196.

Order [233] mandating the establishment of the NSA, as opposed to being mandated by a Congressional Statute, which would serve to oversee its activities. The NSA was created by an Executive Directive and its role and functions have evolved and been maintained by Executive Directives, which have been 'vague in their delegation of authority and in their definition of the type of information permissible for the agency to collect.'[234]

James Bamford, a specialist on the NSA, describes it as 'America's newest and most secret agency, so secret in fact that only a handful in the government would be permitted to know of its existence.'[235] To ensure the secrecy of the NSA, the authorities saw to it that its establishment did not receive any new coverage, was not subject to debate in Congress or a press announcement. The fact that the NSA was created by Presidential Order rather than by State law helped to shield it from public scrutiny. This practice developed as a consequence of the rapid expansion of NSA surveillance initiatives during the Cold War, and again in the aftermath of the terrorist attacks of September 11, 2001, which Bamford attributes 'to limited outside oversight' with a view 'to be able to target thousands **of** people simultaneously, some briefly and some long term, without the hassle of justifying them to anyone higher than an anonymous shift supervisor.'[236] The extent of the surveillance latitude enjoyed by the NSA is indicated in the Church Report which reveals that the agency maintained that 'no existing statutes control, limit or define the signals intelligence activities of the NSA.'[237]

---

[233] 'Executive orders and proclamations are directives or actions by the President. When they are founded on the authority of the President derived from the Constitution or statute, they may have the force and effect of law.... In the narrower sense Executive orders and proclamations are written documents denominated as such.... Executive orders are generally directed to, and govern actions by, Government officials and agencies. They usually affect private individuals only indirectly. Proclamations in most instances affect primarily the activities of private individuals. Since the President has no power or authority over individual citizens and their rights except where he is granted such power and authority by a provision in the Constitution or by statute, the President's proclamations are not legally binding and are at best hortatory unless based on such grants of authority.' Staff of House Committee on Government Operations, 85th Congress., 1st Session, Executive Orders and Proclamations: A Study of a Use of Presidential Powers (Government Printing Office, 1957).

[234] Robert Bloom and William J. Dunn, 'The Constitutional Infirmity of Warrantless NSA Surveillance: The Abuse Of Presidential Power And The Injury To The Fourth Amendment 15 (2006) *William and Mary Bill of Rights Journal* 147, 153.

[235] See Robert N Davis, 'Striking the Balance: National Security vs. Civil Liberties' 29(1) (2004) *Brooklyn Journal of International Law* 175, 182.

[236] James Bamford, *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America* (Anchor Books, 2009) 111.

[237] Church Committee Report, Book 3,736; Deposition of Roy Banner, NSA General Counsel.

The NSA's General Counsel further claimed that the Fourth Amendment to the U.S. Constitution did not apply to the agency when it intercepted international Communications by U.S. citizens.[238] If, by Presidential fiat, the NSA had the freedom to disregard the provisions of the Fourth Amendment when intercepting the communications of U.S. citizens, its activities were rendering its telecommunications surveillance activities largely free from constitutional restrictions, since, in U.S. law, the Fourth Amendment 'is the critical Constitutional provision regarding telecommunications surveillance.' [239] This meant that the NSA was free to violate the privacy rights of U.S. citizens at a fundamental level by denying them their Constitutional rights, and at the same time influencing the data privacy/national security balance in a direction favourable to the latter. In such circumstances, it is not surprising that the Church Committee, in its Report recommended that the NSA should have no greater latitude to monitor the communications of Americans than should any other intelligence agency: To the extent that other agencies are required to obtain a warrant before monitoring the communications of Americans, NSA should be required to obtain a warrant.'[240] The degree of latitude the NSA thought it enjoyed is indicated in the testimony of NSA Deputy Director Benson Buffham as he was being questioned by Senator Walter Mondale in a hearing before the Senate Select Committee investigating the operations of the Intelligence agencies. Mondale's questioning centred on a controversial NSA programme:

> Mondale: “Were you concerned about its legality?”
>
> Buffham: “Legality?”
>
> Mondale: “Whether it was legal.”
>
> Buffham: “In what sense? Whether that would have been a legal thing to do?”
>
> Mondale: “Yes.”
>
> Buffham: “That particular aspect didn't enter into the discussion.[241]

---

[238] ibid.

[239] Paul Schwartz, 'German and U.S. Telecommunications Privacy Law: Legal Regulations of Domestic Law Enforcement Surveillance' 54 (2002) *Hastings Law Journal* 751, 764.

[240] Church Committee Report, Book 2, 309.

[241] *The National Security Agency and Fourth Amendment Rights: Hearing before the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, 94th Cong. 45 (1976). Cited in Margo Schlanger, 'Intelligence Legalism and the National Security Agency's Civil Liberties Gap' 6(1) (2015) *Harvard National Security Journal* 112, 122, fn 28.

10.0 Conclusion

On the basis of the evidence presented in this chapter, in particular the evidence assembled by the expert group which compiled the Church Committee Report, it is clear that at least during the period between 1945 and the passage of the Foreign Intelligence Surveillance Act in 1978, data privacy consistently lost out to national security. The evidence gathered by the Church Committee suggests that the intelligence agencies under Executive Control were enabled to intercept and retain the data of millions of Americans for a number of reasons, among these the sustained failure of the legislature to control the activities of the intelligence community and to ensure its accountability. Another reason was that the intelligence agencies felt able, over a long period, to assume that the secrecy of their operations was absolute and permanent. Feeling able to act in secret and sustained by the authority of the Executive branch, unaccountable to either the judicial or legislative branches of government, and not liable to have their activities tested by public opinion, it is not surprising that various Administrations and their intelligence agencies, NSA CIA and FBI were involved in secret, overbroad domestic surveillance programmes involving the collection of items of citizen-to-citizen communications, postal and telephonic, involving the co-operation of telephone companies and postal services. The interference with data privacy was furthered by the tendency of senior executive intelligence officials to give implicit directions to operatives to intensify their surveillance activities.

This situation raises profound questions about the relationship between the Executive, legislative and judicial branches of government. The nature of this relationship was such that the Executive, largely unfettered by either the legislative or judicial branches, was able to use the authority it enjoyed to employ the intelligence agencies, particularly the NSA, to engage in degrees of surveillance so broad as to violate the data privacy rights of millions of U.S. citizens at a fundamental level over a long period. For its part, the NSA had, from its foundation, been exempted by Presidential Order from public scrutiny and had also enjoyed the assurance that its surveillance activities, however broad, were not controlled, limited or defined by statute law. It thus enjoyed the kind of latitude to monitor the communications of Americans without the

requirement of obtaining a judicial warrant, a latitude not enjoyed by the other intelligence agencies, the CIA and the FBI.

During this period, Presidents, to varying degrees, tended to rely on long-standing tradition and precedent that when confronting emergencies facing that State, their powers were unlimited, even extending to violating the law. Most Presidents during the pre-9/11 period could argue that the USA was involved in an ongoing state of national emergency. In such an emergency, Presidents could plausibly argue that whatever they did was lawful, and when the security of the state was imperilled, measures taken to defend this, even when these involve long-standing rights such as privacy, take precedence. The downside of this was that the President could, and in some cases did, authorise intelligence agencies to stretch their surveillance activities to individuals who posed no demonstrable threat to national security, but who were perceived by the President as posing a threat to the political interests of the Party to which he belonged.

When Congress enacted FISA as a response to the revelations that warrantless surveillance in the name of security had been seriously abused, the FISA response was intended to strike a fair and just balance between the protection of national security and the protection of personal liberties (in this case data privacy). This would suggest that FISA should have had the effect of adjusting the data privacy/national security balance in favour of data privacy to some degree. That it has had this effect cannot be asserted with confidence, mainly because of the rules governing the FISA Court (the FISC) whose *raison d'être* is to adjudicate on government applications for surveillance warrants. One major problem about the FISA Act is that the FISC, as well as being a secret Court and thus lacking transparency, also has another feature which distinguishes it from other U.S. Courts: it works through a non-adversarial process in which surveillance warrants are issued on the basis of information provided exclusively by the Executive branch of Government, the party which is seeking the warrants. Opposition parties, cross examination of government witnesses, and opposing arguments, standard features of the U.S. system, are absent from its deliberations. It is difficult to imagine that the FISC and the Court of Review (FISCR) could exercise objective oversight of the balance

between data privacy and national security in secret, non-adversarial proceedings, strongly influenced by government entities, and lacking the balancing influence that would have been provided by the participation in the proceedings of an independent advocate who could analyse and if appropriate, challenge, for example, the government's justification for bulk surveillance, on a FISC judge's initial analysis. Because the bulk collection programmes have the capacity to compromise the data privacy of countless numbers of U.S. citizens, they thus had the capacity to tilt the data privacy/national security balance in favour of national security. This would frustrate the original purpose of the FISA legislation, which was enacted by Congress to restrict the ability of the government to engage in the overbroad collection of citizens' data.

10.1 Contrasting U.S. and European approaches to Data privacy Pre-9/11

Two features of the U.S. system of governance and U.S. understandings of the relative claims of data privacy and state security help to account for some significant differences between U.S. and European approaches to the protection of data privacy pre-9/11. The system of governance features a Presidency wedded to a long-entrenched theory of prerogative power which holds that when the President deems that the security of the State is under threat, he can take whatever measures he considers appropriate to counter this threat even if this means acting contrary to laws, for example, those protecting the privacy rights of U.S. citizens. Examples of this have been identified throughout this chapter, the most egregious being the deployment by U.S. Presidents of the National Security Agency to conduct secret overbroad surveillance programmes which violated the data privacy rights of millions of Americans.

That this was allowed to happen in violation of the Fourth Amendment, the critical Constitutional provision relating to telecommunications surveillance by the State, represents another difference between U.S. and European approaches to data privacy protection, and illustrates the inadequacy of the Fourth Amendment as a defence of data privacy rights and as a barrier to secret mass surveillance of American citizens. While the U.S. emphasis was on security protection, the emphasis in Europe pre-9/11 was on privacy protection. It is significant that Sweden was the first country to pass a national data protection law in 1973, followed by Denmark in 1979, Norway in 1980 and Finland in

1980.[242] There is a broad consensus in Germany that data protection is important in and of itself. In 1970, the German State of Hessen adopted by the World's first data protection Act,[243] and in 1976, the German Federal Data Protection Act was passed.[244] The widespread abuse of private data in the Third Reich from 1933 to 1948, provides an explanation for the revulsion Germans feel towards State surveillance, and the belief that privacy merits the special protection afforded to it. The controversial surveillance and data collection practices of the U.S. National Security Agency illustrate the wide gulf between U.S. and European approaches to data privacy.

The relative robustness of the European defence of data privacy is manifested in the Council of Europe's ECHR (1950), designed to guarantee data privacy rights in a practical and effective manner; in the jurisprudence of the ECHR Court, (the ECtHR) which has been developing exponentially since the 1980s; the Council of Europe Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (1981) and the European Data Protection Directive (95/46/EC). U.S. provisions, whether Constitutional or statutory, for the protection of data privacy in the pre-9/11 period were exiguous when compared to those from Europe listed above. The absence of an overarching comprehensive U.S. privacy law led an EU Working Party to conclude that the U.S. did not provide adequate privacy protection as this was defined in Directive 95/46/EC.

[242] Herbet Burkert, 'Privacy-Data Protection: A German/European Perspective' in Governance of Global Networks in Christoph Engel and Kenneth H. Keller (eds) *Governance of Global Networks in the Light off Differing Local Values* (Baden-Baden, 2000), 43-70, 48.
[243] ibid, 44.
[244] ibid, 48.

Chapter Three

The Privacy/Security Balance in the U.S. Post-9/11

1.0 Introduction

This Chapter deals with the evolution of the data privacy/national security balance in the United States during the period from September 11 to the present. Discussion of this topic throughout this section is based on the premise that there is a need for balance between individual rights (such as data privacy) and public safety (in the context of this section, national security). One problem in this regard is to determine what the data privacy/national security balance is at a particular point in time. This problem arises when we are faced, for example, with such questions as the following: Did the Executive and legislative responses to the 9/11 attacks reconstitute the existing Constitutional balance? To what extent was the Constitutional balance redefined by this response? What is the Constitutional understanding of what the data privacy/national security balance entails? What is the legislative understanding of what the balance entails? In the wake of the terrorist attacks, was some adjustment of the data privacy/national security balance necessary, or inevitable? Is there a precise point of balance that one can identify at what point the government tilts too far in one direction or another?

An important consideration is whether the new technological surveillance measures adopted post-9/11 enhance national security to the extent needed, to any extent, or intrude excessively into the data privacy rights of U.S. citizens. Another issue considered is, when the government is accorded new powers by the legislature, how closely the government is held accountable regarding the ways in which it uses these powers, and whether mechanisms are in place to ensure that these powers are used appropriately. This leads to a central theme of the section: the position adopted by the Bush Administration that in times when the security of the State is in jeopardy, the President has the exclusive power to determine what the law is when national security concerns are being addressed, and that Congress cannot interfere with security measures adopted by the President in furtherance of his policy of pre-empting further acts of terrorism.

A further issue dealt with is the extent to which and under what conditions, the government should be allowed to use the sophisticated surveillance technologies available to its agencies, which make it possible for the FBI and the NSA, on foot of secret orders from the President, to gain access to the data of millions of American citizens. With regard to accountability mechanisms governing the surveillance measures undertaken post-9/11 by the Bush Administration, the Foreign Intelligence Surveillance Act (FISA) addressed procedures applicable to electronic searches by Government, while the Foreign Intelligence Surveillance Court (FISC) which met in secret, has the duty of authorising NSA surveillance measures.

However, these mechanisms have had little effect in restraining the mass surveillance, privacy-invasive activities of the NSA and the FBI for two reasons. One is that the Department of Justice modified the FISA provisions to facilitate more ready access by the Intelligence agencies to a wider range of personal data. Another reason is that the FISC, which can grant or withhold warrants permitting the FBI or the NSA to intercept data, has a long record of routinely issuing such warrants with the utmost liberality. Between 1979 and 2002, of the 10,000 intercept warrants requested by the intelligence agencies, FISA denied only one request for surveillance.

This section also considers the growing body of evidence that despite the massive sophisticated data surveillance programmes undertaken by the NSA and the FBI from 9/11 to the present, involving unprecedented interference with the privacy rights of U.S. citizens, this interference has had little, if any, demonstrable effect on preventing terrorist attacks. The implications of this for the post-9/11 data surveillance enterprise and for the continuous efforts of two successive Administrations to justify it, raise questions of accountability, oversight, trust and governance, which will be considered in this section.

2.0 Background

The attacks on the Twin Towers and the Pentagon on September 11, 2001, viewed by the U.S. Administration as a declaration of war on the United States, marked a decisive alteration of the balance between data privacy and data surveillance in the interest of national security and the prevention of terrorism. Already, in the aftermath of the World Trade Centre bombing on 27 February

1993,[1] initiatives commenced to institute a scheme of data retention, including the retention of telecommunications data. The result was the passage of the Communications Assistance for Law Enforcement Act 1994 (CALEA),[2] which had been backed by the FBI. This measure was relatively narrow in scope, limited to common carriers, as opposed to all electronic communication service providers, and it did not impose an obligation on telephone companies to make possible the decryption of encrypted conversations, regardless of whether they had an encryption key.[3]

Three days after the 9/11 attacks on New York and Washington D.C., in which up to 4,000 people lost their lives, President Bush declared a State of National Emergency. On the same day, the Joint Houses of Congress gave the President sweeping discretionary authority to act in response to these attacks. With just one dissenting vote in the House of Representatives and none in the Senate, Congress passed a resolution incorporating an Authorisation for the Use of Military Force (AMUF). This Resolution authorised President Bush to use

> [A]ll necessary and appropriate force against those nations, organisations or persons he determined [had] planned, authorised, committed, or aided the terrorist attacks that occurred on 11 September, 2001, or harboured such organisation or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organisations or persons.[4]

It might seem odd that this Resolution authorised the use of force before either President Bush or Congress knew with certainty which 'nations, organisations or persons' were involved in the 9/11 attacks. Thus, war was declared, but

[1] Lindsey Gruson, 'Explosion Displaces Hundreds of Businesses' (*New York Times*. 28 February 1993).
[2] Pub. L. No. 103-414, 108 Stat. 4279, codified at 47 USC 1001-1010.
[3] Susan Landau, *'CALEA and Network Security: Security, Wiretapping and the Internet* ' 3 (6) (2005) 26 *IEEE, Security and Privacy* <http://privacyink.org/pdf/SWatI.pdf> accessed 20 February 2015.
[4] Authorization for Use of Military Force, PL 107-40, Sec 2, (a) The language of this resolution specifically invoked that of the War Powers Resolution of 1973, (WPR) in which Congress authorised President Clinton to involve the U.S. in the NATO air war against Serbia on behalf of ethnic Albanians in Kosovo. See Andrew Rudalevige, *The New Imperial Presidency. Renewing Presidential Power After Watergate.* (The University of Michigan Press, 2005) 215; John Yoo. 'The Terrorist Surveillance Programme and the Constitution,' George Mason Law Review14(3) (2007) 565-604.

without a specified enemy, and the choice of enemy was left to the President. As Lindsay puts it, 'Congress effectively declared war and left it up to President Bush to decide who the enemy was.'[5]

The Congress Resolution also declared that 'the President had authority under the U.S. Constitution to deter and prevent acts of international terrorism against the United States.' [6] It later became clear that the pre-emptive action to deter and prevent acts of terrorism involved the mass collection of domestic phone calls and other telephony data of U.S. citizens by the National Security Agency on the secret orders of the President. In this respect, the early response of the Bush administration to 9/11 had a decisive effect on the privacy/security balance in the U.S. and a profoundly negative effect on the privacy rights of U.S. citizens. As part of the pre-emption policy, Bush directed the NSA to initiate a wide-scale Terrorist Surveillance Programme (T.S.P). The T.S.P was secretly authorised by the President, and did not come to light until 2005 when *The New York Times* revealed that the NSA had, on the instruction of the President, engaged in warrantless wiretapping of American citizens' telephone calls.[7] *The New York Times* revelation was based on leaks of classified information, presumably by NSA officials concerned about the legality of the programme. *The New York Times* reported that at the President's request it had delayed publication of the story for more than a year.[8] As part of the TSP, the NSA listened in on international telephone calls whenever NSA officials believed that the calls were made to people associated with terrorist organisations. These calls included some involving U.S. citizens. The NSA wiretapped without seeking warrants on Court Orders, thus disregarding the Regulation and oversight required by the law.

The Terrorist Surveillance Programme featured a range of measures designed to expand the government's surveillance capabilities. One of these was the Total Information Awareness Programme (YIA) proposed in 2002 by the

[5] James M. Lindsay, 'Deference and Defiance: The Shifting Rhythms of Executive Legislative Relations in Foreign Policy' 33(3) (2003) *Presidential Studies Quarterly* 530-546, 538.
[6] ibid.
[7] James Risen and Eric Lichtblau, 'Bush Lets U.S. Spy on Callers Without Courts: Secret Order to Widen Domestic Monitoring,' *New York Times*, 16 December, 2005.
[8] See David Cole and Martin Lederman, 'The National Security Agency's Domestic Spying Program: Framing the Debate' (2006) 81 (4) *Indiana Law Journal* 1355.

Defence Advanced Research Projects Agency under Admiral Poindexter.[9] The Total Awareness Programme involved the use of supercomputers to data mine both government and commercial data to 'discern potential terrorist activity.'[10] Media reports on this programme led to a public outcry and uniformly hostile media campaign, typified by the comment of a conservative columnist, who condemned the TIA as designed 'to create computer dossiers on 360 million Americans.'[11] This was one case in which Congress intervened to protect the privacy rights of U.S. citizens: The Senate voted unanimously to deny funding to the TSA.[12]

Another surveillance technology, used by federal law enforcement agencies since the 1990s without being scrutinised by Congress, has expanded the Government's surveillance capabilities significantly, without regulation. This technology, called Stingray, enables the Government, directly and in real-time, to intercept communications data and detailed location information of cellular phones. The Stingray has the capacity for invasive surveillance, involving the sending of signals through walls and into homes.[13]

An apologist for the Bush Administration and the components of its Terrorist Surveillance, John Yoo, deplored the abandonment of the Total Awareness Programme as 'another example of libertarian overreaction,' and accused critics of such programmes as being 'mostly interested in blindly limiting the power of the Government even as it fights a tough war.' [14] Yoo concluded that the worst thing Americans could do, 'when confronted by a shadowy, capable enemy like

[9] See Jonathan Levin, 'Total Preparedness,' *National Law Review* (13 February, 2005). <http://www.national review.com/comment/comment-levin02l303.asp.> accessed 20 December 2016. John Yoo, 'The Terrorist Surveillance Program and The Constitution' 14(3) (2007) *George Mason Law Review* 565, 588-590.
[10] Heather MacDonald, 'What We Don't Know Can Hurt Us' (2004) *City Journal* 14 and 18.
[11] William Safire, 'You are a suspect,' *New York Times* 14 November, 2002).
[12] 'Pentagon's Terror Information Awareness will end,' (September 25 2003) USA To Day.com <http://usatoday30.usatoday.com/news/washington/2003-09-25-pentagon-office_x.htm. accessed 4 January 2017.
[13] Stephanie K. Pell and Christopher Soghoian, 'A Lot More than A Pen Register and Less than a Wiretap: What the StingRay Teaches Us About How Congress Should Approach the reform of Law Enforcement Surveillance Authorities' 16 (2013) *Yale Journal of Law and Technology* 134, 143.
[14] John Yoo, 'The Terrorist Surveillance Program and the Constitution' 14(3) (2007) *George Washington Law Review* 565, 580.

al Qaeda would be to change our government to make it harder to develop innovative policies like the NSA surveillance programme.' [15]

As Solove points out, the NSA warrantless surveillance programme violated the Foreign Intelligence Surveillance Act (FISA), a federal law that required judicial oversight and court orders to authorise such wiretapping.[16] However, the government felt able to defend the T.S.P. by pointing out that it was a component of the President's power to wage war. This point was also articulated by Attorney General Alberto Gonzales, who testified before a Congressional hearing that 'the President's Constitutional powers include the authority to conduct warrantless surveillance aimed at detecting and preventing armed attacks on the United States.'[17] Congress gave retrospective endorsement to the T.S.P. by passing new enabling legislation. What Congress did here was condemned by Solove, who claimed that 'the legislative branch set a frightening precedent - effectively confirming that the President could break the law with little consequence.'[18] The basis of Solove's argument is that whenever the Government engages in wiretapping to gather foreign intelligence, it is regulated by FISA, and FISA allows the government to engage in electronic surveillance if it obtains a Court order from the Foreign Intelligence Surveillance Court (FISC). The Government must demonstrate probable cause that the monitored party is a 'foreign power' or an 'agent of a foreign power.'[19] The law thus requires the government to get a Court order to wiretap, the NSA did not get one: thus the NSA's warrantless surveillance under the T.S.P. was illegal, thus involving the President in a violation of the law by allowing the NSA to ignore FISA,[20] thus raising the question: Can the President violate the law?

[15] ibid.
[16] Daniel J. Solove, *Nothing to Hide. The False Tradeoff between Privacy and Security* (Yale University Press, 2011) 82.
[17] Prepared Statement of Hon. Alberto R. Gonzales, Attorney General of the United States. February 6, 2006 <https://www.justice.gov/archive/ag/speeches/2006/ag_speech_060206.html> accessed 28 October 2016.
[18] Daniel J. Solove, *Nothing to Hide. The False Tradeoff between Privacy and Security* (Yale University Press, 2011) 82.
[19] 50 U.S.C. Section 1801.
[20] Daniel J. Solove, *Nothing to Hide. The False Tradeoff between Privacy and Security* (Yale University Press, 2011) 83.

The Attorney General explained to Congress why the President allowed the NSA to circumvent FISA: If the NSA intelligence officers 'had to navigate through the FISA process for each of these intercepts, that would necessarily introduce a significant factor of delay, and there would be critical holes in our early warning system.'[21] This pragmatic defence of the NSA's warrantless surveillance programme was preceded by a trenchant defence of the President's role in the same programme. This defence was based on the principles enunciated by Congress on 14 September 2001, one of these being that the President, in times of national emergency, possessed plenary authority to respond to this emergency as he saw fit. This would mean that the President could alter the data privacy/national security balance as he deemed appropriate. A Department of Justice White Paper, issued on 19 January, 2006, captures the essence of the defence mounted by the President and his Administration, of his management of the terrorist crisis and his involvement in pre-emptive surveillance strategies. Of the main points made by the Department of Justice, in support of the 'lawfulness' claim, one is the traditional deontological one. The basic claims made in the White Paper are that the NSA activities mandated by the President, 'provide the United States with an early warning system to help avert the next attack,' and that NSA activities are lawful and consistent with civil liberties.'[22] Among the President's most basic constitutional duties is to protect the nation from armed attack. The Constitution gives him all necessary authority 'to fulfil that solemn responsibility.'[23] Another point was that the President's broad powers to wage war trump any statute, including FISA, and 'In exercising his constitutional powers, the President has wide discretion, consistent with the Constitution, over the methods of gathering evidence about the nation's enemies in time of armed conflict,' as well as 'inherent constitutional authority' as commander in chief to engage in the surveillance.'[24] The issues raised in this defence are similar to those raised in Ancient Rome when the security of that State was in peril; the Ciceronian

[21] Prepared Statement of Hon. Alberto R. Gonzales, Attorney General of the United States. February 6, 2006 <https://www.justice.gov/archive/ag/speeches/2006/ag_speech_060206.html> accessed 28 October 2016.
[22] U.S. Department of Justice, White Paper. Legal Authorities Supporting the Activities of the National Security Agency Described By The President. (January 19, 2006) <https://www.justice.gov/sites/default/files/opa/legacy/2006/02/02/whitepaperonnsalegalauthorities.pdf> accessed 23 November 2016.
[23] ibid.
[24] ibid.

maxims come to mind: 'Silent enim leges inter arma' (Laws are silent in time of war) and 'Salus populi suprema est lex' (The good of the people is the chief law).[25]

The position taken by Bush and members of his Administration was that when a terrorist emergency threatens the security of the State and the lives of its citizens and this threat becomes more acute an adjustment of the balance between the privacy of the data of citizens and the demands of national security is necessary, even inevitable. One liberal commentator, in the wake of 9/11, formulated that argument as follows:

> Terrorist incidents in the 1970s (such as at the Munich Olympics) had maximum death tolls of about a dozen; attacks in the 1980s and 1990s raised the scale…..to the hundreds; 9/11 lifted the toll into the thousands; and terrorists are now making weapons of mass destruction that could kill hundreds of thousands. As risks change, we who care about civil liberties need to realign balances between security and freedom. It is a wrenching, odious task, but we liberals need to learn from 9/11, just as much as the FBI does.[26]

However, the powers the President asked from Congress did not simply involve an ability to change the data privacy/national security balance. These powers, as the President and members of his Administration insisted, meant that the powers conferred on him to wage war included his 'inherent constitutional authority' to engage in surveillance as a fundamental adjunct to the 'war on terrorism.' Thus, what was being claimed here was that as long as the war on terrorism continued, there was no limit to the President's power. On foot of this broad claim, the President could, and did, authorise the NSA to engage in large-scale warrantless surveillance of U.S. citizens, disregarding statutory limitations on this activity. Given the intensive nature of the secret surveillance that characterised the President's Surveillance Programme (the PSP), the privacy element of this balance was inevitably restricted, if not occulted.

[25] Cicero, Pro Milone, Chapter II; De Legibus, book 3, Chapter 8.
[26] Nicholas Kristoff, 'Liberal Reality Check' *The New York Times* 31 May 2002.

Since national security was an almost exclusive preoccupation of the Bush Administration during the war on terror the President had, with Congressional approval, determined to wage war on terrorism, personified by al-Qaeda, and since he had decided that a programme of mass data surveillance was an essential weapon in that war, data privacy inevitably lost whatever protection it had enjoyed, and became the victim of enhanced Executive discretion.

As part of the strategy underpinning his surveillance programme, Bush developed instruments for further enhancing the powers extended to him by a compliant Congress. He resorted to the use of bill-signing statements to influence the interpretation of Congressional enactments that did not fully accord with his surveillance scheme. Having signed a Bill into law, he would append a statement to the effect that he reserved the right to 'construe the law in a manner consistent with the Constitutional authority of the President as Commander-in-Chief, and 'the shared objective of the Congress and the President….of protecting the American people from further terrorist attacks.'[27] Further, the secrecy surrounding the component elements of the PSP, there was little if any possibility of subjecting it to public accountability or informed assessment. This became possible only when factual details of the true extent of the surveillance programme became available.

The Bush doctrine of executive privilege, a concept not mentioned in the Constitution, not clearly defined in law and never resolved definitively in the Courts [28] was enunciated on several occasions, as well as implemented, by Bush himself, by his Vice-President Dick Cheney, and his Attorney-General Alberto R. Gonzales. In 2006, the Administration rejected requests from the Senate Judiciary Committee for classified opinions from the Justice Department expressing concern over the legality of the NSA's electronic programme.[29] Appearing before the Committee, Attorney-General Gonzales described the NSA programme as 'an early warning system designed for the 21st Century,' but refused to concede that the programme should be made

[27] George W. Bush, President's Statement on Signing of H.R. 2863, December 30, 2005.
[28] Michael C. Dorf 'A Brief History of Executive Privilege, from George Washington to Dick Cheney.' <http://writ.news.findlaw.com/dorf/20020206.html> accessed 20 March 2015.
[29] Eric Lichtbaum, Senate Panel Rebuffed on Documents on U.S. Spying' (The *New York Times*, February 2, 2006).

subject to 1978 FISA law.[30] Gonzales was, in effect, telling the Congress that the Executive would police itself and be the sole arbiter of the appropriate balance between national security and civil liberties which, in the case of the NSA, meant mainly privacy rights.

There were specific cases in which Bush claimed that he alone could exercise the authority of each of the three branches of government. One of these cases concerned the practice of illegal warrantless wiretapping by the NSA. In that case, Bush acted as lawmaker by determining that he could ignore the regularly enacted law and impose his own rules in order to conduct surveillance in the U.S. He acted as executive in ordering the NSA to carry out his policies, and he acted as judge by arguing that it was his inherent right as President to order warrantless surveillance and avoid obtaining warrants from the FISA Court. Furthermore, by resorting to the use of Bill-Signing Statements, Bush was undermining the doctrine of the separation of powers by claiming the authority to ignore those parts of statutes that he had signed into law of which he did not approve and that he claimed impinged on his own prerogatives. He was thereby refusing to accept the legitimacy of either Congress or the Courts to limit his authority.[31]

The procedures adopted by Bush which enabled him to occult data privacy rights should be measured against those principles upon which the Framers of the U.S. Constitution drew. These principles placed explicit limits on the powers of the Executive, and involved a separation of powers structure designed to prevent the accumulation of power in any one branch of government. This fundamental structure was the very one that Bush, and to a large extent Nixon before him, their critics alleged, had set out to undermine. The thinking of those who framed the Constitution on this essential aspect of the document is forcefully expressed by James Madison, who played a key part in framing the Constitution:

[30] Suzanne Goldenberg, 'US law chief defends domestic wiretapping' (*The Guardian* 7 February, 2006).
[31] James P. Pfiffner, 'The Contemporary Presidency. Constraining Executive Power: George W. Bush and the Constitution' 31(1) (2008) *Presidential Studies Quarterly* 123, 140.

> The accumulation of all powers, legislative, executive and judiciary, in the same hands, whether of one, a few, or many, and whether hereditary, self-appointed, or elective, may justly be pronounced the very definition of tyranny.[32]

As long as the Bush Administration succeeded in keeping the data surveillance activities of the NSA secret, it did not need to worry unduly about persisting with them. It was only when whistleblowers began to reveal the nature and extent of the NSA operation and its consequences for data privacy that the Administration felt the need to respond.

Secrecy was not the only factor that facilitated the Administration's data surveillance operations, in particular those impinging on the privacy of U.S. citizens. Both Congress and the Courts, sometimes actively, and sometimes by default, played significant roles in the evolution of what Balkin calls 'the National Surveillance State.'[33] The role of the Courts, in particular of the Supreme Court, in facilitating expansion of secret Executive data surveillance programmes was essentially a negative one. Whereas in Germany, for example, the Constitutional Court has been active in reviewing statutes affecting telecommunications privacy, the U.S. Supreme Court, as Schwartz points out, 'has developed doctrines that have taken it out of the business of constitutional review of laws regarding the processing, collection and sharing of telecommunications attributes.'[34]

Balkin and Levison define the National Surveillance State as 'a special case of Information State - a State that tries to identify and solve problems of governance through the collection, collation, analysis and production of information and production of information.' [35] They argue that the secret NSA programme and similar initiatives reflect a larger trend in how governments

[32] The Federalist No. 47: 'The particular Structure of the New Government and the Distribution of Power Among its Different Parts'. James Madison, (*New York Packet* January 30, 1788).
[33] Jack M. Balkin, 'The Constitution in the National Surveillance State' 93(1) (2008) *Minnesota Law Review* 1.3.
[34] Paul Schwartz, 'German and U.S. Telecommunications Privacy Law: Legal Regulations of Domestic Law Enforcement Surveillance' 54 (2002) *Hastings Law Journal* 751, 782.
[35] Jack M. Balkin and Sandford Levinson, 'The Process of Constitutional Change: From Partisan Entrenchment to the National Surveillance State' 75(2) (2006) *Fordham Law Review* 489, 490; Jack M. Balkin, 'The Constitution in the National Surveillance State' 93(1) (2008) *Minnesota Law Review* 1 2.

discharge their functions which predates the September 11, 2001 attacks and the Bush administration's declaration of a 'war on terror.' They further argue that

> During the last part of the twentieth century, the United States began developing a new form of governance that features the collection, collation and analysis of data about population both in the United States and around the World. This new form of governance is the national surveillance state.[36]

The Balkin/Levinson thesis derives credibility from the fact that the privacy/security balance and the recent data surveillance operations during the two terms of the Bush presidency have remained substantially intact and even intensified under President Obama.

One of the key roles of Congress as Constitutional jurisprudence has traditionally understood it, is oversight, 'making sure that the laws it writes are faithfully executed, and vetting the military and diplomatic activities of the executive.'[37] The oversight responsibility of Congress also includes reviewing data surveillance methods employed by the Administration and its agencies, a major example of which is the Church Committee Investigation of illegal surveillance practices during the Nixon Presidency. However, as Ornstein and Mann point out, 'since George W. Bush has become President, oversight has all but disappeared. From homeland security to the conduct of the Iraq war, from allegations of torture at Abu Ghraib, to the surveillance of domestic telephone calls by the National Security Agency (NSA), Congress has mostly ignored its responsibilities.'[38] They also point out that in the case of such major issues as the NSA's domestic surveillance programme, Congress has generally failed to ask how policies in this area have been implemented, how faithfully laws have been executed, how well the Executive branch of government has stayed within

[36] Jack M. Balkin, 'The Constitution in the National Surveillance State' in Jack M. Balkin and Reva B. Siegel, (eds), *The Constitution In 2020* (Oxford University Press, 2009) 197-208, 198.
[37] Norman J. Bernstein and Thomas E. Mann, 'When Congress Checks Out' 85(6) (2006) *Foreign Affairs* 67.
[38] ibid, 70.

its Constitutional bounds, and how vigorously malfeasance or misfeasance by public agencies and private contractors has been dealt with.[39]

On the few occasions when Congress oversight came into play, this was in response to public exposure of serious breaches of law, one notable example involving illegal data mining by the NSA as a component of the 'war on terror.' On December 15, 2005, *The New York Times* published an article entitled 'Bush lets U.S. spy on Callers without Courts.' The article focused on the warrantless NSA interception of Americans' international phone calls and e-mail traffic, without disclosing the bulk collection of the metadata that provided the NSA with a social network of everyone inside the US and their ties abroad. The public revelations of even this relatively small part of the total picture of NSA data surveillance provoked a strong response from Congress, with Senators from both parties voting to block the reauthorisation of the 2001 Patriot Act which had expanded the President's power to conduct surveillance, with warrants, in the aftermath of the 9/11 attacks. Bush, however, remained adamant. Acknowledging that he had ordered the NSA to conduct an electronic eavesdropping programme in the United States without first obtaining warrants, he declared that he would continue the highly classified secret programme because it was 'a vital tool in our war against the terrorists.'[40] He also defended his action as 'fully consistent with my Constitutional responsibilities and authorities,' adding that 'in the war on terror we cannot afford to be without this law for a single moment.' [41] 'This law' referred to by Bush was not law but an order issued by Bush to a secret security agency, based on his claim that the state of war, the existence of which he had called into being with the backing of Congress, gave him the power to override the prevailing rule of law, whether Constitutional or Statutory.

Bush and his Administration appeared less concerned with conforming to the provisions of the Constitution or Statute law than with the public disclosure of details of their domestic spying programme which had been 'improperly provided to news organisations,' and with the possibility that 'our enemies have

[39] ibid, 72.
[40] David E. Sanger, 'Bush Says He Ordered Domestic Spying.' (*The New York Times*, December 18, 2005).
[41] ibid.

learned information they should not have.'[42] Bush further complained that 'revealing classified information is illegal, alerts our enemies and endangers our country.'[43] The Justice Department opened an investigation, not into the NSA programme, but into its disclosure.[44] When forced to defend its secret data mining programmes, the Bush Administration had recourse to a sweeping statutory theory. This theory interprets a declaration of war or other congressional authorisation to use force, specifically the 2001 Authorisation of the Use of Military Force (AUMF)[45], as providing legislative approval for the otherwise illegal data surveillance programmes authorised by the Administration.[46]

The contrast between the extreme response of the U.S. Executive and Legislature to terrorist attacks on the U.S. mainland detailed above and the more measured and relatively moderate EU response to terrorist attacks in a number of EU countries illustrates the differences between U.S. and EU attitudes to the data privacy/national security balance. In the aftermath of widespread terrorist attacks in Europe, the first response was that information derived from telecommunications traffic data was a necessary component in the fight against terrorism and that data should be shared between law enforcement agencies in EU Member States. Following the terrorist bombings in London in July 2005, a Data Retention Directive (29006/24/EC) was subsequently adopted. This imposed an obligation on Internet and telephone companies to store and retain the metadata relating to the source, address, date and the duration of communications, although the content of these communications was not to be retained or stored.[47]

This Directive was the most robust response of the EU authorities to terrorist attacks on Member States. Moderate as it was compared to the U.S. response to a similar situation, it is significant that the EU Data Retention Directive gave

[42] Transcript. 'President Bush's Address.' (*The New York Times*, December 17, 2005).
[43] ibid.
[44] Eric Lichtblau, 'Bush Defends Spy Program and Denies Misleading Public' (*New York Times*, January 2, 2006).
[45] Pub. L. 107-40, codified at 115 Stat. 224.
[46] Jules Lobel, 'The Commander-in-Chief and the Courts' *Presidential Studies Quarterly* 37(1) (2007) 49 50. See also Joel D. Aberbach, 'What's Happened to the Watchful Eye?' 29(1) (2002) *Congress and the Presidency* 1, 3-24.
[47] For details of the provisions of the Data Retention Directive, see Chapter One, Section Two, at 4.0.

rise to major concerns among EU States regarding its compatibility with fundamental rights provisions (in particular data privacy rights) protected under both EU and Council of Europe primary law. These concerns eventually gave rise to a challenge to the Data Retention Directive before the Court of Justice of the European Union, which struck down the Directive, holding that although it pursued a legitimate objective, the fight against international terrorism, it interfered with the right to privacy in a disproportionate way. It is a token of the difference between EU and U.S. priorities when data privacy rights and national security need are in the balance, that the U.S. Supreme Court was not called upon to decide on whether the secret and warrantless surveillance, privacy-invasive activities of the NSA and the FBI, authorised by the Executive, represented a disproportionate interference with the right to privacy.

This kind of interference, and its extent, was possible in the U.S., but not in the EU, because U.S. lawmakers took the view that intelligence agencies should be exempt from legislative or judicial oversight. Also, the position taken by the Bush Administration between 2001 and 2008, underpinned by the doctrine of Executive privilege, was that when national security is in jeopardy from terrorism, the President has the exclusive power to determine what the law is when national security concerns are being expressed and that the law is what the President says it is. An aspect of the same position is that the legislature cannot interfere with security measures adopted by the President in furtherance of his policy of pre-empting terrorist attacks, even if the measures involve secret programmes of mass data surveillance of U.S. citizens, which, being secret, are not susceptible to public accountability or judicial assessment. When some details of the extent of an NSA electronic surveillance programme became public in 2006, the administration turned down requests from the Senate Judiciary Committee for classified opinions from the Justice Department on the legality of this programme. The system of governance in the EU on the other hand, did not allow for unbridled authority, such as that exercised by the U.S. Presidency, to restrict the data privacy rights of European citizens.

3.0 The Administration's Defence of Its Surveillance Policies and a Scholarly Response

President Bush's defence of the surveillance activities of the NSA was supplemented by the Department of Justice in a document which cited legal precedents for his authorisation of warrantless surveillance by the NSA post-9/11.[48] This document, reiterating the President's claim that he had inherent authority to conduct warrantless searches to obtain foreign intelligence information, observed that while the Supreme Court held that while warrants are generally required in the context of purely *domestic* threats, it expressly distinguished *foreign* threats.[49] The letter also adduced Justice Byron White's recognition in a 1967 case that 'Presidents have long exercised the authority to conduct warrantless surveillance for national security purposes, and a warrant is unnecessary'[50] In his *Katz* judgment, Byron White (concurring) declared that a warrant was unnecessary in a national security context 'if the President of the United States, or his chief legal officer, the Attorney General, has considered the requirements of national security and authorised electronic surveillance as reasonable.'[51] A further point made in the Department of Justice Document was that since the President had determined that it was necessary following September 11 to create an early warning system, 'FISA could not have provided the speed and agility required for the early warning system.' This argument is not convincing: whenever the government engages in wiretapping to gather foreign intelligence it is regulated by FISA, which allows the government to engage in such surveillance provided that it obtains a court order from the Foreign Intelligence Surveillance Court, which meets in secret. The law requires the government to obtain a Court order to engage in wiretapping and the President allowed the NSA to ignore this legal requirement, therefore violating statutory law.

Solove calls this the 'war-powers argument,' which reasons that 'because we're at war with foreign terrorist organisations, the President's war powers allow

[48] William E. Moschella, Assistant Attorney General, Letter from Department of Justice to the Leadership of the Senate Select Committee on Intelligence, and House Parliament Select Committee on Intelligence, December 22, 2005. Reproduced in David Cole and Martin S. Lederman, 'The National Security Agency's Domestic Spying Program: Framing the Debate' 81 (2006) *Indiana Law Journal* 1355-1425,1364.
[49] Citing *United States v United States District Court*, 407 U.S. 297, 308 (1972).
[50] Citing *Katz v United States*, 389 U.S. 347, 363-64 (1967).
[51] ibid, 389 U.S. 347, 364 (1967).

him to bypass the law'.[52] Solove also comments on the Terrorist Surveillance Programme, of which the NSA surveillance programme constitutes a major part that 'the worst part of the TSP wasn't its invasion of privacy but what it revealed about the infirmity of the rule of law.'[53] If Solove's argument is valid, the extreme adjustment of the data privacy/national security balance in favour of the latter may be regarded as a consequence of the infirmity of the rule of law in the post-9/11 period.

A group consisting of constitutional law and former government officials responded to the attempt by the Department of Justice to mount a plausible legal defence of the NSA domestic spying programme, arguing that 'in such a democracy [as the U.S.], the President cannot simply violate criminal laws [FISA being an example] behind closed doors because he deems them obsolete or impracticable.'[54] Reflecting the need to maintain an appropriate balance between such civil liberties as the right to data privacy on the one hand, and national security on the other, the authors of this document maintained, as the House of Representatives had when dealing with FISA legislation in 1977, that the decision as to the standards governing electronic surveillance should be a potential decision involving 'the weighing of important public policy concerns-civil liberties and national security.'[55]

They further maintained that such a political decision 'is one properly made by the political branches of Government together, not adopted by one branch [the President] on its own with no regard for the other.'[56] The letter from scholars and former government officials points out that the FISA statute 'specifically allows for warrantless wartime domestic electronic surveillance - but only for the first fifteen days of a war, and criminalises any electronic surveillance prohibited by statute. It also points out that the NSA surveillance programme

[52] Daniel J. Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security* (Yale University Press, 2011) 82-3.
[53] ibid.
[54] Letter from Scholars and Former Government Officials to Congressional Leadership in Response to Justice Department Letter of December 22, 2005, January 9, 2006. Reproduced in David Cole and Martin S. Lederman, 'The National Security Agency's Domestic Spying Program: Framing the Debate' *Indiana Law Journal* 81(4) (2006) 1355-1425, 1364-1373.
[55] ibid, 1371, fn 13.
[56] Foreign Intelligence Surveillance Act of 1978: Hearings before the Subcomm on Intelligence and the Rights of Americans of the Senate Select Comm on Intelligence, 95th Congress, 2nd Session 12 (1977).

was not authorised by any of the FISA provisions.[57] The central point made in the letter is that Congress did not implicitly authorise the NSA Domestic Spying Programme when it enacted the Authorisation for Use of Military Force (AUMF) against al Qaeda, that Congress expressly prohibited this spying programme in FISA, and that 'the President acted unilaterally and secretly in contravention of FISA's terms.' The letter also adduces Justice Jackson's celebrated dictum in *Youngstown Sheet and Tube Co. v Sawyer*[58] that when the President acts in defiance of 'the expressed or implied will of Congress,' his power is 'at its lowest ebb.'[59] In this setting, Justice Jackson wrote, 'Presidential power [is] most vulnerable to attack and in the least favourable of possible constitutional postures.'[60] There is the further point that Article II of the Constitution imposes on the President the general obligation to enforce laws that Congress has validly enacted: 'He [the President] shall take care that the laws be faithfully executed.'[61] the laws that Congress has validly enacted include FISA, and the use of the mandatory 'shall' in Article II of the Constitution indicates that under the U.S. system of separated powers, 'the President is duty-bound to execute faithfully the provisions of FISA, not to defy them,' as he has in ordering the NSA warrantless domestic spying programme.[62]

In this connection, it should be pointed out that President Bush, instead of ignoring the provisions of FISA in secretly ordering the NSA to engage in an open-ended warrantless domestic surveillance programme, and thereby acting outside the law, could have asked Congress to amend a key provision of FISA. This provision, entitled 'Authorisation during time of war,' dictates that

> Notwithstanding any other law, the President, through the Attorney General, may authorise electronic surveillance without a Court order

[57] Letter from Scholars and Former Government Officials to Congressional Leadership in Response to Justice Department Letter of December 22, 2005, January 9, 2006. Reproduced in David Cole and Martin S. Lederman, 'The National Security Agency's Domestic Spying Program: Framing the Debate' 81(4) (2006) *Indiana Law Journal* 1355-1425,1364.
[58] 343 U.S. at 640.
[59] ibid, at 637.
[60] ibid, at 640.
[61] United States Constitution, Article II, Section 3.
[62] Letter from Scholars and Former Government Officials to Congressional Leadership in Response to Justice Department Letter of December 22, 2005, January 9, 2006. Reproduced in David Cole and Martin S. Lederman, 'The National Security Agency's Domestic Spying Program: Framing the Debate' 81(4) (2006) *Indiana Law Journal* 1355-1425,1369, fn 8.

> under this subchapter to acquire foreign intelligence information for a period not to exceed fifteen calendar days following a declaration of war by the Congress.[63]

However, Congress, in framing the 'Authorization in time of war,' had in mind that if the President required further, more extensive warrantless surveillance during wartime, the fifteen days would be sufficient for Congress to consider and enact further authorization.[64] Had the President followed the course outlined by Congress, and received the authorisation he needed under amended FISA rules, his warrantless domestic programme would have enjoyed legal protection. Attorney-General Gonzales admitted that the Administration did not seek to amend FISA to authorise the NSA spying programme because various members of Congress advised the Administration that it would be 'difficult, if not impossible,' to do so.[65] This excuse for not asking Congress to amend FISA so as to authorise the NSA spying programme is not plausible. Cole points out that the Administration 'cannot argue on the one hand that Congress authorised the NSA programme in the AMFU and, at the same time, that it did not ask Congress for such authorisation because it could be difficult, if not impossible, to get it.'[66] In any case, the Administration, as Cole, observes, had, in the form of the U.S.A. Patriot Act of 2001, a convenient vehicle for seeking whatever amendment in FISA it needed to bring its domestic spying programme under legal protection.[67]

What such considerations suggest, in the context of the data privacy/national security balance, is that the massive security-based adjustment of the pre-9/11 balance, as a result of the Executive response to the 9/11 terrorist attacks,

---

[63] Foreign Intelligence Surveillance Act § 1811. Authorization during time of war. Pub. L. 95–511, title I, § 111, Oct. 25, 1978, 92 Stat. 1796.

[64] 'The Conferees intend that this [15 day] period will allow time for consideration of any amendment to this Act [FISA] that may be appropriate during a wartime emergency… The Conferees expect that such amendment would be reported with recommendations within 7 days and that each House would vote on the Amendment within 7 days thereafter.' House of Representatives Report No. 95-1720, at 34 (1978).

[65] Press Briefing from Alberto Gonzales, U.S. Att'y Gen., and General Michael Hayden, Principal Deputy Director for National Intelligence (Dec. 19, 2005) <http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html> accessed 23 November 2016.

[66] David Cole, 'Reviving the Nixon Doctrine: NSA Spying, the Commander-In-Chief, and Executive Power in the War on Terror' 13 (2006) *Washington and Lee Journal of Civil Rights and Social Justice* 1, 9.

[67] ibid, 9, fn 36.

violated both statutory and Constitutional law. On the question whether, in the wake of 9/11, the adjustment of the data privacy/national security balance as a consequence of the President's anti-terrorism programme was necessary, or expedient, the comments of the privacy advocate, Schneier, are pertinent.

Schneier observes that:

> Some countermeasures provide the feeling of security *instead* of the reality. These are nothing more than security theatre. They're palliative at best…. Massive surveillance systems that deprive people of liberty and invade their privacy are never worth it… Since 9/11 the security we're getting against terrorism is largely ineffective… But it comes at enormous expense, both monetarily and in loss of privacy.[68]

Evidence outlined in a later section of this chapter tends to support Schneier's view that the security Americans have been receiving against terrorism since 9/11 has been largely ineffective.[69]

During the period before 1975-6, United States lawmakers tended to take the view that intelligence agencies should enjoy exemption from legislative oversight, given the scope to work in secrecy and engage in activities that would be deemed inappropriate for other government agencies.[70] In 1975, however, the policy of intelligence exceptionalism was reviewed in a fundamental way by Congress following the publication of a series of articles in *The New York Times* in 1974 alleging that the CIA had abused its power by spying inside the United States.[71] In 1975-76, when government investigators examined the charges of domestic spying, they uncovered a multiplicity of intelligence transgressions, many of them violations of privacy, including illegal mail opening, wiretaps, international cable interceptions and intelligence

[68] Bruce Schneier, *Beyond Fear. Thinking Sensibly About Security in an Uncertain World* (Copernicus Books, New York, 2003) 38 and 249.
[69] See Section 13.0 *The Consequentionalist Defence of the Terrorist Surveillance Programme* (TSP).
[70] See generally, Stephen F. Knott, *Secret and Sanctioned: Covert Operations and the American Presidency* (Oxford University Press, 1996).
[71] See Seymour M. Hersh, 'Underground for the C.I.A. in New York: An Ex-Agent Tells of Spying on Students' (*New York Times* December 29, 1974).

files on over a million U.S. citizens.[72] In 1976, Senators created a permanent Senate Select Committee on Intelligence (SSCI) and a year later, the House of Representatives established a House Permanent Select Committee on Intelligence (HPSCI). In 1978, Congress brought the judicial branch more directly into the sphere of intelligence oversight by establishing a secret FISA Court to review national security wiretap requests from the government. In 1980, Congress passed the Intelligence Oversight Act,[73] a statute that further tightened legislative supervision over the secret agencies.[74]

Writing in 2008, at the end of the Bush Presidency, Johnson remarked that in the years since 1975, members of Congress had displayed various levels of commitment to the job of intelligence supervision. Johnson distinguishes four kinds of response displayed by those members to the calls for greater intelligence accountability.[75] The first category of members, the 'ostriches' were happy to 'ignore these calls, and acquiesce in the decisions of the executive branch within the domains of intelligence and defence. The second category, the 'cheerleaders,' had chosen to become unabashed boosters for intelligence, and saw their job as one of explaining the value of intelligence to the American people and supporting the funding of surveillance programmes. The third group, the 'skeptics,' tended to see secret agencies as inherently immoral due to the opening and reading of other people's mail, eavesdropping on telephone and e-mail traffic and stealing documents. The final group were the 'guardians,' who tried to strike a balance between privacy rights and the need for state security, serving as partners of intelligence agencies while at the same time conducting a thorough examination of budgets and intelligence operations, demanding competence and law-abiding behaviour from these agents.[76] The majority of legislators, Johnson finds, have become cheerleaders for surveillance. He also concludes that despite the importance of the oversight work of Congress:

[72] Loch K. Johnson, 'Congressional Supervision of American's Secret Agencies: The Experience and Legacy of the Church Committee' 64(1) (2004) *Public Administration Review* 1, 3-14.
[73] Pub. L. No. 96- 450, § 501, 94 Stat. 1975, 1981 (1980).
[74] Loch K. Johnson, 'Legislative Reform of Intelligence Policy' 17(5) (1986) *Polity* 49-73.
[75] Loch K. Johnson, 'Ostriches, Cheerleaders, Skeptics and Guardians: Role Selection by Congressional Intelligence Overseers' 28(1) (2008) *SAIS Review* 93, 98-101.
[76] ibid.

> [A]nd the startling revelations of domestic spying in 1975, the contemporary [Bush era] practice of intelligence accountability on Capitol Hill has been largely desultory. The number of intelligence oversight hearings has declined in recent years…..and lawmaker attendance at hearings has been off-and-on.[77]

There is evidence that even before 9/11, the Bush Administration was violating the Communications Act of 1934,[78] the FISA Act of 1978 and the U.S. Constitution. In June 2006, it came to light that the NSA asked AT and T, the largest telecommunications company in the United States, to help it set up a domestic call-monitoring site seven months before the September 11 attacks.[79] In response, the Bush Administration asserted that what the NSA had done had become necessary after 9/11, an assertion totally undermined by the fact that the NSA request was made well in advance.[80]

On 16 December, 2005, two journalists, James Risen and Eric Lichtblau, reported that months after the 9/11 attacks, President Bush secretly authorised the NSA to eavesdrop on Americans and others inside the U.S. to search for evidence of terrorist activity without the Court-approved warrants required under the terms of FISA for domestic spying, These two journalists won a Pulitzer Prize for reporting how the second Bush Administration appeared to have violated the FISA requirement even for national security wiretaps. They revealed that under a Presidential Order signed in 2002, the NSA had 'monitored the international telephone calls and international e-mails of hundreds, perhaps thousands, of people inside the United States without warrants over the past three years,' and that the NSA was still seeking warrants to monitor 'entirely domestic communications.'[81] This Executive decision to permit eavesdropping inside the United States without Court approval represented a major change in American intelligence-gathering practices, in particular for the NSA, whose function is to spy on communications abroad. It

[77] ibid, 97.
[78] Title 47, Chapter 5 Subchapter 1 S 151.
[79] Andrew Harris, 'Spy agency Sought U.S. Call Records Before 9/11, Lawyers Say.' (*Bloomberg* 30 June 2006) <http://www.bloomberg.com/apps/news?pid=newsarchive&sid=abIV0cO64zJE> accessed 29 March 2015.
[80] ibid.
[81] James Risen and Eric Lichtblau, 'Bush Lets U.S. Spy on Callers Without Courts.' *New York Times* (14 December, 2005).

also recalibrated the existing data privacy/national security balance in order to address threats to national security that might be posed by anticipated further terrorist attacks. This recalibration was effected in a climate of widespread fear not conducive to calm assessments of the potential threats to national security. It is understandable that in such a climate, anticipation of unpredictable but possibly devastating events tended to override concerns over the inevitable loss of data privacy involved in the recalibrating process. The end result of this kind of rebalancing process, as Zedner points out, is that 'fundamental rights that ought to be considered non-derogable and to be protected are sacrificed to the consequentialist claims of security.'[82]

The response of the Bush Administration to criticisms of these new privacy-invasive practices undertaken without Court-approved warrants and targeting up to 500 people in the U.S. at any given time was that these were necessary because the NSA had 'to move quickly to monitor communications' that might 'disclose threats to the United States.'[83] Furthermore, these warrantless eavesdrops on U.S. citizens 'had been a critical tool in helping disrupt terrorist plots and prevent attacks inside the United States.'[84] The White House asked *The New York Times* not to disclose details of NSA domestic spying, arguing that 'it could jeopardize continuing investigations and alert would-be terrorists that they might be under scrutiny.'[85] Advocates of privacy rights might have good reason to draw attention to the paradox that while compromising the privacy of their fellow-citizens, NSA operatives needed to keep their own privacy-invasive activities private.

The major U.S. legislative response to the 9/11 attacks on the American mainland was the passage of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 [86] This Act is popularly known by its acronym, the Patriot Act. It is important to note that, as its full title suggests, the Act departs from the established legal policy of 'consequence management' in managing threats, that is by simply responding to terrorist acts committed by enemies of the State

[82] Lucia Zedner, *Security: Key Ideas in Criminology* (Routledge, London, 2009) 136.
[83] ibid.
[84] ibid.
[85] ibid.
[86] Public Law No. 107-56, 115 Stat. 272, at 50 U.S.C. Section 401(a).

identified by the security agencies as having perpetrated, or having been associated with, these acts.[87] Instead, those who devised the terms of the Patriot Act took the view that those who threatened the security of the State employed methods so unconventional that they could not be defeated under traditional rules governing law enforcement, and as a consequence, a policy of pre-emption, underpinned by law, remained the only way to prevent terrorism.

4.0 Ideological Context of the Patriot Act

The post-9/11 pre-emptive security policy is commonly seen as the implementation of the 'Ashcroft Doctrine,' the law-enforcement strategy devised by John D. Ashcroft, Attorney-General in the first George W. Bush Administration from 2000 to 2004. The Ashcroft Doctrine has four basic tenets: (1) The potential toll of terrorism is so enormous that prevention is essential (2) A powerful government [Executive] is a prerequisite for real liberty (3) Terrorism [in the form of the 9/11 attacks, for example] is an act of war, and therefore should be treated differently from other crimes and (4) The rules of war trump normal civil rights protections [e.g. data protection] when the government is pursuing alleged terrorists. In the context of the Ashcroft Doctrine, pre-emption, or prevention, in contrast to traditional law enforcement, means that 'the focus is not on punishing past criminal activity, but on getting potential terrorists behind bars - using any available pretext - before they can do harm.'[88] The 'available pretexts' were to involve, among other privacy-invasive measures, the collection and analysis of 'vast amounts of U.S. Internet and telephone communications' by the National Security Agency and a Classified order from the U.S. Foreign Intelligence Court (FISC) compelling Verizon, a major U.S. telecommunications company, to 'deliver millions of its customers' telephone calls to the National Security Agency.' [89] As Gorman suggests, Ashcroft's anti-terrorism' policy is in many respects a domestic mirror-image of President Bush's foreign policy: '[j]ust as Bush talks of promoting peace by using the nation's war machine, Ashcroft talks of promoting liberty by using the government's police powers.'[90]

[87] Christopher P. Banks, 'Security and Freedom After September 11: 'Limits and Ethical Costs of Terrorism Prosecutions' *Public Integrity* 1(1) (2010-2011) 5 6; Michael T. McCarthy, 'USA Patriot Act' 39 (2002) *Harvard Journal on Legislation* 435, 435-453.
[88] Siobhan Gorman, 'The Ashcroft Doctrine' 34 (51-52) (2002) *National Journal* 3712.
[89] Joseph D. Mornin, 'NSA Metadata Collection and the Fourth Amendment' 29(4) (2014) *Berkeley Technology Law Journal* 985.
[90] Siobhan Gorman, 'The Ashcroft Doctrine' 34 (51/52) (2002) *National Journal* 3712.

While the pre-emption policy was a major component of Administration security strategy post-9/11, another significant one was to persuade Congress to move swiftly to authorise new surveillance powers for the federal government, in effect, for the President. The new powers were comprehensively embodied in the Patriot Act, which was signed into law on October 26, 2001, less than six weeks after the attacks on New York and Washington. Broadly speaking, from the point of view of the privacy/security balance, the Patriot Act legislation enacted by Congress granted additional wiretapping and surveillance authority to federal law enforcement agencies, removed communication barriers hitherto existing between law enforcement and intelligence agencies (the FISA Wall), mandated financial disclosure and reporting requirements to combat terrorist funding.[91]

5.0 Provisions of the Patriot Act

The Patriot Act embodies a series of amendments to existing laws enacted in the 1970s and 1980s. These amendments were designed to make it easier for U.S. law enforcement agencies 'to conduct surveillance and to access data for the purpose of preventing, detecting and investigating crimes and terrorist acts.'[92] For example, previously, if law enforcement needed to have access to data held by communication providers in multiple states, it had to seek separate search warrants from separate judges. The Patriot Act amendments allowed for this type of investigation to require only one search warrant to be obtained from one federal judge. This change streamlined the process for U.S. government searches.[93] Title II of the Act greatly extended the availability and scope of surveillance provisions and wiretapping orders. Any District Court judge in the U.S. was empowered to issue a surveillance order,[94] while the scope of search warrants was expanded by means of an Amendment of Title III of the Stored Communications Act (1986).[95] As a result, access to stored voicemail could be obtained by the FBI by means of a search warrant, as opposed to the provisions made in wiretap laws.[96] Subpoenas issued to Internet Service Providers were expanded in scope and now included addresses,

[91] Pub. L. No. 107-56, 115 Stat 272 (2001).
[92] ibid.
[93] Francois Gilbert, 'Demystifying the United States Patriot Act' *Journal of Internet Law* 16(8) (2013) 1, 3-4.
[94] Title II, Section 216.
[95] 18 U.S.C. SS 2701-12 ('ECPA').
[96] Patriot Act, Title II, Sections 204 and 209.

telephone numbers, long distance and local telephone billing records, other subscriber information, the length of service of a subscriber in addition to IP addresses.[97] Communication service providers were given the right to disclose consumer records or communications should they suspect that a threat to 'life and limb' might exist.[98]

The Patriot Act provided a number of mechanisms by which the government could override previous legal controls on privacy-invasive methods of intelligence-gathering. The wiretapping and intelligence provisions of the Act minimise the role of the Court in ensuring that wiretapping is undertaken in accordance with law and are shown to be justified; they also permit the use of intelligence investigative authority to circumvent standard procedures that protect privacy rights. Before the Patriot Act came into force, its preceding legislative forerunner, the Foreign Intelligence surveillance Act (FISA) (1978) could be used only when foreign intelligence gathering was the primary purpose of the surveillance. The Patriot Act allows the use of FISA surveillance authority, even in cases where the primary purpose of such surveillance is a criminal investigation, and intelligence surveillance is merely a 'significant purpose.' It also provides for unconstitutional physical searches and wiretaps, contrary to the Fourth Amendment, and also for the conduct of such searches without probable cause, while extending a very low threshold of proof for the right of access to Internet communications.

One key provision of the Act, its allowance for nationwide service of pen registers (logs of phone numbers) and trap and trace orders, does not appear to conform to the Fourth Amendment protection requiring that warrants specify the place to be searched. This has profound implications, from the perspective of the evidential concepts of mirror and similar fact evidence, particularly in relation to remote devices, especially when these are synchronised with fixed terminals or desktop computers. This provision means that judges cannot effectively monitor the extent to which their orders are used to access information about the content of Internet communications. As a consequence, the supervisory role of the judiciary is marginalised. A further provision, the

[97] ibid, Title II, Section 210.
[98] ibid, Title II, Section 212.

granting of wide access to the FBI to the records of an individual employed in a business, represents a notable invasion of the privacy of that individual. To obtain this access, the FBI is merely required to certify to a court that the records it seeks may be relevant to an intelligence investigation. Thus, the FBI can require a business to turn over such confidential details as a person's medical, financial, mental health and travel records based on a low standard of proof and in the absence of appropriate judicial oversight. It is important to note that the provisions of the Patriot Act, discussed above, seen in the context of 'the fight against terrorism,' have little if any relevance to this 'fight,' and may be regarded as supererogatory, since before the Act came into force, the FBI already had authority to monitor Internet and telephone communications. What the Act facilitates is not merely the surveillance of terrorists, but all surveillance in the U.S.A., including the investigation of political opponents.

The Patriot Act explicitly revised FISA to make it easier for the government to conduct surveillance under the FISA framework.[99] One of its significant amendments to FISA allowed for 'roving' warrants that applied to all telephones used by a particular target rather than to specific telephone numbers,[100] while another amendment permitted intelligence agencies to share among themselves information they secured through eavesdropping.[101] It had been noticed by a number of commentators that while the Bush Administration was publicly canvassing the Patriot Act, with the purpose of easing the FISA requirements, it was at the same time secretly initiating an NSA programme which totally ignored the FISA framework and Bush was publicly declaring that the FISA modifications under the Patriot Act were sufficient for fighting terrorism.[102]

In the course of the decade in which it was passed, the Patriot Act was amended, refined and supplemented by other enactments with similar purposes. The Intelligence Prevention Act 2004, amended in 2006, included a definition

[99] Public Law No. 107-56, 115 Stat. 272 (2001). See Amitai Etzioni, 'Imperfections of Select New Technologies for Individual Rights and Public Safety' 15(2) (2002) *Harvard Journal of Law and Technology* 258, 266ff.
[100] ibid, at 206.
[101] ibid, at 203.
[102] Glenn Greenwald, *How would a Patriot Act? Defending American Values from a President Run Amok* (Working Assets Publishing, 2006) 14; James Risen and Eric Lichtblau, 'Bush Lets U.S. Spy on Callers Without Courts' (*New York Times*, December 16, 2006).

of *agent of a foreign power* as any person other than a United States person, 'who engages in international terrorism or activities in preparation therefor.'[103] This was followed by the Protect America Act which amended the Foreign Intelligence Surveillance Act and was signed into law by President George W. Bush on 5 August, 2007.[104] This authorised wide-ranging harvesting of every kind of information, in effect mandating a massive surveillance dragnet. One of its controversial elements was the removal of the requirement for government surveillance of foreign intelligence targets, if these were 'reasonably believed to be outside the United States.'[105]

The part played by Congress in the passage of the USA Patriot Act came in for strong criticism by civil liberties groups. Under the U.S. system of checks and balances, Congress has traditionally been expected to oversee the work of the executive branch and its agencies. One civil liberties group, the American Civil Liberties Union (the ACLU), argued that many of the surveillance measures included in the Patriot Act were enacted in extreme haste without the customary hearings and deliberations. Representatives of the ACLU, in a letter to the U.S. Senate, urging rejection of the final version of the Act, described the process leading to the drafting of the legislation as 'terribly flawed,' involving 'a few Senators [meeting] behind closed doors on October 12, 2001 to craft a Bill.'[106]

The full Senate was presented with anti-terrorism legislation 'in a take-it-or-leave-it' fashion, with little opportunity for input or review,' and would be forced to vote on legislation that it has not had the opportunity to read. The process involved a rejection of regular order and was 'an offence to the thoughtful legislative procedures necessary to protect the Constitution and the Bill of Rights at a time when the [privacy] rights of so many Americans are being jeopardised.'[107] Supporters of the Administration, however, shared the common assumption that there were other terrorist agents in the U.S. after 9/11, and that other attacks were imminent, and that on that basis tried to

[103] Title VI, Subtitle A, Section 6001: Individual Terrorists As Agents of Foreign Powers, (a) Publ. Law, 108-458, December 17, 2004. 50 USC, 1801.
[104] Pub. L. 110-55, 121 Stat. 552, enacted by S. 1927.
[105] ibid, Section 105B. (a).
[106] Amitai Etzioni, 'Imperfections of Select New Technologies for Individual Rights and Public Safety,' 15(2) (2002) *Harvard Journal of Law and Technology* 258-290, 286, fn 191.
[107] ibid.

hasten the passage of the Patriot Act. This view was articulated by Senator Hatch, who argued that if [surveillance] tools in the Patriot Act 'will help us in our continued pursuit of terrorists - then we should not hesitate to enact these measures into law…. the legislation we pass to-day will enhance our abilities to protect and prevent the American people from ever again being violated as we were on September 11.'[108]

On 19 January 2006, the U.S. Department of Justice issued a document setting out the legal basis for warrantless surveillance and other privacy-invasive measures undertaken by the NSA, on the authorisation of President Bush. This document placed considerable emphasis on the express recognition by Congress, in its passage of a measure, The Authorization for Use of Military Force Against Terrorists (AUMF), that 'the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States.'[109] In reference to specific measures taken by the NSA with Presidential authority, the document claimed that 'a consistent understanding' had developed 'that the President has inherent constitutional authority to conduct warrantless searches and surveillance within the United States for foreign intelligence purposes.'[110] Furthermore, it claimed that every federal appellate court to rule on the question 'has concluded that the President has inherent Constitutional authority to conduct searches for foreign intelligence purposes without securing a judicial warrant.'[111] The document also dealt with the problem that under the FISA statute, warrants authorising the conduct of such searches were required, by again invoking the principle that since the President has inherent authority to conduct warrantless searches, 'FISA could not encroach on the President's constitutional power.'[112] This same principle was also strongly affirmed by Supreme Court Justice Clarence Thomas in a dissenting opinion in *Hamdan v Rumsfeld,*[113] when he wrote that ‘military and foreign policy judgements are decisions of a kind for which the Judiciary has neither aptitude nor responsibility, and which has long been held

[108] ibid, fn 192, 287.
[109] 'Legal Authorities Supporting the activities of the National Security Agency Described by the President' US Department of Justice, Washington D.C., 20530, January 19, 2006 1. 6. <https://epic.org/privacy/terrorism/fisa/doj11906wp.pdf> accessed March 22, 2015.
[110] ibid, 7.
[111] ibid, 8.
[112] ibid.
[113] 548 U.S. 557 (2006).

to belong in the domain of political power not subject to judicial intrusion or inquiry'.[114] However, the Department of Justice argued that the President had inherent authority to conduct foreign surveillance, and that this authority trumped the judicial warrant requirement under the FISA statute. The basis of this argument was called into question by the Supreme Court ruling in *Hamdi v Rumsfeld*.[115]

Here, the Court refrained from deciding whether the President possessed inherent authority, as he claimed he did, to convene military commissions in the absence of Congressional authorisation. The majority held that the President 'may not disregard limitations the Congress has, in proper exercise of its own war powers, placed on his powers.'[116] Although *Hamdan v Rumsfeld* deals with a specific issue - whether the military commission set up by the Executive had authority to try Hamdan - it raises significant issues which have a bearing on national security law and executive power, and by extension, on national security law and privacy, in the context of Executive surveillance policies post-9/11. In *Hamdan*, the Supreme Court concluded that the Congress and President share power over the execution of a war, significantly rejecting the Bush Administration's theory over unilateral executive power in times of war. The judgment in *Hamdan*, insofar as it has relevance to the privacy/security balance 'signalled that the Supreme Court would not automatically defer to the President in all matters related to national security'.[117]

As if to illustrate the degree of confusion surrounding the scope of Executive power, inherent or otherwise, in respect of wholesale warrantless data mining, a U.S. Foreign Intelligence Court of Review, in a heavily redacted opinion delivered in January 2009, ruled in favour of the warrantless wiretapping provision in the Protect America Act of 2007. In a rare public ruling, the secret Federal Appeals Court said that telecommunications companies must co-operate with the government to intercept international telephone calls and e-

[114] Cited in *Hamdi v Rumsfeld*, 542 US 507, 582-583 (2004).
[115] *Hamdan v Rumsfeld*, 548 US 557 (2006).
[116] Ibid, 1, 29 (fn 23) (Opinion of the Court), citing *Youngstown Sheet & Tube Co v Sawyer*, 343 US 579, 637 (1952) (Justice Jackson, concurring).
[117] Julia Lohman, 'Hamdan v Rumsfeld, 548 U.S. 557 (2006)' *Lawfare Hard National Security Choices* (12 November, 2012) <http://www.lawfareblog.com/wiki/the-lawfare-wiki-document-library/post-911-era-materials/post-911-era-materials-court-cases/hamdan-v-rumsfeld-548-us-557 2006/> accessed 23 March 2015.

mails of American citizens suspected of being spies or terrorists. This ruling came in a case involving an unidentified company's challenge to the 2007 Act, which had enlarged the President's legal power to conduct wiretapping without warrants for intelligence purposes. The FISA Court of Review ruling is 'the first by an Appeals Court that says that the Fourth Amendment's requirement for warrants does not apply to the foreign collection of intelligence involving Americans.'[118]

A further significant development in the etiolation of data privacy rights was The Foreign Intelligence Surveillance Act 1978 Amendments Act,[119] passed by Congress in 2008, which retroactively legalised the warrantless wiretapping programme, thus effectively immunising telecommunications companies that had participated in the secret NSA programme.[120] The FISA Amendments Act allowed the president to engage in a broad range of electronic surveillance without being obliged to seek warrants against particular individual targets of such surveillance.[121] A report describes this Amendment as posing 'a much graver risk to EU data sovereignty than other laws hitherto considered by EU policy makers.'[122] The gravity of this risk, according to Casper Bowden, formerly Chief Adviser to Microsoft Europe and co-author of the Report, arises from the fact that the FISA Amendment created a power of mass surveillance 'specifically targeted at the data of non-U.S. persons located outside America, which applies to cloud computing'.[123] As a consequence, U.S. companies with a presence in the EU can be compelled, under a secret surveillance order, issued by a secret court, to hand over data on Europeans. According to Bowden, The Foreign Intelligence Surveillance Act 1978 Amendments Act (2008) makes it expressly lawful for the U.S. to do 'continuous mass surveillance of the ordinary, lawful democratic political activities, and could even go so far as to

[118] James Risen and Eric Lichtblau, 'Court Affirms Wiretapping without warrants' (*New York Times,* 16 January, 2009).
[119] Pub. L. No. 110-261, 122 Stat. 2436, 2437-78 (2008) Codified in 50 U.S.C. §§ 1801-12.
[120] Jack M. Balkin, 'The Constitution in the National Surveillance State' 93 (2008) *Minnesota Law Review* 1, 2.
[121] H.R. 6304, 1801-12.
[122] 'Fighting Cyber Crime and Protecting Privacy in the Cloud' Directorate-General For Internal Policies. Centre for the Study of Conflicts, Liberty and Security (European Parliament, 2012). 1 34.<http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/study_cloud_/study_cloud_en.pdf> accessed 1 April 2015.
[123] ibid, 33.

oblige U.S. cloud providers such as Google to make available a live 'wiretap' of European users' data.'[124]

6.0 Executive Dominance, Congressional Acquiescence and Marginalisation of Data Privacy Concerns

The significant extension of Executive authority in the wake of September 11 and the exercise of this authority to facilitate programmes of data mining which, civil libertarians and privacy advocates alleged, constituted an overbroad and unjustified infringement of privacy,'[125] has, as McCarthy points out, become 'a focal point for the ongoing national debate over balancing protection against terrorism with preserving civil liberties.'[126] At the heart of this debate are the powers granted to the executive by the Patriot Act, and the 'secret' wholesale data-mining activities of the National Security Agency, brought to light in 2013 by Edward Snowden, a former employee of the Agency.[127]

The privileges for national security extend to oversight and have invariably conflicted with accountability. Public accountability necessitates an important degree of transparency in data processing operations. The national security privileges, however, grant *secrecy* to data surveillance operations. There is consequentially an inherent contradiction between the secrecy of intelligence operations and the requisite transparency for public accountability. The balance between these privileges for national security and effective oversight either by Congress or the judiciary is unstable. The Chief Judge of the FISA Court admitted that the Foreign Intelligence Surveillance Court is forced to rely on the accuracy of the information that is provided to the Court.[128] The Director of National Intelligence, James Clapper, even testified before Congress in 2014

[124] Ryan Gallagher, U.S. Spy Law Authorizes Mass Surveillance of European Citizens' *future*tense The Citizen's Guide To The Future* (January 8, 2013). <http://www.slate.com/blogs/future_tense/2013/01/08/fisa_renewal_report_suggests_spy_law_allows_mass_surveillance_of_european.html> accessed 29 March 2015.
[125] Walter Shapiro, Usual Adversaries Unite Over Threat to Liberties, *USA Today* 26 (September 2001) at A6.
[126] Michael T. Mc Carthy, 'Recent Developments' (39 (2002) *Harvard Journal on Legislation* 435, 436.
[127] Luke Harding, *The Snowden Files*, (New York, 2014).
[128] Carol D. Leonnig, 'Court: Ability to Police U.S. Spying programme Limited' *Washington Post* (15 August, 2013).

that the NSA was not collecting intelligence on millions of Americans.[129] The testimony turned out to be false.[130]

7.0 The Obama Presidency: Continuity with the Surveillance Policies Under President Bush

While the Obama Administration promised substantial changes from that of its predecessor in the areas of transparency, intelligence gathering and national security, it differed very little from the Bush Administration in any of these respects, and in many instances, the Obama Administration augmented and increased its surveillance activities in its 'secret war' on information and on those actors it deemed to be adversaries and threats to 'state secrets.' As Warren and Dirksen point out:

> Instead of a dramatic break from the politics of his predecessor, Obama's approach to the balance of national security objectives and privacy concerns, has deeply contravened the Administration's initial pronouncements of a new 'openness' and 'transparency'…. From the treatment of whistleblowers to the assertive expansion of the National Security Agency (NSA) surveillance programmes, it has been an amplified 'business as usual' approach that could significantly mar the Obama Administration's legacy.[131]

While initially characterising the acts of whistleblowers as manifestations of 'courage and patriotism' that 'should be encouraged rather than shifted,'[132] in speaking of the Edward Snowden disclosures he offered a rebuttal of his earlier position on whistleblowers, saying he did not welcome leaks, 'because there's a good reason why these programs are classified.'[133] On the basis of his rhetoric during his campaign for the Presidency in 2008, it was widely expected that the

---

[129] Hearing on Current and Projected National Security Threats to the United States Before the Senate Select Committee on Intelligence, 113th Cong., 1st Sess., at 66 (March 12, 2013). Available at: <http://www.intelligence.senate.gov/131113pdfs/11389.pdf> Accessed 29 March 2015.

[130] James Risen and Laura Poitras, 'NSA Examines Social Networks of US Citizens' (*New York Times* September 29, 2013).

[131] Aiden Warren and Alaxendar Dirsken, 'Augmenting State Secrets: Obama's Information War' 9(1) (2014) *Yale Journal of International Affairs* 68-84, 68.

[132] See Joseph Toomey, *Change You Can Really Believe In. The Obama Legacy Of Broken Policies and Failed Policies* (AuthorHouse, 2012) 338, fn 1118.

[133] Tom McCarthy, ' Obama defends secret NSA surveillance programs,' *The Guardian* (7 June 2013).

Presidency of Barack Obama would bring significant changes in security policy, particularly in relation to mass surveillance of data, privacy rights, the use of torture to obtain information and indefinite detention without trial. During the Democratic Party Primaries of 2008, he promised to filibuster against a proposal amnesty for telecoms firms that had illegally co-operated with a request by the Office of Bush's Vice-President to divulge information about their customers. The conduct of the telecoms firms was a violation of the Foreign Intelligence Surveillance Act (FISA), which forbade eavesdropping on Americans, without judicial oversight. However, in July 2008, once he had secured the Democratic Party nomination, this became the first promise on which he reneged, in keeping with a slogan adopted by his administration in its early days: '[w]e look to the future not the past.'[134]

However, for a brief period upon taking office in 2009, he championed the cause of government transparency in matters of data surveillance, and spoke admiringly of whistle-blowers, describing them as 'often the best source of information about waste, fraud and abuse in government.'[135] This outlook is of a piece with Obama's rhetoric in the lead-up to the 2008 Presidential Election, when he signified that, should he be elected, a key tenet of his presidency would be 'reversing President Bush's policy of secrecy' in relation to data surveillance and data mining.[136] On his first day in office, Obama called for a 'new standard of openness' in the federal government, and issued three memoranda in support of increased transparency and open government.[137] He also declared that 'transparency and rule of law will be touchstones of this presidency.'[138]

In the first of his three memoranda, the 'Transparency and Open Government' memorandum for the Heads of Executive Departments and Agencies, Obama declared that his Administration was committed to creating an unprecedented

[134] David Bromwich, 'Obama's Mental Bookkeeping,' *London Review of Books* 27 May, 2011.
[135] Jane Meyer, 'The Secret Sharer,' *The New Yorker* 23 May, 2011.
[136] Blueprint for Change: Obama and Beiden's Plan for America' *Obams'08* 1 75 <https://s3.amazonaws.com/s3.documentcloud.org/documents/550007/barack-obama-2008-blueprint-for-change.pdf> accessed 1 May 2015.
[137] Barack Obama, 'A New Standard of Openness,' White House Video, January 21, 2009. <https://www.whitehouse.gov/photos-and-video/video/a-new-standard-openness> accessed 3 May, 2015.
[138] Sheryl Stolberg, 'On First Day, Obama Quickly Sets a New Tone,' *The New York Times* January 21, 2009.

level of openness in government. His aim was to enhance public trust by establishing a transparent system based on the principle that openness 'will strengthen our democracy and promote efficiency and effectiveness in Government.'[139] While the Obama Administration appeared to herald significant changes in transparency, intelligence gathering and national security policies, it has differed very little from the Bush Administration in its substantive approach. The evidence suggests that, as President, Obama could no longer regard himself as an advocate of privacy rights or a defender of whistle-blowers, but instead saw himself as having responsibility for the protection of all Americans against the threat, real or perceived, posed by terrorists, and as heir to the practices of the National Surveillance State inaugurated by George W. Bush.[140] Instead of being characterised by a dramatic break from the policies of the Bush era, the Obama Administration has featured 'an apparent continuation of and, in some cases, an augmentation' of these policies.[141] As with the Bush Administration, the Obama Government works to safeguard 'state secrets' while it 'simultaneously accumulates more of them than ever before, collating a significant amount of data through classified programs that are exempt from the traditional avenues of public access.'[142]

There is considerable evidence to suggest that the White House, in the opening years of the Obama Presidency systematically pursued policies in relation to the privacy/security balance consistent with those pursued during the second term of the Bush Administration from 2004 to 2008. Obama's changed attitude to whistleblowers, whom he once publicly vindicated for exposing 'fraud and abuse in government' and as champions in the cause of government transparency, whose acts exemplified 'courage and patriotism' that should be encouraged rather than stifled'[143] and later came to see as enemies of the State, is one notable illustration of this tendency, which was highlighted in the case of

[139] Barack Obama, 'President's Memorandum on Transparency and Open Government - Interagency Collaboration. Memorandum For Heads Of Departments And agencies M-09-12. February 24, 2009 <https://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_fy2009/m09-12.pdf> accessed 2 May 2015.
[140] For a good treatment of the characteristics of the National Surveillance State, see Jack M. Balkin, 'The Constitution in the National Surveillance State' 93 (2008) *Minnesota Law Review* 1.
[141] Aiden Warren and Alexander Dirksen, 'Augmenting State Secrets: Obama's Information War' 9(1) (2014) *Yale Journal of international Affairs* 68, 69.
[142] ibid, 70.
[143] ibid, 74.

whistle-blower Thomas Drake. A former senior executive of the NSA, Drake retained top secret documents which he leaked to a reporter on the *Baltimore Sun*, who wrote a series of prize-winning articles based on the material supplied by Drake, exposing dubious legal practices in the NSA counterterrorism programmes. Legal proceedings against Drake were initiated under the Bush administration. In 2010, under the Obama Administration, ten charges were brought against Drake by the Department of Defence, with five citing the 1917 Espionage Act. Conviction on all counts could have carried a prison sentence of thirty-five years. He was facing some of the gravest charges that could be brought against an American citizen. Prosecuting the case against Drake involved two difficulties for the government. Firstly, it would have faced the problem of having to reveal information on a covert intelligence programme in order for the case to proceed, and secondly, any case would have been undermined by a revelation that the government sought a plea bargain with Drake in June 2011 after five years of investigation, half of which was pursued under the Obama Administration.[144] In 2010, the year in which proceedings against Drake were instituted, Gabriel Schoenfeld, a Conservative political scientist at the Hodson Institute, an advocate for more stringent protection of classified information, was able to argue that 'Obama has presided over the most draconian crackdown on leaks in our history - even more than Nixon.'[145]

Two significant security statements, one by Bush and the other by Obama, make it clear that Obama's understanding of the duties and responsibilities of his office as President, when security/privacy policies were in question, had significant commonalities with that of George W. Bush. The continuities between the security priorities of the two Administrations become manifest when one compares Obama's major security policy speech at the National Archives in May 2009 [146] with Bush's defence of his own security measures in

[144] Marcy Wheeler, 'Government Case Against Whistleblower Thomas Drake Collapses,' *The Nation*, June 13, 2011).
[145] Gabriel Schoenfeld, *Necessary Secrets* (2010), cited by Jane Mayer, 'The Secret Sharer: Is Thomas Drake an Enemy of the State?,' *New Yorker*, May 23, 2011.
[146] Remarks By The President On National Security. *The White House* Office of the Press Secretary May 21, 2009. *National Archives*, Washington D.C. <https://www.whitehouse.gov/the_press_office/Remarks-by-the-President-On-National-Security-5-21-09/> accessed 20 April 2015.

January 2006.[147] While Obama was critical of some aspects of Bush's security initiatives - the use of torture, waterboarding and detention without trial, for example, he was nevertheless prepared to believe that many of these decisions 'were motivated by a sincere desire to protect the American people.'[148] Obama's 2009 speech echoed much of what Bush had to say in 2006. For example, where Bush had said that 'the al Qaeda terrorist network launched the deadliest foreign attack on American soil in history,' Obama's version of 9/11 was '[w]e are less than eight years removed from the deadliest attack on American soil in our history.'[149] Bush had declared that '[t]he President has chief responsibility under the Coalition to protect America from attack,'[150] while Obama asserted that 'my single most important responsibility as President is to keep the American people safe.'[151] Bush had warned that '[a]l Qaeda's leadership has pledged to attack the United States again at a time of its choosing.'[152] Obama's version of this was that '[w]e know that al Qaeda is actively planning to attack us again'[153] Bush explained that NSA activities 'enable us to move faster and quicker….We've got to be fast on our feet, quick to detect and prevent.'[154] Obama endorsed this by assuring his listeners that '[w]e're investing in the 21st Century military and intelligence capabilities that will allow us to stay one step ahead of a nimble enemy.'[155]

---

[147] Legal Authorities Supporting the Activities of the National Security Agency Described by the President, (January 19, 2006) US Department of Justice, Washington D.C. 20530. <http://www.justice.gov/sites/default/files/olc/opinions/2006/01/31/nsa-white-paper.pdf> accessed 22 March, 2015. Henceforth cited as LA.

[148] ibid, at 2.

[149] ibid, at 1.

[150] ibid.

[151] Remarks By The President On National Security. *The White House* Office of the Press Secretary May 21, 2009. *National Archives*, Washington D.C. <https://www.whitehouse.gov/the_press_office/Remarks-by-the-President-On-National-Security-5-21-09/> accessed 20 April 2015.

[152] Legal Authorities Supporting the Activities of the National Security Agency Described by the President, January 19, 2006. <http://www.justice.gov/sites/default/files/olc/opinions/2006/01/31/nsa-white-paper.pdf> accessed 18 April, 2015, 2.

[153] Remarks By The President On National Security. *The White House* Office of the Press Secretary May 21, 2009. *National Archives*, Washington D.C. <https://www.whitehouse.gov/the_press_office/Remarks-by-the-President-On-National-Security-5-21-09/> accessed 20 April 2015.

[154] Legal Authorities Supporting the Activities of the National Security Agency Described by the President, January 19, 2006. <http://www.justice.gov/sites/default/files/olc/opinions/2006/01/31/nsa-white-paper.pdf> accessed 18 April, 2015, 5.

[155] Remarks By The President On National Security. *The White House* Office of the Press Secretary May 21, 2009. *National Archives*, Washington D.C. <https://www.whitehouse.gov/the_press_office/Remarks-by-the-President-On-National-Security-5-21-09/> accessed 20 April 2015.

Bush had explained that the surveillance activities of the NSA were 'carefully reviewed approximately every 45 days to ensure that [they were] being used properly,' further explaining that they were reviewed for legality for the Department of Justice and 'monitored by the General Counsel and Inspector General of the NSA to ensure that civil liberties were being protected.'[156] The nature of such assurances can scarcely have impressed privacy and other human rights advocates or civil liberties groups who were left to wonder what the Administration understood by the 'proper' use of NSA surveillance, which civil liberties were being protected, and how such protection could be safely left to officials associated with those entrusted with the duty of surveillance. In his address, Obama spoke much of the need to protect the American people while at the same time retaining largely unspecified American values. He had his own version of what privacy might mean when any of the agencies of national security were in question. He could never accept that 'our most sensitive national security matters should simply be an open book' and would 'vigorously defend the necessity of classification [i.e secrecy] to defend our troops at war, to protect sources and methods, and to safeguard confidential actions that keep the American people safe.'[157] He also upheld the doctrine of 'state secrets privilege' involving unspecified 'secret programmes' as being 'absolutely necessary in some circumstances to protect national security, acknowledging at the same time that 'we must not protect information merely because it involves the violation of a law [by agencies of State] or embarrassment to the government.'[158]

The continuity between the Bush and Obama Administrations can further be demonstrated by the willingness of the latter to replicate the policies of the former when dealing with mass surveillance and illegal invasions of privacy by means of illegal operations by security agencies. Those whistleblowers in particular who attempted to release critical classified information exposing illegal privacy-invasive practices by the NSA outside bureaucratic constraints,

[156] Legal Authorities Supporting the Activities of the National Security Agency Described by the President, January 19, 2006. <http://www.justice.gov/sites/default/files/olc/opinions/2006/01/31/nsa-white-paper.pdf> accessed 18 April, 2015, 5.
[157] Remarks By The President On National Security. *The White House* Office of the Press Secretary May 21, 2009. *National Archives*, Washington D.C. <https://www.whitehouse.gov/the_press_office/Remarks-by-the-President-On-National-Security-5-21-09/> accessed 20 April 2015.
[158] ibid.

have faced draconian responses from the Obama administration. Obama's pursuit of whistleblowers has been on an unprecedented scale. The journalist Amy Goodman has pointed out that 'evoking the Espionage Act of 1917, the [Obama] Administration has pressed criminal charges against no fewer than six government employees, more than all previous Administrations combined.'[159] The whistleblower Peter Van Buren observed that while the Obama Administration

> [H]as pursued no prosecutions against CIA torturers, senior leaders responsible for Abu Ghraib or other crimes, or anyone connected with illegal surveillance of American citizens, it has gone after whistleblowers and leaders with increasing fierceness, both in court and inside the halls of various government agencies.[160]

Before 9/11, an NSA employee, a crypto-mathematician and technical director named Bill Binney, devised a programme, ThinThread, to track enemies outside the U.S.A. His tracking system featured privacy controls and an anonymising device so that all American communications would be encrypted when a legally-mandated warrant was issued.[161] The system was small, cost-effective, and protected the identity of Americans, and thus their privacy.[162] Binney's model was rejected by the NSA Directorate, and a more elaborate one, known as the Trailblazer Project was put in its place, which was deployed to collect information on Americans.[163] However, Trailblazer was abandoned in 2006, having accumulated a loss of €1.2 billion. [164] Following the 9/11 attacks, under pressure from the White House and in nearly total secrecy, General Hayden, head of the NSA, sanctioned warrantless domestic surveillance.[165] Binney responded with frustration when he sensed that a version of his

---

[159] Amy Goodman, 'NSA Whistleblower Thomas Drake Prevails Against Charges in Unprecedented Obama Administration Crackdown.' *Democracy Now* March 21, 2012. <http://www.democracynow.org/2012/3/21/in_unprecedented_obama_admin_crackdown_nsa> accessed 21 April 2015.

[160] Peter Van Buren, 'Fear the Silence, Not the Noise.' *TomDispatch.com* February 9, 2012. <http://www.tomdispatch.com/blog/175500/tomgram%3A_peter_van_buren,_in_washington,_fear_the_silence,_not_the_noise/> accessed 23 April 2015. Abu Ghraib was a prison in Iraq where prisoners of war were questioned.

[161] Jane Mayer, 'The Secret Sharer,' *The New Yorker* 23 May, 2011.

[162] ibid.

[163] ibid.

[164] ibid.

[165] James Risen and Eric Lichtblau, 'Bush Lets U.S. Spy on Callers Without Courts *The New York Times* 16 December 2005.

programme, stripped of its privacy controls, was used in a new, privacy-invasive secret surveillance programme. With the removal of the protections afforded by the economisation process, the NSA could now target anyone. It had twisted a programme he had designed to track enemies outside the U.S.A. into an instrument for wholesale domestic spying, in addition to spying on suspects outside the U.S.A., converting the NSA into a potential violator of everyone's privacy rights, at home and abroad. He felt he had a duty to 'apologise to the American people,' since the programme he had devised for other purposes 'has violated everyone's rights,' and 'can be used to eavesdrop on the whole world.'[166]

Binney was a 32-year old veteran of the NSA, whose principles motivated him to become a whistleblower. He revealed details about Stellar Wind, the NSA's top-secret domestic spying programme, begun after 9/11, which proved so controversial that it almost led senior Department of Justice officials to resign in protest in 2004. In August 2012, Binney agreed to be interviewed by a journalist for *The New York Times*, Laura Poitras, telling her that he was 'tired of my government harassing me and violating the Constitution.'[167] The interviewer described Binney as 'among a group of NSA whistleblowers, including Thomas A. Drake, who have each risked everything - their freedom, livelihoods and personal relationships, to warn Americans about the dangers of N.S.A. domestic spying.'[168] Binney resigned from the NSA on principle in October 2001 but remained silent about the illegal activities of the NSA until after *The New York Times* revealed that the Agency was engaged in large-scale warrantless electronic surveillance. The controversy generated by this revelation eventually led to the passing of amendments to the Foreign Intelligence Surveillance Act in 2008, which Binney and others realised, simply gave legal protection to the NSA's data-mining operations, which were continued under the Obama Administration. When Binney began to protest behind the scenes, his home was raided by armed FBI agents.[169] In late 2011 Binney went fully public, giving details of what he considered 'a massive effort

[166] Cited by David Bromwich, 'Obama's Mental Bookkeeping,' *London Review of Books*, 27 May, 2011.
[167] Laura Poitras, 'The Program,' *New York Times* August 22, 2012.
[168] ibid.
[169] Binney was interviewed by Paul Harris, 'U.S. data whistleblower: 'It's a violation of everybody's rights,' *The Guardian* 15 September, 2012.

under the Obama Administration to collect virtually all electronic data in the country, from Facebook posts to Google searches to emails.'[170] As evidence for this contention, he pointed to the NSA's creation of enormous electronic storage facilities in Texas and Utah, with the capacity to store copies of all e-mails transmitted in America, for possible future retrieval. A consequence of the NSA's exhaustive data mining programme is that the entire United States can be watched, and any specific group or organisation monitored. Binney claims that the gigantic NSA building in Utah, as part of the Stellar Wind secret domestic spying system, is being designed to store huge amounts of accessible web information, such as social media updates, 'but also information in the "deep web" behind passwords and other firewalls that keep [the stored information] away from the public.'[171]

Binney has also been spreading his message beyond the U.S. In Berlin in July 2014, he was one of two former NSA operatives-turned-whistleblowers, the other being Thomas Drake, who testified before a cross-party Bundestag enquiry, giving his views on the NSA's 'wrong turn in using the 9/11 attacks to justify a mass global surveillance drive.' He told German M.P.s that '[t]he goal is control of the people. They want to have information about everything; this is really a totalitarian approach.'[172] A key issue for the participants in the Berlin enquiry was whether there was intelligence collaboration between the NSA and the German federal foreign intelligence service, the *Bundesnachtendienst* or DND. Binney dealt with this issue only after the enquiry committee went into closed session. Drake, however, was much more forthright. He dismissed as 'beyond any credibility' the claims of German Intelligence that it knew nothing of mass data collection by the NSA on German soil. He accused the German authorities of duplicity in its outrage over U.S. mass surveillance, claiming that the BND operated as an 'addendum or appendix of the NSA.' What is clear is that some German citizens were targets of NSA surveillance. Like Chancellor Merkel's phone, the computer of the German IT student, Sebastian Hahn, was

[170] ibid.
[171] ibid.
[172] Derek Scally, 'NSA Whistleblowers' testimony electrifies Bundestag committee' *Irish Times* 5 July, 2014.

identified in July 2014 as a further target of NSA surveillance via the XKeyscore programme.[173]

Obama's thinking on the privacy/security balance was revealed in his public comments as well as in his acts. At a time when the privacy rights of individuals throughout the U.S.A. and abroad were, as a few major whistleblowers were later to reveal, being routinely violated by the NSA with the connivance and acquiescence of the Administration over which he presided, Obama, in his National Archives Speech of May 2009, was defending the privacy rights of the U.S. military personnel. These had been photographed while torturing and dehumanising internees, or, as Obama euphemistically put it, 'violated standards of behaviour in these photos.'[174] Obama explained that he had recently opposed the release of these photographs on the advice of his security team because releasing them, would 'inflame anti-American opinion and allow our enemies to paint U.S. troops with a broad, damning and inaccurate brush, thereby endangering them in theatres of war.'[175]

In the Autumn of 2013, it became publicly known that the Obama Administration had been presiding over the monitoring by the NSA of the telephone records of foreign leaders, including those of the German Chancellor Angela Merkel. It also became known that the monitoring operation was still in place when Obama visited Berlin in June 2013. A spokesman for the Chancellor described the operation as 'a grave breach of trust.'[176] About the same time leaked U.S. Intelligence documents revealed that the Presidents of other nations friendly to the U.S.A. were also subject to intelligence surveillance. In September 2013, President Rousseff of Brazil postponed a State visit to the United States following news media reports that the NSA had intercepted messages from Ms. Rousseff, her aides, and the Petrobras state oil company. Other leaked documents indicated that U.S. Intelligence services had

[173] ibid.
[174] Remarks By The President On National Security. *The White House* Office of the Press Secretary May 21, 2009. *National Archives*, Washington D.C. <https://www.whitehouse.gov/the_press_office/Remarks-by-the-President-On-National-Security-5-21-09/> accessed 20 April 2015.
[175] ibid.
[176] 'Obama "knew and approved" NSA spying on Chancellor Merkel,' *Russia Today* October 27, 2013. < http://rt.com/news/obama-nsa-spying-merkel-808/> accessed 25 April 2015.

gained access to the communications of President Felipe Calderón of Mexico.[177]

Obama's renewal of some of the measures which had laid the legislative foundation for the surveillance operations undertaken and expanded during the Bush era further demonstrated the continuity between the privacy/security policies of the Bush and Obama Administrations. In 2001, the USA Patriot Act had facilitated the expansion of federal oversight capabilities, overthrowing traditional constitutional limits on government investigators, and altering, in a privacy-invasive sense, the oversight provisions embodied in the Foreign Intelligence Surveillance Act (FISA). On May 26, 2011, in the face of their imminent expiration on the following day, three amendments to FISA were extended by Obama until June 1, 2015. All three amendments were first enacted to expand the scope of federal intelligence-gathering agencies following the 9/11 attacks. Two of these amendments were enacted as part of the USA Patriot Act: Section 206 of the Act amended FISA to permit multipoint or 'roving' wiretaps by adding flexibility to the degree of specificity with which the location or facility subject to electronic surveillance under FISA must be identified. Section 215 of the Patriot Act amended FISA by enlarging the scope of materials that could be sought under FISA to include 'any tangible thing.' The same section also lowered the standard required before a court order may be issued to compel the production of materials relevant to an investigation.

The third amendment was enacted in 2004 as part of the Intelligence Reform and Terrorism Prevention Act (IRTPA). Section 60001(a) of that Act changed the rules regarding the types of individuals who may be targets of FISA-authorised searches. Also known as the 'lone wolf' provision, it permits surveillance of non-U.S. persons engaged in international terrorism without requiring evidence linking those persons to an identifiable foreign power or terrorist organisation.[178] Attempts by privacy and transparency advocates in the Senate to increase transparency as to how these amendments were to be

[177] Alison Smale, 'Anger Growing Among Allies on U.S. Spying,' *The New York Times* October 23, 2013.
[178] See Amendments to the Foreign Intelligence Surveillance Act (FISA), extended until June 1, 2015. Congressional Research Service, June 16, 2011.

interpreted were defeated, and the Senate renewed the legislation. The major objection of those who opposed Obama's unqualified extension of the FISA Amendments was that the FISC, the Court charged with oversight of the implementation of FISA, was a secret Court, the rulings of which were classified. Senate objectors to Obama's reauthorisation of this Bush-era legislation wanted the government either to declassify FISC rulings or to provide unclassified summaries of these rulings. Obama was unwilling to concede this.[179] Obama's position on preserving the secrecy of NSA activities and of the FISC that was supposed to oversee these was made clear after the extent of the NSA's massive illegal spying programme was revealed by whistleblowers in 2013, when he declared that he did not 'welcome leaks, because there's a reason why these programs are classified.'[180]

Despite a growing body of evidence of frequent and pervasive abuse of the scope of the NSA's powers, the Obama Administration has continued to afford 'steadfast support for the NSA programs.'[181] However, the secrecy surrounding the illegal activities of the NSA and the collusion of the government with these activities could no longer be guaranteed. In June 2013, a draft report by the NSA Inspector General leaked to *The Guardian* revealed that 'the Obama Administration, for more than two years, permitted the National Security Agency to continue collecting vast amounts of records detailing the email and internet usage of Americans.' [182] Following a lawsuit filed by the Electronic Frontier Foundation, the Obama Administration was forced to release an eighty-six page opinion of the secret Foreign Intelligence Surveillance Court (FISC) on August 21, 2013, which found that 'the surveillance conducted by the NSA under the FISA Amendments Act (2008), which had been extended by Obama until 2015, was unconstitutional and in violation of 'the spirit of

[179] See Mark Rumold, 'A New Year, A New FISA Amendments Reauthorisation, But the Same Old Secret Law,' *Electronic Frontier Foundation,* January 10, 2013. <https://www.eff.org/deeplinks/2013/01/new-year-new-fisa-amendments-act-reauthorization-same-old-secret-law> accessed 27 April 2015.
[180] Dan Roberts and Spenser Ackerman, 'Obama defiant over NSA revelations ahead of summit with Chinese Premier,' *The Guardian* June 7, 2013.
[181] Aiden Warren and Alexander Dirksen, Augmenting State Secrets: Obama's Information War' 9(1) (2014) *Yale Journal of International Affairs* 68, 75.
[182] Glenn Greenwald and Spenser Ackerman, 'NSA Collected US email records in bulk for more than two years under Obama,' *The Guardian* June 27, 2013.

federal law.'[183] The FISC judge noted that the NSA 'frequently and systematically violated' its own requirements by collecting up to 56,000 e-mails of Americans 'with no known connection to terrorism.'[184] The same FISC judge declared that 'contrary to the government's repeated assurances, the NSA had been routinely running queries of metadata using quarrying terms that did not meet the required standard for quarrying.'[185] Despite these FISA Court findings, leaks to *The Guardian* suggest that certifications required to conduct intelligence operations in co-operation with US technology firms were merely modified to allow the continuation of the programme, with the costs of these modifications borne by federal funds.[186] It further emerged that by December 2012, a new programme, codenamed (EVIL OLIVE) had been established to conduct the same type of surveillance that Obama Administration officials claimed had ceased in 2011.[187]

In the face of a continuing and growing stream of credible reports of irregular NSA privacy-invasive activities and the realisation among Americans that effective oversight mechanisms were not in place to set adequate limits on the telephone and internet data the government security apparatus was collecting as part of its 'war on terror,' Obama's response was to try to justify the massive range of data surveillance programmes that had been developing during the Bush Presidency and his own on the basis that the events of 9/11 had made such programmes necessary. However, Obama also found it difficult to ignore Congressional criticism of his Administration's anti-terrorist policies. In response to this criticism, he undertook to endorse more oversight, transparency and constraints, particularly on the use of Section 215 of the Patriot Act, which allows for the bulk collection and storage of domestic telephone records.

---

[183] Mark Rumold, EFF Victory Results in Release of Secret Court Opinion Finding NSA Surveillance Unconstitutional,' August 21, 2013 <https://www.eff.org/deeplinks/2013/08/eff-victory-results-expected-release-secret-court-opinion-finding-nsa-surveillance> accessed 27 April 2015.

[184] Ellen Nakashima, 'NSA gathered thousands of Americans' emails before Court ordered it to revise its tactics.' *The Washington Post* August 21, 2013.

[185] ibid.

[186] Ewen MacAskill, 'NSA paid millions to cover PRISM compliance costs for tech companies.' *The Guardian* August 23, 2013.

[187] Glenn Greenwald and Spenser Ackerman, 'How the NSA is still harvesting your online data' *The Guardian* June 27, 2013.

Some of the criticism came from unexpected sources. Then most trenchant critique of the consequences for privacy rights of the application of the Patriot Act and the workings of the FISA Court was that Congressman Jim Sensenbrenner, who was dismayed by *The Guardian's* revelations that the NSA was secretly collecting all the records from Verizon, the major U.S. telecoms company. The significance of this critique lay in the fact that Sensenbrenner was the author of the original Patriot Act in the aftermath of the September 11 attacks. He had become a vocal critic of the way in which, under the Bush and Obama Administrations, the legislation embodied in the Patriot Act had been used to justify the broad NSA spying powers brought to light by Edward Snowden in 2013 and other whistleblowers before him. In an interview with Andrea Peterson of *The Washington Post* in October 2013, Sensenbrenner spoke of the need to restrict the expanded scope of Section 215 of the Patriot Act, to bring it back to its original intent. This intent, he pointed out, was that once the Justice Department identified a non-U.S. person who was part of a terrorist organisation, it could apply for a FISA order in order to ascertain who that person was in contact with, and thus 'be able to spread that spider web to see who was involved in a plot that might target people either domestically or internationally.'[188]

Sensenbrenner recognised that some matters coming before the FISA Court needed to be classified. Speaking in the context of what had been learned about the illegal practices of both the FISA Court and the NSA, he declared that 'if the FISA Court changes policy or attempts to reinterpret the law, we require the publication of that so it is not a secret decision when basically the FISA Court allows the NSA to shift gears.'[189] He also recognised the need for a public advocate with the authority to appeal a decision of the FISA Court in cases where the advocate feels that this decision 'does not comport with the law or comport with policies.' [190] Finally, Sensenbrenner felt able to assert that if Congress had known the nature of the privacy-invasive programmes the Patriot Act would eventually be used by the NSA to facilitate, and justify, the Act would never have been passed, and he would not have supported it. His verdict

[188] Andrea Peterson, 'Patriot Act Author: 'There has been a failure of oversight' *The Washington Post* October 11, 2013.
[189] ibid.
[190] ibid.

on post-9/11 surveillance was that what the NSA had done, with the connivance of the Bush and Obama Administrations, represented a betrayal of civil liberties. The Patriot Act, he claimed, had been devised to prevent the very abuses perpetrated in its name during the Bush and Obama Presidencies.[191]

At a press conference on August 9, 2013, Obama announced new measures designed to enhance transparency and reform the Foreign Intelligence Surveillance Court. The measures Obama had in mind focused on reforming Section 215 of the Patriot Act and Section 702 of the FISA Amendments Act, under which the NSA surveillance programmes are considered lawful. The most significant reform was to relate to modifications of the Foreign Intelligence Surveillance Court, (the FISC), the problem with which was that it authorised surveillance on foot of highly classified opinions. Obama came up with a specific proposal to deal with the objection that the FISC enables the security apparatus to procure legislation which gives priority to its own interests over individual rights, excluding its antagonists (civil liberties and privacy advocates, for example) from judicial processes and exempt from public scrutiny. In response to this deficiency, Obama declared that he wanted to increase public confidence in the FISC by including a special advocate in its proceedings, the role of this advocate being to challenge government lawyers, who, on existing arrangements, had attained surveillance powers via the Court without being challenged before the judges. The new advocate envisaged by Obama would defend the cause of privacy and civil liberties before the Court. Critics of these 'reform' proposals pointed out that the new panel of outside experts that would be set up under these proposals to 'review the government's surveillance efforts, in terms of both privacy rights and impact on foreign policy' would be under the Office of the Director of National Intelligence, and could therefore not be seen as either independent or impartial. Furthermore, the proceedings of this panel would be closed to the public, and its membership would comprise officials sympathetic to the intelligence community, the President, or both.[192]

[191] ibid.
[192] Aiden Warren and Alexander Dirksen, Augmenting State Secrets: Obama's Information War' 9(1) (2014) *Yale Journal of International Affairs* 68, 76.

More credible and far-reaching proposals came from Congress, the most radical of these being embodied in the USA Freedom Act, a measure introduced by Senator Leahy and Congressman Sensenbrenner in 2013 and passed in May 2014 by the House of Representatives. This envisaged the creation of an Office of Special Advocate within the judicial branch. In contrast with the kind of Advocate envisaged by Obama, this one would be selected by the Chief Justice of the United States from a list of candidates proposed by the independent Privacy and Civil Liberties Oversight board (PCLOB). The panel of candidates from whom the Special Advocate would be chosen would be people whom the PCLOB believe would be 'zealous and effective advocates in defence of civil liberties.'[193] The Leahy-Sensenbrenner measure was modified as a result of hard-fought compromises between the White House, the Department of Justice, the Intelligence Community and key Congressional leaders. A key change from the original measure was that in the new version, the Special Advocate would be chosen from a pool of five outside lawyers appointed by the FISC. Even this compromise, however, failed to be enacted and the Leahy-Sensenbrenner measure, and the prospects for FISA reform were killed in November 2014 in the 113th Congress.[194]

8.0 The Snowden Revelations

Up to the summer of 2013, successive reports on NSA surveillance activities, based on information provided by whistleblowers to journalists, had enhanced public awareness that some people within the United States and larger numbers abroad, were subject to warrantless surveillance by that Agency. There were also indications that the government might be misusing the information gathered as a result of this surveillance, and that NSA surveillance programmes had been in place even before the 9/11 attacks. Following the initial public disclosure of the NSA programme by the *New York Times* on December 16, 2005, a pattern began to emerge in subsequent media reporting, inspired by leaks from within the U.S. surveillance system, which indicated that the dimensions of NSA programmes were much larger than were originally disclosed. For example, in March 2012, James Bamford published an article in Wired Magazine about the construction of a massive NSA data-storage facility

[193] Stephen I. Vladeck, 'The Case for a FISA 'Special Advocate,' *Texas A and M Law Review* (2015) (forthcoming) 1 at 7 <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2546388> accessed 27 April 2015.
[194] ibid, 13-14. For details of the subsequent enactment of the Freedom Act, Section 9.

in Bluffdale, Utah, expected to house a '1-million-square-foot data storehouse,' capable of storing the digital equivalent of 500 quintillion [in numerical form, a five followed by twenty zeros] pages of text.[195] However, it was not until the incremental publication of leaks from Edward Snowden in June 2013 that the full extent of the privacy-invasive activities of U.S. and other security services was opened to public scrutiny by a source whose credibility could not be called into question. Snowden, a security analyst, computer expert and former NSA contractor, had, while working for the Agency, been collecting and copying masses of classified documents containing details of digital surveillance programmes operated by his employers. He gradually released copies of these documents to media organisations. The primary publication was featured in three newspapers: *The Guardian*, *The Washington Post* and *Der Spiegel*. They were followed by *The Guardian* (U.S. edition), *The New York Times* in conjunction with *Pro Publica* after the UK government insisted on destroying the UK *Guardian's* copy of the Snowden material held in its London offices under the supervision of G.C.H.Q.[196]

The documents leaked by Snowden revealed, in unprecedented detail, information about the surveillance capacities and worldwide reach of the NSA and the equivalent British spying agency, General Communications Headquarters (GCHQ). This material was analysed, with Snowden's collaboration, before being published *in extenso* in the media to which Snowden had entrusted it, and subsequently in other media worldwide. The consequence was the public disclosure of what Snowden called 'the largest programme of suspicionless surveillance in human history.'[197] Snowden's first revelation, published in the U.K. edition of *The Guardian* on June 6, 2013, was that the NSA, on foot of an order from the Foreign Intelligence Surveillance Court (FISC) had ordered the telecommunications giant, Verizon, to hand over metadata (the data about data: for example, the IP addresses, the identity of the contact, the location of calls or messages, the duration of the content from

[195] James Bamford, 'The NSA Is Building The Country's Biggest Spy Centre (Watch what you say)' *Wired Magazine* March 15, 2012 <http://www.wired.com/2012/03/ff_nsadatacenter/> accessed 28 April 2015.
[196] Luke Harding, 'Footage released of Guardian editors destroying Snowden hard drives' *The Guardian* 31 January 2014.
[197] *The Guardian* 22 June, 2013.

millions of American telephone calls) to the FBI and the NSA.[198] At the same time, Verizon was forbidden to disclose to its subscribers either the order from FISC or the demand for customer records.

On June 7, 2013, both the *Washington Post* and *The Guardian* gave details of a file provided by Snowden revealing collaboration between the NSA and giant internet corporations under a secret programme called PRISM. This programme gave the NSA direct access to the servers of some of the world's biggest technology companies, including Apple, Facebook, Google, Microsoft, Skype, Yahoo and YouTube.[199] In the United Kingdom, the Tempora programme was another dragnet which gave similar access to the GCHQ, the U.K. partner of the NSA in the 'Five Eyes,' the other participants being Canada, Australia and New Zealand.

Snowden's PRISM documents reveal a number of surveillance programmes, codenamed Upstream, XKeyscore and Bullrun. As part of the Upstream data collection programme, data are copied from both public and private networks to the NSA from international fibre-optic cables at landing points, and from central exchanges which switch Internet traffic between the major carriers, through agreements negotiated with, or legal orders served on, the operating companies. Upstream may also involve the interception of the undersea cables by U.S. submarines specially equipped for the purpose. The XKeyscore system was described in slides published by *The Guardian* on July 31, 2013. XKeyscore is a top-secret NSA programme that allows analysts to search without prior authorisation through vast databases, online chats and the browsing histories of millions of individuals. Snowden was able to cite evidence from NSA training manuals for the XKeyscore programme, that the Agency regards it as its 'widest-reaching system for developing intelligence from the internet.'[200] These training manuals outline in detail how analysts can use it to mine enormous agency databases by filling in a simple on-screen form giving only a broad justification for the search. The request is not revealed to a

[198] Glenn Greenwald, 'NSA Collecting phone records of millions of Verizon Callers daily.' *The Guardian* June 6, 2013.
[199] Barton Gellman and Laura Poitras, 'U.S., British intelligence mining data from nine U.S. internet companies in broad secret programme' *Washington Post* June 6, 2013.
[200] Glenn Greenwald, 'XKeyscore: NSA toll collects 'nearly everything a user does on the internet,' *The Guardian* 31 July, 2013.

court or any NSA personnel before it is processed. Analysts can also use XKeyscore and other NSA systems to obtain ongoing 'real time' interception of an individual's internet activity. A primary purpose of XKeyscore is to allow analysts to search the metadata as well as the content of emails and other internet activity, such as browser history, even when there is no known email account associated with the individual being targeted. Analysts can also search by name, telephone number, IP address, keywords, as well as the language in which the internet activity was conducted or the type of browser used. By way of justification for the use of this privacy-invasive programme, NSA documents assert that by 2008, 300 terrorists had been captured, using intelligence from XKeyscore.[201]

The veracity of such claims was subsequently called into question by privacy advocates. Soon after the Snowden revelations, General Keith Alexander, former head of the NSA, claimed that the Agency's surveillance programmes had prevented 'fifty-four terrorist-related activities,' and that 'most of these were terrorist plots,' thirteen of which involved the United States. Credit for foiling these plots, he continued, was partly due to the metadata programme, intended to 'find the terrorist that walks among us.'[202] At a Senate Judiciary Committee hearing in October 2013, Senator Patrick Leahy called the fifty-four plots statistic 'plainly wrong,' claiming that 'these weren't all plots, and they weren't all thwarted.' [203] In support of this, he cited a statement from Alexander's deputy that 'there's only one example of a case where, but for the use of Section 215 bulk phone-records collection, terrorist activity was stopped.' [204] However, President Obama persisted in canvassing the benefits of the metadata programme. In June 2014, at a press conference with the German Chancellor Angela Merkel, he professed to know 'of at least fifty threats that have been averted because of this information. Lives have been saved.' [205]

Under United States law, the NSA is required to obtain a FISA warrant only if the target of their service is a US citizen, but no such warrant is required for the

[201] ibid.
[202] Matthias Schwartz, 'The Whole Haystack. The NSA claims it needs access to all our phone records. But is that the best way to catch a terrorist?' *New Yorker* 26 January, 2015.
[203] ibid.
[204] ibid.
[205] ibid.

interception of the communications of Americans with foreign targets. XKeyscore provides the technological tools if not the legal authority for targeting even U.S. persons for extensive electronic surveillance without a warrant, provided that some identifying information, such as their email or IP address, is known to the analyst. In a video interview, published in *The Guardian* on June 10, 2013, Snowden explained how such a process can be implemented. 'I, sitting at my desk,' he remarked, could 'wiretap anyone, from you or your accountant, to a federal judge or even the president,' if I had a personal email.'[206] A third NSA surveillance programme, codenamed Bullrun, named after a battle in the American Civil War, was designed to facilitate what *The Guardian* described as 'an aggressive multi-pronged effort to break into widely-used encryption technologies.'[207] Bullrun has its counterpart in the British GCHQ cryptographic encryption programme codenamed EDGEHILL, named after a famous battle in the English Civil War of the mid-seventeenth century.[208]

The international, even global, dimensions of the Snowden revelations had profound implications for the privacy rights, not alone of U.S. and U.K. citizens, but of people far beyond the borders of the U.S.A. or the U.K. In the U.S., the breaches of privacy rights disclosed in Snowden's material provoked public controversy and led to constitutional challenges in federal courts.[209] European concerns receive detailed consideration in a report drawn up by a group of privacy experts for the European parliament in 2013, in the immediate aftermath of the Snowden revelations.[210] NSA surveillance programmes and related legislation and the implications of those for EU citizens and other non-U.S. citizens were the principal concerns of the report. Among the key findings were the following:

[206] Glenn Greenwald, 'XKeyscore: NSA tool collects 'nearly everything a user does in the internet' *The Guardian* July 31, 2013.
[207] 'Secret Documents Reveal NSA Campaign Against Encryption' *New York Times* 5 September, 2013 and James Ball, Julian Border and Glenn Greenwald, 'Revealed: how US and UK spy agencies defeat internet privacy and security.' *The Guardian* 6 September, 2013.
[208] The Bullrun and Edgehill programmes are dealt with in Section 8.0.
[209] For example, see 'Obama Administration drowning in lawsuits filed over NSA surveillance' RT.COM July 16, 2013 <http://rt.com/usa/snowden-leaks-surveillance-suits-174/> accessed 24 May 2015.
[210] Caspar Bowden, 'The US surveillance programmes and their impact on EU citizens' fundamental rights.' *European Parliament* Directorate-General For Internal Policies (2013).

1. The complexity of U.S. legislation pertaining to foreign intelligence information and its interpretation by secret Courts and executive legal memoranda has led to unlawful practices affecting both U.S. citizens and non-U.S. Citizens.

2. The consequences of this legal uncertainty, and lack of Fourth Amendment protection for non-U.S. citizens, means that no privacy rights for non-Americans are recognised by the U.S. authorities under FISA.

3. A review of the mechanisms that have been put in place in the EU to protect EU citizens' rights in relation to data exported, shows that these mechanisms actually function as loopholes.[211]

The Report pointed out that the greatest legislative controversy in the United States was not relating to PRISM, but to the indiscriminate blanket collection of all telephone metadata (call details records) which appears to exceed the terms of the Patriot Statute. Under those terms, data could be acquired under Section 215 in the first place only if it meets the requirement that it must be 'relevant' to an authorised investigation. A serious problem was created, however, when the Patriot Act was amended in 2006 to include the 'relevant standard,' with the intention of limiting the collection of data, as claimed by the chief architect of the Patriot Act, Representative Sensenbrenner.[212] This intention was seemingly interpreted by the government and NSA to mean its opposite: a justification for massive data collection. This questionable paradoxical rationale behind this massive programme of data collection involving an entire database was summed up in the Report by the citation of a comment made by a privacy advocate: 'they (the NSA) were conducting suspicionless searches to obtain the suspicion the FISA Court required to conduct searches.'[213] The Report underlined the mammoth nature of the U.S. surveillance programme since 9/11 by quoting published budget statistics

[211] ibid, at 16.
[212] Audie Cornish, 'Patriot Act Architect Critizises NSA's Data Collection' *NPR* August 20, 2013. <http://www.npr.org/templates/story/story.php?storyId=213902177> accessed 30 April 2015.
[213] Caspar Bowden, 'The US surveillance programmes and their impact on EU citizens' fundamental rights.' *European Parliament* Directorate-General For Internal Policies (2013) 1, 18.

relating to this programme.[214] These statistics revealed that the secret ('black') budget of the United States Intelligence Community amounted to 50 billion dollars per annum, and that the U.S. had spent 500 billion on secret intelligence since 9/11. The NSA budget was about 10 billion dollars per annum, while that of the CIA had grown to 15 billion dollars per annum.[215]

A further significant concern expressed in the Report is that while the FISA definition of 'foreign intelligence information' has been amended several times, it has always included two limbs which seem to those who wrote the Report, almost unlimited in scope. When the terms of the definition are unwound, foreign intelligence information includes:

> [I]nformation with respect to a foreign-based political organization **or** foreign territory that **relates** to, and if concerning a United States person is **necessary** to the conduct of the foreign affairs of the United States. [emphasis added] [216]

Bowden comments that this definition, 'is of such generality that from the perspective of a non-American it appears [that] any data of assistance to US foreign policy is eligible, including expressly political surveillance over ordinary lawful democratic activities'.[217] A further point bearing on the existence of two different régimes of data processing and protection: one for U.S. citizens and residents, another without any protection whatsoever for non-U.S. citizens and residents. While the Fourth Amendment offers a degree of privacy protection to U.S. citizens, it does not apply to non-U.S. persons outside the U.S. General Hayden, the former NSA Director, made this clear in June 2013 when he observed that 'the Fourth Amendment……. is not an international treaty' and that the U.S. enjoys a 'home field advantage' of

[214] Barton Gellman and Greg Miller, 'Black budget summary details U.S. spy network's successes, failures and objectives' *The Washington Post* 29 August, 2013.
[215] Caspar Bowden, 'The US surveillance programmes and their impact on EU citizens' fundamental rights.' *European Parliament* Directorate-General For Internal Policies (2013) 1, 19.
[216] 50 USC, Section 1801 (e) 2 (B). cited in Bowden, Report, 19.
[217] Caspar Bowden, 'The US surveillance programmes and their impact on EU citizens' fundamental rights.' *European Parliament* Directorate-General For Internal Policies (2013) 19.

untrammelled access to foreign communications routed via U.S. territory, or foreign data stored there.[218]

Another aspect of U.S. surveillance law dealt with in the Report concerned cloud computing risks for non-U.S. persons. Cloud computing may be defined as the distributed processing of data on remotely located computers accessed through the internet. From 2007, the benefits of cloud computing to business, governments and policy-makers were widely canvassed by Internet industry marketers, beginning with Google and followed by Microsoft and others. This marketing campaign made cloud computing a new software business sector. When the FISA Amendments Act was introduced in 2008, it made provision for the terms on which surveillance agencies could access data on 'remote computing services.'[219] One of the findings of the report was that 'the accelerating and already widespread use of cloud computing further undermines data protection for EU citizens…'.[220] The reason for this concern was that cloud computing 'dramatically widened' the scope of law enforcement access to stored communications.[221] Furthermore, there is the problem that cloud providers cannot fulfil any of the privacy principles on which the Safe Harbour Agreement is founded.[222] This problem was never satisfactorily resolved by the European Commission before the Safe Harbour Agreement was hastily concluded over the objections of European Data Protection Authorities. Consequently, many U.S. cloud providers advertise Safe Harbour Certification with insupportable claims that this legalises transfers of EU data into U.S. clouds.[223]

---

[218] CBS News, 30 June, 2013. Cited in Bowden, Report, 20, fn 47.
[219] Caspar Bowden, 'The US surveillance programmes and their impact on EU citizens' fundamental rights.' *European Parliament* Directorate-General For Internal Policies (2013) 21.
[220] ibid, 5.
[221] ibid, 21.
[222] In an effort to avoid an interruption of data transfers between the European Union and the United States and to develop a congenial environment for e-commerce, the U.S. Department of Commerce proposed a 'safe harbour' agreement designed to reconcile the divergent approaches to privacy taken in the U.S. and the EU. The U.S. Department of Commerce developed a set of principles to provide a safe harbour from Article 25 of the EU Privacy Directive, which prohibits data transfers to non-member states that do not satisfy the EU standard for adequate privacy protection. The EU Commission approved the Safe Harbour principles on 27 July 2000, and the Safe Harbour Agreement took effect on 1 November 2000. These principles represent an integration of the EU Directive's regulations for the collection and processing of personal data with the self-regulatory principles favoured by the U.S.
[223] ibid, 21-22.

9.0 Significance of the Snowden Revelations

A number of conclusions can be drawn from the revelations of Edward Snowden and others relating to the surveillance activities of the NSA and its closest European collaborator, the U.K. intelligence agency, G.C.H.Q. It is now clear, and has been since the first of Snowden's revelations was published in June 2013,[224] that the U.S. authorities are accessing and processing the personal data of U.S. and EU citizens on an unprecedented scale, and that U.S. and U.K. surveillance practices represent a radical reconfiguration of traditional intelligence gathering. It is now known *how* the U.S. authorities are accessing these data on the scale they are: through the NSA's wiretapping of cable-bound internet traffic by means of the Upstream programme, which was revealed as early as 2006; [225] through direct access to the personal data stored in the servers of U.S.-based private companies such as Microsoft, Yahoo, Google, Apple, Facebook, PalTalk, YouTube, AOL and Skype, achieved through the PRISM programme.[226]

It is also known that the U.S. authorities have access to stored communications, and can perform real-time collection of the data of targeted users through cross-database search programmes such as XKEYSCORE.[227] Other U.S. electronic surveillance programmes include BOUNDLESS INFORMANT, a data analysis and visualisation tool used by the NSA to obtain an overview of worldwide data collection activities by means of counting metadata,[228] BULLRUN, a highly classified decryption programme, whose GCHQ counterpart is codenamed EDGEHILL,[229] MARINA, an NSA database which harvests and stores intercepted internet metadata for up to a year,[230] and STELLAR WIND, the codename for information collected under the U.S.

[224] Glenn Greenwald, 'NSA Collecting Phone Records of Millions of Verizon Customers Daily' *The Guardian* 5 June 2013.
[225] Leslie Cauley, 'NSA has massive database of Americans' phone calls' (10 May, 2006) USATODAY <http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm> accessed 29 April 2015.
[226] Barton Gellman and Laura Poitras, 'U.S., British intelligence mining data from nine U.S. Internet companies in broad secret programme' *The Washington Post* 7 June 2013.
[227] Glenn Greenwald, 'NSA tool collects 'nearly everything a user does on the internet' *The Guardian* 30 July 2013.
[228] Glenn Greenwald and Ewen MacAskill, 'Boundless Informant: the NSA's secret tool to track global surveillance data' *The Guardian* June 8 2013.
[229] Nicole Perlroth, Jeff Larson and Scott Shane, 'NSA Able to Foil Basic Safeguards of Privacy on Web' *The New York Times* 5 September 2013.
[230] James Ball, 'NSA stores metadata of millions of web users for up to a year, secret files show' *The Guardian* 30 September 2013.

President's Surveillance Programme (PSP).[231] The expansion of cloud computing, involving the processing of data on remotely located computers accessed through the internet, has increasingly compromised the data protection rights of citizens on both sides of the Atlantic.

The massive scope of the surveillance operations of the British GCHQ, whose collaboration with the NSA involves interpretation of data under a programme code-named TEMPORA, marks a further enlargement of the NSA's surveillance capacities. It is instructive to note that the chairman of the House of Commons Intelligence and Security Committee (ISC) Sir Malcolm Rifkind, though acknowledging his awareness of GCHQ's broad surveillance capabilities, professed to be unaware of the existence of TEMPORA prior to the Snowden revelations.[232] It now appears that these capacities are being further augmented by the collaboration of EU States other than the UK with the NSA. A paper published by the Centre for European Policy Studies (CEPS) in November 2013, examines evidence that three EU Member States, Sweden, France and Germany may be running or developing their own large-scale internet interception programmes and collaborating with the NSA and GCHQ in the exchange of data.[233]

The exposure of PRISM and other NSA programmes and the relationship of these to other intelligence services and private companies in the U.S. demonstrates the limitations of judicial power over intelligence activities, as well as the difficulty of implementing Congressional oversight of these activities. This is especially so in a political system which makes it possible for the President to invoke plenary powers of dubious Constitutional validity as a basis for ordering the NSA to monitor data to or from domestic parties in the United States without a warrant, or to give secret orders to the NSA to conduct surveillance as George W. Bush did, and when these actions were disclosed, to claim that he had the constitutional authority to disregard the Fourth

[231] Michael Isikoff, 'The Whistleblower Who Exposed Warrantless Wiretaps' (13 December, 2008) *Newsweek* <http://www.newsweek.com/whistleblower-who-exposed-warrantless-wiretaps-82805> accessed 28 April 2015.
[232] Luke Harding, *The Snowden Files* (Random House, 2014) 314.
[233] Didier Bigo, Sergio Carrera, Nicholas Hernanz, Julien Jeandesboz, Joanna Parkin, Francesco Radazzi and Amanda Scherrer, 'Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law; CEPS Paper, in *Liberty and Security in Europe* 61, November 2013.

Amendment and laws enacted by Congress, and to impose his own rules in order to facilitate secret large-scale data surveillance.[234]

The same system that permits violations of statutory law in the pursuit of secret surveillance programmes involving the wholesale violation of the privacy of U.S. and EU citizens also lacks credible oversight systems, the most egregious example being the secret FISA Court (FISC), whose *de facto* function was to rubber-stamp in routine fashion NSA requests for warrants to conduct surveillance. A further dubious feature of FISC was its exclusion of any privacy advocate from its decision-making process. Even more significant, from the point of view of privacy rights, was the government's coercion of content providers to make Internet traffic and other telecommunications data available to U.S. intelligence and law enforcement agencies. A further inhibition on privacy rights is the collaboration of the British GCHQ and some other European intelligence agencies with the NSA's data surveillance programmes. It now appears that these capacities are being further augmented by the collaboration of EU States other than the UK with the NSA. A paper published by the Centre for European Policy Studies (CEPS) in November 2013, examines evidence that three EU Member States, Sweden, France and Germany may be running or developing their own large-scale internet interception programmes and collaborating with the NSA and GCHQ in the exchange of data.[235]

From 2001, the EU Commission drafted approved model clauses for inclusion in contracts for both Controllers and Processors located outside the EU, intended to guarantee privacy rights for individuals comparable to those they would have if the data remained inside the EU. However, Casper Bowden, in his Report for the European Parliament on the U.S. surveillance programmes and their impact on EU citizens' fundamental rights, drew attention to '[t]he conceptual flaw in this general approach.'[236] This flaw, he pointed out, was 'the

[234] James P. Pfiffner, 'The Contemporary President: Constraining Executive Power. George W. Bush and the Constitution' 38(1) (2007) *Presidential Studies Quarterly* 123, 133.
[235] Didier Bigo, Sergio Carrera, Nicholas Hernanz, Julien Jeandesboz, Joanna Parkin, Francesco Radazzi and Amanda Scherrer, 'Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law; CEPS Paper, in *Liberty and Security in Europe* 61, November 2013. 1.
[236] Caspar Bowden, 'The US surveillance programmes and their impact on EU citizens' fundamental rights.' (2013) *European Parliament* Directorate-General For Internal Policies, 26.

supposition that computer systems can be audited to guarantee the three essential requirements of information security: confidentiality, integrity and availability.'[237] While integrity and availability of data are technically and logically verifiable properties, confidentiality is not. Bowden concluded that it is impossible to know with certainty 'whether either an 'insider' or external unauthorised party had seen or copied data, and even if data are 'encrypted with a mathematically strong cipher, the algorithm implementation may have software defects, or the key many be leaked or stolen secretly.'[238]

Bowden further argues that Snowden's revelations about PRISM 'dramatically illustrate the folly' of the EU privacy protection regime in the face of an adversary such as the NSA trying to breach them, and operating lawfully in its own terms.'[239] Bowden might have added that the NSA is operating, whether lawfully or unlawfully, under orders from the President of the United States. Finally, when EU intelligence agencies engage in interpretation and surveillance of telecommunications data of EU citizens for transmission to their counterparts in the U.S.A., two points made in a study commissioned as a briefing by the European Parliament's Committee on Civil Liberties, Justice and Home affairs are worth bearing in mind. The first is that 'surveillance programmes in EU Member States are incompatible with minimum rule of law standards derived from the EU Charter of Fundamental Rights and the European Convention of Human Rights.'[240] The second point is more pertinent: 'Under European law, the individual has ownership of his data, unlike in the United States where ownership belongs to the company or service that assembled the data. This principle is central to and protected by the EU Charter and the Treaty.[241] Therefore, it can be contended that transnational programmes linking the NSA with a series of European intelligence services and facilitating data exchange, could potentially be considered as a theft of correspondence in addition to constituting illegal access, collection and processing of data, if this had been done without the authorisation and/or knowledge of the national authorities in charge of the management of those electronic data. Only the

[237] ibid.
[238] ibid, 26-7.
[239] ibid, 27.
[240] ibid, 19.
[241] ibid.

latter may authorise derogations of national security with respect to existing bilateral, European and international agreements.'[242]

In 2003, a legal framework for a U.S.-EU Mutual Legal Assistance Agreement (MLAA) was ratified by the EU and the U.S. Congress. This provides for collaboration in criminal investigations and counter-terrorism activities in search of evidence for law-enforcement purposes. This Agreement stipulates the modalities for gathering and exchanging information, and for requesting and providing assistance in obtaining evidence located in one country to assist in criminal investigations or proceedings in another.[243] However, in the briefing paper commissioned by the European Parliament's Committee on Civil Liberties, Justice and Home Affairs, it is pointed out that the available evidence provided by revelations of the activities conducted by the NSA that the U.S. intelligence services and their European Member State partners have not followed the legal rules laid down in the MLAA. Instead, the authors of the briefing paper assert that the partners to this Agreement have bypassed or ignored its terms 'in favour of covert cooperation that goes beyond counter-terrorism and serves a multitude of other purposes.'[244]

10.0 Anglo-American Surveillance Collaboration

Some of these 'other purposes' included U.S. surveillance of the German Chancellor, Angela Merkel, head of the government of one of the most loyal allies of the United States. A leading German newspaper, *Suddeutsche Zeitung*, reported that the surveillance was allegedly conducted by a special collection service run by the NSA and the CIA. Two European heads of Government, Chancellor Merkel and the French Prime Minister, François Hollande, considered this episode sufficiently serious to warrant a joint statement calling for a new transatlantic pact, incorporating a new international code of conduct on intelligence gathering to prevent American intelligence services spying on Europe. The German and French governments were prepared to take the

[242] ibid.

[243] Agreement on Mutual Legal Assistance between the European Union and the United States of America, OJ L 181/34, 19 July 2003.

[244] Didier Bigo, Sergio Carrera, Nicholas Hernanz, Julien Jeandesboz, Joanna Parkin, Francesco Radazzi and Amanda Scherrer, 'Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law' (November 2013) 62 CEPS Paper, in *Liberty and Security in Europe* 19. Caspar Bowden, 'The US surveillance programmes and their impact on EU citizens' fundamental rights.' (2013) *European Parliament* Directorate-General For Internal Policies, 19.

initiative regarding this matter. At the same time, Deutsche Telekom announced that it wanted Germany's communications companies to cooperate in shielding local internet traffic from foreign intelligence services.[245]

The governments of the two countries whose surveillance practices were exposed to adverse comment following the Snowden revelations did all they could to discredit Snowden's claims. Denials from official sources, British and U.S., have tended to be framed in formulaic, ambiguous terms, and fail to take account of the distinction between the letter of the law and the latitude allowed by governments and oversight bodies to intelligence agencies in the interpretation of the law. In 2014, classified documents revealed by Edward Snowden showed that FISA authorised the NSA to 'intercept through U.S. companies not just the communications of its overseas targets'[246] but also permitted the NSA to gather intelligence about the World Bank, the International Monetary Fund, the European Union and the International Atomic Energy Agency. FISC also authorised the NSA to intercept information concerning 193 countries, leaving only four countries exempt from NSA surveillance.[247] On 22 June 2013, *The Guardian* newspaper cited leaked documents it had seen, giving the views of 'some high-ranking officials at GCHQ' on practices at Agency. The impression given by these documents is that the GCHQ has a light oversight régime compared with its U.S. counterparts. Just as the FISC in the United States routinely complies with NSA requests for surveillance warrants, the leaked Snowden documents seen by *The Guardian* give the impression that British oversight bodies take a similarly benevolent view of GCHQ activities. One of GCHQ's senior legal advisors remarked that

> [C]omplaints against [intelligence agencies] undertaken by the interception Commissioner, are conducted under the veil of secrecy. And

[245] Bruno Waterfield, Christophe Hope and Peter Foster, 'EU leaders warn US spying could harm fight against terror' *Daily Telegraph* 25 October 2013.
[246] Ellen Nakashima and Barton Gellman, 'Court Gave NSA broad leeway in surveillance, documents show' *The Washington Post* June 30 2014.
[247] ibid.

> the investigatory powers tribunal, which assesses complaints against the agencies, has so far always found in our favour.[248]

This assertion was challenged by Liberty, Privacy International and other civil liberties groups, who claimed that GCHQ's receipt of private communications intercepted by the NSA through its mass surveillance programmes PRISM and Upstream, was illegal. Lawyers for Liberty and Privacy International argued that receiving information about people in Britain from the NSA sidestepped protections provided by the U.K. legal system. Snowden's PRISM slides indicated that there was a back-door method for content-providers such as Google to give data to the NSA, although a Google executive declared that no such method existed: 'It's all through the front door. They send us court orders. We are obliged by law to follow them.' [249] The question was settled in October 2012 when it transpired that there was a back door. *The Washington Post* revealed that the NSA was secretly tapping data from Yahoo and Google: on British territory, the NSA had hacked into the fibre-optic links that inter-connect Yahoo and Google's own data centres around the world, with British operatives doing the hacking.[250]

The Investigatory Powers Tribunal (IPT) declared on February 6 2015, that '[t]he regime governing the soliciting, receiving, storing and transmitting by U.K. authorities of private communications of individuals located in the U.K., which had been obtained by U.S. authorities……contravened Article 8 of the European Convention on Human Rights.[251] The IPT might also have declared that this regime also contravened the relevant terms of the EU Charter of Fundamental Rights. In November 2014, details of previously unknown internal policies, which GCHQ was forced to reveal during legal challenges to its surveillance practices, in the wake of the Snowden revelations, showed that U.K. intelligence agencies can gain access to unlimited bulk data collected from U.S. cables or through U.S. corporate partnerships without having to obtain a warrant from the UK Secretary of State. This information conflicts

[248] Ewen MacAskill, Julian Borger, Nick Davies, Nick Hopkins and James Ball, 'How GCHQ watches your every move' *The Guardian* 22 June 2013.
[249] Luke Harding, *The Snowden Files* (Random House, 2014) 206.
[250] ibid.
[251] Owen Boycott, 'UK-US surveillance régime was unlawful for seven years' *The Guardian* 6 February 2015.

with reassurances by the U.K. Intelligence Services Committee that a warrant is in place whenever GCHQ seeks information from the U.S.[252]

11.0 U.S. and EU Surveillance Practices in the Context of the International Covenant On Civil and Political Rights

Especially since the Snowden revelations in mid-2013, it is now widely accepted that since shortly after 9/11, and probably earlier, the NSA has been collecting massive quantities of data about U.S. citizens and permanent residents, with the ostensible purpose of forestalling terrorist attacks. The scholarly and media focus has largely been on the compliance, or non-compliance, of the NSA and other U.S. intelligence agencies with the U.S. Constitution, particularly the Fourth Amendment protection of privacy rights and U.S. statutes. More recently, the emphasis has shifted to an appraisal of the surveillance programmes of U.S., British and Continental European intelligence agencies in the context of a wider international legal framework, devised under the auspices of the United Nations, laying down the obligations of member governments to protect and promote the right to privacy. Such a framework, The International Covenant on Civil and Political Rights, has been in place decades before 9/11. This Covenant (the ICCPR) was adopted and opened for signature, ratification and accession by resolution of the United Nations General Assembly in 1966 [253] and entered into force on 23 March, 1976. It was ratified by the U.S.A. on June 8, 1992.[254]

Article 17 of the ICCPR provides that:

> 1. No one shall be subject to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
>
> 2. Everyone has the right to the protection of the law against such interference or attacks.

[252] 'Secret Surveillance Policy Gives U.K. Government Warrantless Access to Bulk NSA Data' *LIBERTIES.EU* <http://www.liberties.eu/en/news/gchq-access-bulk-data> accessed 1 May 2015.
[253] General Assembly Resolution 2200A (xxi), 16. December 1966.
[254] G. Alex Sinha, 'NSA Surveillance Since 9/11 and the Human Right to Privacy' 59 (2013) *Loyola Law Review* 861, 866, fn 13.

In his commentary on the ICCPR, Manfred Nowak observes that

> [D]isregard for personal data and secret surveillance by private security companies led during the drafting of Article 17 to a certain emphasis on the positive obligation of the States to protect privacy against interference and attacks from others.[255]

Nowak also observes that there was little controversy about adopting a general protection for the right to privacy in the ICCPR because of the inclusion of a similar right in the Universal Declaration of Human Rights (UDHR).[256] It is worth noting that Article 8(1) of the European Convention on Human Rights (ECHR) strongly resembles Article 17 of the ICCPR. Article 8 reads as follows:

> 1. Everyone has the right to respect for his private and family life his home and his correspondence.[257]
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[258]

The main distinction between Article 17 of the ICCPR and Article 8 of the ECHR is that the latter includes a list of specific limitations on the right to privacy, the former does not. However, this does not mean that Article 17 excludes the possibility of justified interference with the right to privacy. Instead, the phrasing of Article 17 (1) clearly implies that State interference with the right to privacy can be permissible, but that the two necessary conditions for such interference are lawfulness and non-arbitrariness.[259] The question then arises: are the NSA and U.S. surveillance programmes, and those

[255] Manfred Nowak, *U.N. Convention on Civil and Political Rights CCPR Commentary* (2nd revised edition) (Kehl an Rhein Engel 2005) 379.
[256] ibid, 385.
[257] Article 8 (1) ECHR.
[258] Article 8 (2) ECHR.
[259] Manfred Nowak, *U.N. Convention on Civil and Political Rights CCPR Commentary* (2nd revised edition) (Kehl an Rhein Engel 2005) 520.

of their collaborators abroad, compatible with the provisions of Article 17(1) of the ICCPR? How we answer this question depends on how we define 'arbitrary.' The Human Rights Committee of the United Nations observed that the concept of arbitrariness in Article 17(1) 'is intended to guarantee that even interference provided for by law….should be, in any event, reasonable in the particular circumstances.'[260]

The Human Rights Committee further stated that:

> In order to have the most effective protection of his private life, every individual should have the right to ascertain in an intelligible form, whether, and if so, what personal data [are] stored in automatic data files, and for what purposes. Every individual should also be able to ascertain which public authorities or bodies control their files.[261]

The term 'correspondence' as used in ICCPR, Article 17(1) as understood in a modern context, covers all forms of communication over distance, by telephone, telegram, e-mail and other mechanical or electronic means of communication.[262] In the light of such a definition, Nowak takes the view that under Article 17(2), state parties to the ICCPR have 'a comprehensive obligation' to ensure that 'letters, telegrams, e-mails etc. are actually delivered to the desired recipient and are not inspected by third parties,' which means that 'every withholding, censorship, inspection of, or publication of, private correspondence represents *interference* within the meaning of Article 17.'[263]

In the light of the foregoing observations, and of what Snowden and others have revealed about the surveillance practices of the NSA, it seems clear that the United States, as Sinah puts it, 'is potentially infringing the right to privacy under the ICCPR in three major ways.'[264] This potential infringement involves

---

[260] U.N. Human Rights Committee, General Comment 16. The Right to Respect of Privacy, Family, Home and Correspondence and Protection of Honour and Reputation (Article 17). Section 3, U.N. Doc.HRI/GEN/I Rev. 6 (April 8, 1988). Henceforth cited as General Comment.
[261] General Comment 16.
[262] Manfred Nowak, *U.N. Convention on Civil and Political Rights CCPR Commentary* (2nd revised edition) (Kehl an Rhein Engel 2005) 401.
[263] ibid.
[264] G. Alex Sinah, 'NSA surveillance Since 9/11 And The Human Right To Privacy' 59 (2013) *Loyola Law Review* 861, 917.

the collection or inspection of e-mails; the recording or analysis of telephone calls and the storing or reviewing transactional data. All of these forms of data-gathering or review appear to constitute 'interference' under Article 17(1). Sinah highlights several major reasons for thinking that the NSA programme might have failed, and potentially continues to fail, to meet the lawfulness requirements of Article 17 of the ICCPR. These reasons include: the collection of data beyond the scope intended by the U.S. Government; the extra-legal origins of the NSA programme, which bypassed the governing domestic statute (FISA); the numerous doubts as to the legality of the programme among government officials; the provision of immunity to complicit private parties; the sheer size and scope of the programme and the outsourcing of surveillance about Americans to friendly foreign governments.[265]

In December 2013, the United Nations General Assembly requested a report from the U.N. High Commissioner for Human Rights on government surveillance programmes worldwide, in response to widespread concern prompted by Snowden's revelations over the previous months. The Commission's Report, 'The Right to privacy in the digital age', was published on June 30, 2014, and based on an examination of existing national and international legislation, a number of recent Court judgments, and information from a broad range of sources, including a questionnaire sent to Member States of the United Nations, international and regional organisations, national human rights organisations, non-governmental organisations and private sector businesses.[266] The main points made in the report, taken together, amount to an indictment of the surveillance policies and practices of governments around the world. They also amount to an endorsement of the positions taken by privacy campaigners over many decades. Among the issues raised in the report were the following:

[265] ibid, 927.

[266] United Nations Human Rights Office of the High Commissioner for Human Rights. 'Dangerous practice of digital mass surveillance must be subject to independent checks and balances.' (16 July, 2014). <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=14875> accessed 24 March, 2015.Report of Remarks by U.N. High Commissioner for Human Rights, Navi Pillay at a Press Conference held in Geneva.

1. The proliferation of overt and covert digital surveillance in jurisdictions around the world, with governmental mass surveillance emerging as a dangerous habit rather than an exceptional measure.[267]

2. Reports that governments have threatened to ban the services of telecommunications wireless equipment companies unless given direct access to communications traffic, and required companies systematically to disclose bulk information on customers and employers. There are also reports that authorities in some states routinely record all phone calls and maintain them for analysis.[268]

3. Surveillance practices in the United States and the United Kingdom come in for specific attention in the Report, in the context of revelations in 2013 and 2014 that the NSA and GCHQ have developed technologies in allowing access to much global Internet traffic through the tapping of undersea fibre-optic cables for surveillance purposes.[269]

4. A further concern is the deployment of these privacy-invasive technologies through a trans-national network comprising strategic intelligence relationships between Governments, regulatory control of private companies and commercial contracts.[270]

5. The Report draws attention to the fact that following the concerns of Member States and other stakeholders at the negative impact of these surveillance practices on privacy rights in particular, a resolution (68/167), co-sponsored by 57 Member States was passed by the U.N. General assembly affirming that privacy rights held by people offline must also be protected online, and calling on all Member States to protect the right to privacy in digital communication. The same Resolution called upon all states to review their practices, procedures and legislation related to communications surveillance and collection of data with a view to ensure the full and effective

[267] 'The right to privacy in the digital age.' Report of the Office of the United Nations High Commissioner for Human Rights. United Nations General Assembly (30 June 2014), para 3. Henceforth cited as A/HCR/27/37.
[268] ibid.
[269] ibid, para 4.
[270] ibid.

implementation of their obligations under international human rights law, as outlined in the ICCPR, to date ratified by 167 states.[271]

6. The Report laid special emphasis on a disturbing aspect of U.S. surveillance practices, pointing out that the 'secret rules and secret interpretations - even secret judicial interpretations,' of law associated with the operations of the NSA and FISC, 'do not have the necessary qualities of law,' as these are understood by the ICCPR.[272] Furthermore, 'neither do laws or rules that give the executive authorities, such as security and intelligence services, executive discretion.' Instead, 'the scope and manner of authoritative discretion granted must be indicated (in the law itself, or in binding, published guidelines) with reasonable clarity.' Even a law that is accessible, but does not have foreseeable effects is not adequate. The secret nature of specific surveillance powers brings with it 'a greater risk of arbitrary exercise of discretion,' a hallmark of U.S. surveillance practice since the post-World War Two formation of the NSA.[273]

The Report of the U.N. High Commissioner (the Pillay Report) was followed by that of the Special Rapporteur, Ben Emmerson on 'Promotion and Protection of Human Rights and fundamental freedoms while countering terrorism.'[274] This was transmitted to the U.N. General Assembly on 23 September 2014. This Report examines the use of mass digital surveillance for counter-terrorism purposes, and considers the implications of bulk technology for the right to privacy under Article 17 of the ICCPR. The Emmerson Report concurs with the findings of the Pillay Report, emphasising the obligations of States under Article 17 of the ICCPR '[T]o respect the privacy and security of digital communications,' and the rights of individuals to 'share information and ideas with one another without interference by the State, secure in the knowledge that their communications will reach, and be read by, the intended recipient alone.'[275] Further, the Report argues that measures that interfere with this right 'must be authorised by domestic law that is accessible and precise,

[271] A/HCR/27/37.
[272] ICCPR/C/USA/CO/4, para 22.
[273] A/HRC/27/37, para 29.
[274] 'Report of the Special Rapporteur on the protection and protection of human rights and fundamental freedom' United Nations General Assembly (23 September 2014). Henceforth cited as A/69/397.
[275] A/69/397, para 58.

and that conforms with the Covenant' [the ICCPR].[276] Such conformity would require that such measures 'must also pursue a legitimate aim and meet the needs of security and proportionality.'[277]

Among the key recommendations of the Emmerson Report are that states with bulk access technology, 'which is indiscriminately corrosive of online privacy.' should 'revise and update national legislation to ensure consistency with international human rights law.'[278] In a situation 'where the privacy rights of the entire digital community are at stake,' the Report concludes that 'nothing short of detailed and explicit primary legislation should suffice.' [279] In addition, '[a]ppropriate restrictions should be imposed on the use that can be made of captured data, requiring relevant public authorities to provide a legal basis for the reuse of personal information.'[280] A further recommendation, in the interests of transparency and accountability, is that States should establish 'strong and independent oversight bodies' which are 'adequately resourced and mandated to conduct *ex ante* review, considering applications for authorisation [of surveillance] not only against the requirements of domestic law, but against the necessity and proportionality requirements of the ICCPR.'[281]

12.0 Revelations of Overbroad Interpretation of Section 215 of the Patriot Act and the Response of the Obama Administration

In June 2013, as a result of an unauthorised disclosure to the media by Edward Snowden, it emerged that the U.S.A. Patriot Act, a major component of the pre-emptive surveillance strategy devised by the Bush administration, had been used, or misused since 2006, to facilitate the collection by the NSA of almost all U.S. telephone call detail records and other telephony metadata. The bulk collection of metadata was kept secret from the public until Snowden's 2013 revelation, although known to some members of Congress, who also knew of the statutory interpretation of Section 215 of the Patriot Act which the government was using to justify it. However, since the Section 215 metadata programme was classified, those members of Congress who knew of its existence and of the controversial interpretation by government of Section 215,

[276] ibid, para 30.
[277] ibid, para 61.
[278] ibid, para 60.
[279] ibid.
[280] ibid, paras 59-60.
[281] ibid, para 61.

were prevented from alerting the public to the implications for citizens' privacy of what the NSA was doing.[282]

Schneier remarks that the Patriot Act was never intended to authorise mass surveillance, and that 'strong arguments can be made that the Act's language doesn't allow it.'[283] Schneier further observes that '[t]he idea was that the 'FBI would be able to get information relevant to an authorised [national security] investigation - that is, about a specific subject of investigation - from a wider set of sources that it could previously.'[284]

Schneier's interpretation of what the Patriot Act was *not* intended to do was anticipated by no less an authority that the author of the Act, Representative Jim Sensenbrenner, who introduced it in 2001, and who remarked that twelve years later that the National Security Agency overstepped the bounds [of the Patriot Act] by obtaining a secret order to collect phone log records from millions of Americans, adding that 'seizing phone records of millions of innocent people is excessive and un-American,' and that while he believed that the Patriot Act appropriately balanced national security concerns and civil rights, I have always worried about potential abuses.'[285] The origin of the difference between Section 215 of the Patriot Act as written by Sensenbrenner and understood by him and Section 215 as redacted by the U.S. Department of Justice with the collaboration of the secret FISA Court (FISC) is explained by Schneier. After the Patriot Act was passed in 2001, national security lawyers from the Department of Justice combed through the law for loopholes that might facilitate extended surveillance. Even though the law, as the author explained, was intended to facilitate targeted surveillance, the Department of Justice lawyers declared that it could be stretched to authorise mass surveillance. Even though the Patriot Act empowered the FBI only, the Department of Justice lawyers suggested that the FBI could demand that the information harvested from mass surveillance should be sent to the NSA. The

[282] See Stephanie K. Pell and Christopher Soghoian, 'A Lot More than a Pen Register, and Less Than a Wiretap: what the Stingray teaches us about how Congress should Approach the Reform of Law Enforcement Surveillance Authorities' 16(1) (2014) *Yale Journal of Law and Technology* 134.
[283] Bruce Schneier, *Data and Goliath: The Hidden Battle to Collect Your Data and Control Your World* (W.W Norton, New York and London 2015) 173.
[284] ibid.
[285] 'President Obama's Dragnet' *New York Times* 6 June 2013.

DOJ lawyers argued this case before the secret FISA Court, and because there was no one arguing the opposite position they were able to convince the FISC judge that *everything* was relevant to an investigation.[286] When Sensenbrenner learned that the NSA used the Patriot Act as a legal justification for collecting mass surveillance data on Americans, he remarked: '[i]t's like scooping up the entire ocean to guarantee you catch a fish.'[287]

On June 6, 2013, the British newspaper *The Guardian*, revealed that the NSA had been collecting phone records of millions of Verizon customers. In particular, Verizon was required to hand the metadata of all its customers to the NSA. These metadata include the phone numbers of both callers and recipients, the time and duration of phone calls in addition to the location of the participants at the time of the call. [288] A series of articles published on the same day in *The Guardian* and *The Washington Post* also revealed that the NSA was operating a secret electronic surveillance programme called PRISM. [289] This programme granted the NSA access to Internet data, such as e-mail, chat, videos, photographs and file templates held by leading Internet companies such as Google, Microsoft, Facebook, Skype, Apple and YouTube.[290]

Following concerns raised by civil liberties groups, and a continuous stream of revelations from Edward Snowden, President Obama publicly acknowledged the secret surveillance of telephonic and Internet communications, However, he also tried to make a case for the necessity of the surveillance programme as an element in the defence of national security and the fight against terrorism.[291] In the light of what the public had learned about the provenance of NSA secret surveillance and the implications of this for the privacy of U.S. citizens, President Obama's line of defence was unconvincing. For example, with regard to the NSA's request for Verizon customer data, he assured Americans that 'nobody is listening to your telephone calls,' and maintained that:

---

[286] Bruce Schneier, *Data and Goliath: The Hidden Battle to Collect Your Data and Control Your World* (W.W Norton, New York and London 2015) 173.
[287] Jennifer Valentino-DeVries and Siobhan Gorman 'Secret Court's Redefinition of 'Relevant' Empowered Vast NSA Data-Gathering' *The Wall Street Journal* 8 July 2013.
[288] Glenn Greenwald, 'NSA collecting phone records of millions of Verizon customers daily' *The Guardian* 6 June 2013.
[289] 'NSA slides explain the PRISM data-collection program' *The Washington Post* 6 June 2013.
[290] ibid.
[291] Ewen MacAskill, 'Obama defends "system of checks and balances" around NSA surveillance' *The Guardian* 17 June 2013.

> [W]hat the intelligence community is doing is looking at phone numbers and duration of calls….they are not looking at people's names, and they're not looking at content. But by sifting through this so-called metadata, they may identify potential leads with respect to folks who might engage in terrorism.[292]

Two months later, the Obama Administration issued a White Paper, the purpose of which was to assure the American public that the Government had a sound legal basis for the intelligence-collection programme under which the FBI obtains orders directing certain telecommunications service providers to produce telephony metadata in bulk for analysis by the NSA. In support of the 'sound basis' argument, the secretly redacted Section 215 of the Patriot Act authorised by the Secret FISC Court in 2006 was invoked in the White Paper, in which it was further pointed out that the bulk collection programme was renewed thirty-four times, between 2006 and 2013 by the Secret FISC Court under orders issued by fourteen different FISC judges. The secrecy elements surrounding the 2006 bulk surveillance programme are acknowledged and even emphasised: 'Because aspects of the programme remain classified, there are limits to what can be said publicly about the facts underlying its legal authorisation.'[293] The last comment should not come as a surprise, since for the Administration to disclose all the facts underlying the 'legal authorisation' of the bulk collection of metadata by the FBI and the use of these metadata by the NSA would be to expose the role of the Department of Justice national security lawyers in secretly having a redacted Section 215 of the Patriot Act authorised by FISC, thus fundamentally altering its meaning to the detriment of the data privacy rights of millions of Americans and further tilting the data privacy/national security balance to the detriment of data privacy.

In an earlier statement cited above, President Obama claimed, surprisingly so in the light of information revealed by Edward Snowden, that 'the telephony metadata collection programme is subject to an extensive regime of oversight and internal checks, and is monitored by the Department of Justice (DOJ), the

[292] Statement by the President, Fairmont Hotel San Jose, California. The White House Office of the Press Secretary June 7, 2013 <https://www.whitehouse.gov/the-press-office/2013/06/07/statement-president> accessed 1 November 2016.
[293] Administration White Paper. Bulk Collection Of Telephony Metadata Under Section 215 Of The USA Patriot Act (August 9, 2013), 1.

FISC, and Congress, as well as by the Intelligence Community.'[294] This statement, that NSA surveillance programmes are reviewed and approved by all three branches of government is 'deeply misleading,' as Schneier points out, since:

> Before Snowden, the full range of government surveillance activity was known by only a few members of the Executive branch, disclosed to a few members of the legislative branch (Congress) and approved by a single judge of the FISA Court (FISC) - a Court that rejected a mere 11 out of 34,000 warrant requests between its formation in 1979 and 2013.[295]

The various attempts by the Bush and Obama Administrations and their apologists to justify secret bulk surveillance[296] were met with growing media scepticism and cynicism, especially post-Snowden. The response of *The New York Times* to a statement made by President Obama on 7 June 2013 is similar to many others:

> Within hours of the disclosure that federal authorities routinely collect data on phone calls Americans make, regardless of whether they have any bearing on a counterterrorism investigation, the Obama administration issued the same platitude it has offered every time President Obama has been caught overreaching in the use of his powers: Terrorists are a real menace and you should just trust us to deal with them because we have internal mechanisms (that we are not going to tell you about) to make sure we do not violate your rights.[297]

The same newspaper adverted to disclosures in two newspapers: *The Washington Post* and *The Guardian*. Both of these described a process by

[294] Administration White Paper. Bulk Collection Of Telephony Metadata Under Section 215 Of The USA Patriot Act (August 9, 2013) 1, 4-5.
[295] Bruce Schneier, *Data and Goliath: The Hidden Battle to Collect Your Data and Control Your World* (W.W Norton, New York and London 2015) 175-6.
[296] For some of these, see John Yoo, 'The Terrorist Surveillance Programme and the Constitution,' 14(3) (2007) *George Mason Law Review* 565-604, 566; John Yoo, War by Other Means. An Insider's Account Of The War On Terror (Atlantic Monthly Press, 2006); John E. Owens, *Presidential Power and Congressional Acquiescence in the "War" on Terrorism*: A New Constitutional Equilibrium' 34(2) (2006) *Politics and Policy* 258-303.
[297] 'President Obama's Dragnet' *New York Times* 6 June 2013.

which the NSA was able to capture Internet communications directly from the servers of nine of the leading American content providers. *The Guardian* revealed that the FBI and the NSA used The Patriot Act to obtain a secret warrant to compel Verizon's business services division to turn over metadata on every single call that went through its system.[298] What this suggested was that without any individual suspicion of wrongdoing 'the government is allowed to know whom Americans are calling every time they make a phone call, for how long they talk and from where.[299] The bulk metadata thus acquired can reveal a considerable amount of information about an individual. The overboard nature of the surveillance presided over by the Executive branch of government represents a fundamental shift in the data privacy/national security balance.[300]

The assurances offered to Americans by Obama that nobody was listening to their telephone calls, that the intelligence community was merely looking at phone numbers and the duration of calls and were not looking at the content of these calls were beside the point. The bulk metadata he was acknowledging were acquired by the NSA and could reveal a considerable amount of information about the private life of an individual. For example, the sophisticated technology at the disposal of the intelligence community made it possible to link known phone numbers to the individuals whose numbers these were. The overbroad secret surveillance capacities involved in the pre-emptive surveillance strategy devised by the Bush Administration, and endorsed by its successor, represented a fundamental change in the data privacy/national security balance in favour of the latter.

The Obama Administration White Paper on the bulk Collection of Metadata, cited above, mentions 'a reasonabless standard' established by the Supreme

[298] ibid.
[299] ibid.
[300] It is noteworthy that the EU Data Retention Directive of 2006, legislated for as a response to terrorism, and which also facilitated the bulk collection and retention of metadata, was declared invalid by the European Court of Justice [the CJEU] on 8 April 2014, mainly because it violated the rights to privacy and data protection and failed to meet the requirements of proportionality.

Court.[301] The argument advanced by the Administration in its White Paper was that even if one were to assume that the collection of metadata involved a search within the meaning of the Fourth Amendment, that search would satisfy the Supreme Court 'reasonableness standard' established 'in its cases including *Maryland v King* authorising the government to conduct large-scale, but minimally intrusive, suspicionless searches.'[302] As has been suggested above, the searches are far from 'minimally intrusive.' The 'reasonableness standard' set by the Supreme Court in *Maryland v King* requires a balancing of 'the promotion of legitimate Governmental interests against the degree to which [the search] intrudes upon an individual's privacy.'[303]

13.0 The Consequentialist Defence of the Terrorist Surveillance Programme (TSP)

When, in December 2005, two *New York Times* journalists revealed the existence of the TSP, which allowed the NSA to intercept phone calls and e-mails travailing in and out of the U.S., academic and political critics claimed that the programme violated FISA, and represented an unconstitutional expansion of Presidential power.[304] The standard Administration response, whether under Bush or Obama, has been that the NSA programme and others like it are fully legal, and that the TSP has produced valuable information allowing the government to prevent terrorist attacks on the United States. In a December 19, 2005 Press Briefing, General Michael Hayden, the leader of the NSA during most of the existence of the TSP programme, asserted that 'this

[301] *Maryland v King*, 133. S. Court. 1958 [2013]. King was arrested on a variety of assault charges. Prior to King's trial, a sample of King's DNA was obtained from him to ascertain whether he had been engaged in other criminal activities. THE DNA sample taken from King corresponded to a DNA sample relating to an unsolved rape case. Based on the matching DNA samples, King was charged with the rape and was tried. He was convicted by the trial Court on the basis of the matching DNA samples, but appealed the verdict, which was overturned. The appellate Court held that obtaining King's DNA without a warrant violated the Fourth Amendment which prohibits unreasonable searches. The State of Maryland appealed the verdict to the U.S. Supreme Court, which, by a majority verdict overturned the appellate Court's verdict. The Supreme Court held that the taking of a DNA sample by the police on the basis of probable cause, was akin to the taking of fingerprints and photographs and constituted a reasonable and acceptable police procedure. Accordingly, the Supreme Court held that the taking of King's DNA sample without a warrant did not violate the Fourth Amendment.

[302] Administration White Paper. Bulk Collection Of Telephony Metadata Under Section 215 Of The USA Patriot Act (August 9, 2013) 1, 21.

[303] ibid.

[304] For example, Senator Russell Feingold introduced a motion in the Senate to censure President Bush for approving an illegal programme 'to spy on American soil.' Statement on the President's Warrantless Wiretapping Programme (7 February 2006). The Conservative columnist George Will argued that Presidential powers 'do not include deciding that a law - DISA for example - is somehow exempted from the Presidential duty to 'take care that the laws be faithfully executed,' *The Washington Post* (February 16, 2006).

programme has been successful in detecting and preventing attacks inside the United States,' and when pressed to say whether it had succeeded where no other method would have, he answered 'I can say unequivocally, all right, that we have got information through this programme that would not otherwise have been available.' At the same Press Briefing, the Attorney General, Alberto Gonzales informed the press that the NSA Programme was perhaps the most classified programme in the U.S. Government, and that it had prevented attacks within the United States.[305]

On June 5, 2013, after *The Guardian* published the first of a series of articles detailing Edward Snowden's revelations of the true nature and extent of the NSA's surveillance programmes, the Obama Administration faced an uproar over the threat that this and similar programmes posed to privacy. The same line of defence of the utility of the NSA surveillance programme that the Bush Administration had offered was maintained by the Obama Administration. Two weeks after the first revelations by Snowden were published, President Obama defended the NSA surveillance programmes during a visit to Berlin, where, he asserted that: 'We know of at least 50 threats that have been averted because of this information, not just in the United States, but in some cases, threats here in Germany.'[306]

General Keith Alexander, the Director of the NSA, testified before Congress that the information gathered from these [NSA] programmes provided the U.S. government with critical leads to help prevent over 50 potential terrorist events in more than 20 countries around the world, while the Chairman of the House Permanent Select Committee on Intelligence said on the House floor in July 2013 that '54 times [the NSA programmes] stopped and thwarted terrorist attacks both here and in Europe - saving real lives.'[307]

---

[305] Press Briefing by Attorney General Gonzalez and Michael Hayden, Principal Deputy Director for National Intelligence (December 19, 2005) <https://georgewbush-whitehouse.archives.gov/news/releases/2005/12/20051219-1.html> accessed 2 November 2016.

[306] Jackie Colmes, 'Obama says surveillance helped Case in Germany' *The New York Times* 19 June, 2013.

[307] Bailey Cahall, Peter Bergen, David Sterman and Emily Schneider, 'International Security Policy Papers: Do NSA's Bulk Surveillance Programs Stop Terrorists? *International Security* (January 13, 2014) <https://www.newamerica.org/international-security/policy-papers/do-nsas-bulk-surveillance-programs-stop-terrorists/> accessed 10 November 2016.

The authors of the White Paper defended the mass surveillance of metadata by government agencies which did not include the content of any conversations, as constituting a minimal interference with the privacy interest component of the legitimate balancing exercise. Dealing with the other side of the balance, the government's interests in security protection, the authors emphasised 'an exceptionally strong public interest in the prevention of terrorist attacks,' claiming that 'telephony metadata analysis can be an important part of achieving that objective,' that objective being 'the forward-looking prevention of the loss of life, including potentially on a catastrophic scale.'[308] Reduced to its essentials, the argument advanced in the White Paper was that the secret NSA mass surveillance of metadata under the Department of Justice revised version of Section 215 of the Patriot Act was acceptable in the context of a legitimate data privacy/national security balancing paradigm, 'given the exceedingly important objective' of preventing terrorist attacks, and the 'minimal, if any Fourth Amendment intrusion that the [NSA] programme entails.'[309]

The two main elements of this argument - that mass surveillance of metadata represents a minimal, if any, interference with privacy rights, and that the NSA programme plays an important part in preventing terrorist attacks - have become increasingly untenable. As suggested above, the mass collection and retention of metadata can reveal a considerable amount of information about a person's private life, and its implications for privacy are by no means minimal. The numerous attempts to justify surveillance programmes such as that operated by the NSA by stressing their significant role in preventing terrorism have been shown in recent times to lack credibility.

A series of reviews of the government's claims about the role that NSA bulk surveillance of phone and e-mail communication records has had in keeping the U.S. safe from terrorist attacks have shown that these claims are overblown and even misleading. One in-depth analysis of 225 individuals recruited by al-Qaeda or inspired by its ideology, and charged in the U.S. with an act of terrorism since 9/11:

[308] ibid.
[309] ibid.

> [D]emonstrates, as its authors point out, 'that traditional investigative methods, such as the use of informants, tips from local communities and targeted intelligence operations provided the initial impetus for investigations in the majority of cases, while the contribution of NSA's bulk surveillance in these cases was minimal.[310]

The four investigators who carried out this analysis calculated that the controversial bulk collection of U.S. telephone metadata under Section 215 of the Patriot Act 'appears to have played an identifiable role in initiating, at most, 1.8 per cent of these 225 cases.'[311] The analysis finds that 'surveillance of American phone metadata has had no discernible impact on preventing acts of terrorism and only the most marginal of impacts on preventing terrorist-related activity, such as fundraising for a terrorist group.'[312] The conclusion reached by the authors of this review is that the overall problem for U.S. counterterrorism officials is not that they need vast amounts of information from the bulk surveillance programmes, 'but that they don't sufficiently understand or widely share the information they already possess that was derived from conventional law enforcement techniques.'[313] This was true in the case of the 9/11 hijackers who were known to be in the U.S. before the attacks on New York and Washington.

A former Administration insider who had worked for three Presidents, Clinton, Bush and Obama, as a security official, speaking at a conference organised by RSA, a security industry pioneer specialising in encryption tools, rebutted the persistent claims by government that 55 possible terrorist attacks had been stopped by the NSA metadata programme. The former White House National Security official, Richard Clarke, having reviewed each of the 55 cases, declared that the NSA Section 215 metadata programme 'did not influence the outcome of any of those cases,' insisting that the programme was a waste of time, and unethical as well.'[314] Clarke also acknowledged that 'we [the various

[310] ibid.
[311] ibid.
[312] ibid.
[313] ibid.
[314] Paul Wagenseil, 'NSA Mass Surveillance Useless, Former Bush Official Says,' (24 *Tom's Guide* (26 February, 2014) <www.tomsguide.com/us/rsa-nsa-spy-program-useless,news-18384.html. accessed 21 December 2016.

Administrations under which he worked] were collecting a lot of stuff we shouldn't have been collecting' also pointing out, as security specialists such as Schneier had done, that Section 215 [which was invoked by the government to justify the NSA programme] is only legal if you take the law and stretch it beyond all understanding of the English language.'[315] He also referred to an alleged attempt by the NSA to subvert encryption standards. The RSA company had been accused of co-operating with the NSA to weaken RSA's own commercial security software.[316] Reuters News Agency had reported in December 2013 that the NSA had paid ten million dollars for an encryption tool called Dual Elliptic Curve, with a deliberately engineered flaw, or back-down that allowed the NSA to crack the encryption. In July 2013, *The Guardian*, on the basis of information supplied by Edward Snowden, revealed the existence of another secret NSA programme code-named XKeyscore, 'which allowed analysts to search, with no prior authorisation, through vast databases containing e-mails, online chats and the browsing histories of millions of individuals.' [317]

The proliferation of revelations such as the latter particularly post-2013, indicating the massive breadth and depth of NSA secret surveillance projects, was not accompanied by credible evidence from the government that these projects played a significant part in identifying or thwarting specific terrorist plots. The evidence to hand, such as that outlined above, suggests that the reason there have not been any large-scale terror attacks in the United States since 9/11 is not that they were averted by the NSA or other elements of the intelligence community, but because, 'with the possible exception of one that was foiled by the local police, none were actually planned, and even before Snowden, the NSA wasn't able to provide a single substantial example of its surveillance dragnet preventing any domestic attack at all'.[318] A White House panel concluded in December 2013 that the NSA's bulk collection of

[315] ibid.
[316] ibid.
[317] Glenn Greenwald, 'XKeyscore: NSA tool collects 'nearly everything a user does on the internet.' *The Guardian* 31 July 2013.
[318] Jenna McLaughlin, 'US Mass Surveillance Has No Record of Thwarting Large Terror Attacks Regardless of Snowden Leaks,' (7 November, 2015) *The Intercept*, <https://theintercept.com/2015/11/17/u-s-mass-surveillance-has-no-record-of-thwarting-large-terror-attacks-regardless-of-snowden-leaks/> accessed 1 November 2016.

Americans' telephone information was 'not essential in preventing attacks'.[319] A member of the panel took this one step further, when he told ABC News that there were no examples of the NSA, using this programme, stopping 'any [terror attacks] that might have been really big'.[320]

In December 2013, a special Review Group consisting of an expert panel of Constitutional scholars and former national security officials appointed by President Obama issued a 303-page report asserting that the NSA's surveillance, including but not limited, to its metadata programme, raising serious legal and policy concerns, and proposing forty-six reforms. The Review Group included constitutional law scholars Cass Sustein and Geoffrey Stone; privacy expert Peter Swire; Richard Clarke, the former chief counterterrorism adviser to the National Security Council and Michael Morell, the former Acting Director of the CIA.[321] The Review Group made forty-six recommendations, with four in particular representing what the expert panel considered to be significant recommendations.

These recommendations were, firstly that Section 215 of FISA be amended to authorise the FISC to issue a section 215 Order compelling a third party to disclose private information about private individuals only if it finds that the government has reasonable grounds to believe that the information sought is relevant to an authorised investigation. Such an investigation must be intended to protect against international terrorism or clandestine intelligence activities, and the Section 215 Order must be reasonable in focus, scope and breadth.[322] Secondly, the Review Group was critical of the policy involving the mass retention of the data resulting from mass surveillance. Significant reforms were advocated in relation to surveillance of U.S. persons. The main recommendation here was that Congress should end the storage of bulk metadata and transition to a system where such metadata are held privately for

[319] ibid.
[320] ibid.
[321] Richard A. Clarke, Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein and Peter Swire, 'Liberty And Security In A Changing World' *Report and Recommendations of The President's Review Group On Intelligence and Communications Technologies* (12 December, 2013) <https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf> accessed 28 December 2016.
[322] ibid, at 24.

the government to query when necessary for national security purposes.[323] Thirdly, the Review Group was critical of the policy of harvesting vast amounts of data on a blanket basis. The recommendation here was that any programme involving government collection or storage of such data should be narrowly tailored to serve an important government interest.[324] Fourthly, the review Group recommended that legislation should be enacted to ensure greater transparency attaching to data retention models. Detailed information about retention involved in the metadata programme should be made available on a regular basis to Congress and the American people to the greatest extent possible, consistent with the need to protect classified information.[325]

A second study was issued by the Privacy and Civil Liberties Oversight Board, an independent watchdog entity created by Congress and appointed by the President. This Report dealt with the Section 215 surveillance programme and the FISC. The Board determined in relation to the Section 215 surveillance programme that '[g]iven the limited value this program has demonstrated to date, as outlined above, we find little reason to expect that it is likely to provide significant value, much less essential value, in safeguarding the nation in the future.' [326] The Board proposed a series of reforms aimed at helping to 'bolster public confidence in the operation of the court.'[327] To achieve this aim, the Board postulated the necessity of:

> (1) providing a greater range of views and legal arguments to the FISC as it considers novel and significant issues; (2) facilitating appellate review of such decisions; and (3) providing increased opportunity for the FISC to receive technical assistance and legal input from outside parties.[328]

The Board's assessment of the effectiveness of the NSA metadata programme was based on a review of seven years of NSA amassing comprehensive records

[323] ibid,17.
[324] ibid, recommendation number 4, 25.
[325] ibid, recommendation number 7,122.
[326] David Medine, (Chairman), Rachael Brand, Elisabeth Collins Cook, James Dempsey and Patricia Wald, 'Report on the Telephone Records Program Conducted under Section 215 of the USA Patriot Act and on the Operations of the Foreign Intelligence Surveillance Court' (January 23, 2014) *Privacy and Civil Liberties Oversight Board* 155 <https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf> Accessed 28 December, 2016.
[327] ibid, 182.
[328] ibid.

on every American's phone calls, classified briefings with the NSA and other security officials, access to classified information, and a painstaking analysis of each of the 'success stories' that the government had claimed for NSA surveillance. The assessment concluded that, based on the information provided to it, the Board had not identified a single instance involving a threat to U.S. security in which the metadata programme made a concrete difference to the outcome of a counterterrorism investigation. Furthermore, the Board was not aware of any instance in which the programme directly contributed to the discovery of a previously unknown terrorist plot on the disruption of a terrorist attack. The Board was convinced that in only one instance between 2007 and 2013 the programme arguably contributed to the identification of an unknown terrorist suspect. Even in that case there was reason to believe that the FBI had discovered that suspect without the contribution of the NSA's programme.[329]

In the context of both reports, particular with regard to the findings of the Privacy Board, Cole comments that 'any such assessment necessitates a balancing of the program's costs to our fundamental freedoms against the security benefits it provides. If the program is essential to maintain our way of life, the sacrifices might well be reasonable.'[330]

However, with balancing being in question, let us suppose that the NSA's programme could be shown not to be essential to maintain the American way of life, in the sense that it does not contribute significantly to national security, for example, by detecting terrorist plots or preventing terrorist attacks. This is precisely the conclusion drawn by the President's Privacy and Civil Liberties Board on the basis of a long drawn out programme of comprehensive research. In that case, the sacrifice of privacy could not be considered reasonable.

President Obama accepted two of the recommendations of the Special Review Group's expert panel, namely that the NSA no longer hold the telephone metadata, but that these metadata should be held by private companies, and that the NSA should be permitted to access the data only upon specific court orders

[329] ibid, 11.
[330] David Cole, 'Can Privacy Be Saved?' *The New York Review of Books* (March 6, 2014).

approving specific searches.[331] At the same time, legislation under consideration in Congress also pointed towards shifting retention away from the NSA to private companies.[332] The question then arises: Does the distinction between private company retention of the telephone metadata of citizens really matter? The judgment of the European Court of Justice in *Digital Rights Ireland*[333] throws light on this question. The *Digital Rights Ireland* case dealt with a retention system in which private companies collected the metadata. In that case, the European Court of Justice ruled that it was the retention in itself which constituted an infringement on the right to privacy, irrespective of whether a government agency (like the NSA) or private telephone companies, collected the metadata.[334] The larger and more pressing question arising from the decision of the Court of Justice and the U.S. Government's practice of collecting and storing metadata through its hitherto secret NSA electronic surveillance programme, is whether the collection, retention and storage of metadata that tells so much about a citizen's private life should, in any circumstances, be one of the government's weapons in the fight against terrorism. As Cole puts it, 'the bigger issue is not who holds the data, but the very fact that the government is engaged in the dragnet collection of data on all of us, rather than conducting the more traditional targeted searches that the Constitution has so long required.'[335]

If it is the case that the massive surveillance programme undertaken post-9/11 for the purpose of identifying potential terrorists and preventing further terrorist attacks failed to achieve its aims, what are the implications of this? One approach is to address this issue in the context of the civil liberties/national security paradigm and to consider whether the abrogation of civil liberties, including the right to data privacy, is an acceptable part of a strategy, involving mass surveillance, designed to prevent further terrorist catastrophes. Waldron points out that 'the balancing argument is supposed to

[331] Charlie Savage, 'Obama says NSA Curbs would Address Worries' *The New York Times* 25 March 2014.
[332] ibid.
[333] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others*. Grand Chamber CJEU, 8 April 2014. The instant case along with its significance and implications have been assessed in Chapter One, Sections 8.0, 9.0 and 10.0.
[334] See European Chapters for more on the judgment.
[335] David Cole, 'Can Privacy Be Saved?' *The New York Review Of Books* 6, (19 March 2014) 23-24.

turn on what we can achieve by diminishing liberty; it is not supposed to turn on the sheer horror at what has happened, nor on fear of what might happen.'[336] Waldron's point is that while fear is only half a reason for modifying civil liberties, 'the other and indispensable half is a well-informed belief that the modification [of civil liberties] will actually make a difference to the prospect that we fear.' [337] Waldron further argues that the fact that a certain degree of liberty is associated in the public mind with a certain degree of risk is not itself a ground for diminishing the liberty given a concern for the risk. 'We must,' he claims, 'also be sure that the diminution of liberty will in fact have the desired consequence.'[338] Polling data revealed that after the 9/11 attacks, 85% of those surveyed thought another terrorist attack against the United States was likely, a number that decreased to 52% by 2002 and stood at 38% in 2011. Polling data also show that from 2003 to 2011, between 65% and 71% of respondents felt that government actions against terrorism should not violate the civil liberties of Americans. Following the Snowden revelations, survey data show that 90% of Americans felt they had less privacy than previous generations when it comes to personal data, while data collected in June 2013 show that 53% of Americans disapproved of government surveillance programmes.[339]

Waldron's conclusion is that the government's case for restricting liberty must be based on the actual prospect that security will be enhanced if liberty is reduced. However, it may be said, quite reasonably, that we cannot know what that prospect is. In that case, 'what has to be inferred is that we cannot know whether it is worth giving up this liberty, and thus cannot talk with any confidence about an adjustment of the balance.'[340]

If, as indicated earlier, the elaborate surveillance measures undertaken since 9/11 had little or no effect as a terrorist prevention programme, it conveyed the impression to the American people that decisive measures, including the NSA spying programme and the Patriot Act, were undertaken with the objective of

[336] Jeremy Waldron, 'Security and Liberty: The Image of Balance' 11(2) (2003) *The Journal of Political Philosophy* 191, 198.
[337] ibid.
[338] ibid.
[339] Mathiew Deflem and Shannon McDonough, 'The Fear of Counterterrorism: Surveillance and Civil Liberties since 9/11' 52(1) (2015) *Global Society* 70, 77.
[340] Jeremy Waldron, 'Security and Liberty: The Image of Balance' 11(2) (2003) *The Journal of Political Philosophy* 191, 208-09.

preventing further terrorist incidents such as those of 9/11. The massive public approval for such measures in the atmosphere of a terrorist emergency was indicated in a dramatic increase in George Bush's popularity: his approval ratings rose by 35 points to 87 per cent, the highest in American history.[341] Waldron remarks that the psychological reassurance that people derived from Bush's surveillance measures 'is a consequential gain from the loss of liberty.'[342] However, although Waldron was writing in 2003, before the reports of the futility of these measures were circulating, his comment on those who remain receptive to the need to compromise civil liberty without due regard for the possible effectiveness of the surveillance measures for which civil liberty has been sacrificed might serve as an appropriate verdict on the ill-fated surveillance programmes: 'We should not give up our liberties, or anyone else's liberties, for the sake of purely symbolic gains in the war on terrorism.'[343]

14.0 In Defence of Communications Data Retention

In certain instances, the provision of robust telecommunications data retention mechanisms is essential to promoting the objective of upholding public safety. The comments of Ban Ki-moon, Secretary General of The United Nations, regarding the use of the Internet for terrorist purposes, are instructive: '[t]he Internet is a prime example of how terrorists can behave in a truly transnational way; in response, States need to think and function in an equally transnational manner.'[344] The global nature of the Internet has given rise to a large increase in data volumes, with one exabyte of data representing the equivalent of 500 billion pages of text. It is estimated that 76 exabytes of data will travel across the Internet from 2015.[345] The ongoing opportunities for such large-scale data transfers pose increasing difficulties for intelligence and law enforcement agencies when digital communications are misused for criminal or terrorist purposes.

In the wake of the Snowden revelations, General Keith Alexander, head of the NSA defended his agency's ability to retain and examine mass retained

[341] John E. Owens, 'Presidential Power and Congressional Acquiescence in the "War" on Terrorism: A New Constitutional Equilibrium?' 34(2) (2006) *Politics and Policy* 258, 259.
[342] ibid.
[343] ibid, 210.
[344] UNODC: United Nations Office on Drugs and Crime (2012) *The Use of the Internet for Terrorist Purposes.* New York: United Nations.
[345] Bruce Schneier, *Data and Goliath. The Hidden Battles To Collect Your Data And Control Your World* (Norton 2015). Chapter 1.

electronic communications traffic by means of surveillance programmes.[346] Alexander observed that such surveillance programmes had been essential in preventing terror plots in the USA and elsewhere.[347] He highlighted the case of Najibullah Zazi, an Afghan American whose plan to perpetrate suicide attack in New York was detected and foiled because of NSA, surveillance, and that of David C. Hedley, whose plan to attack the offices of a Danish newspaper that published a cartoon of the prophet Mohammad. Hedley had been arrested in 2009 for his participation in a terrorist attack in Mumbai.[348]

Alexander, appearing before a US Senate Appropriations Committee, contended that the Snowden revelations had serious consequences for the prevention of terrorism and commented that '[g]rave harm has already been done by opening this up,' and further contended that undoubtedly, 'we will lose capabilities as a result of this, and that not only the United States but those allies that we would help will no longer be as safe as they were two weeks ago.'[349] An example of the benefits of NSA data retention policies helping to thwart terror plots outside the US is the use by German authorities of communications data retained by the NSA in the prevention of acts of terror on German soil. Intelligence information supplied by the NSA to German authorities has played a role in nearly every major German terrorist case over the past decade.'[350] Such information enabled German authorities to arrest and subsequently convict those who participated in the German-based 'Sauerland cell' led by Fritz Gelowicz, a German convert to Islam, which planned a series of bomb attacks on American targets in Germany. Had these attacks been thwarted, the result would have been 'a notorious blood bath,' according to a State Court judge in Düsseldorf. [351] The prevention of the atrocities was due to the interception of e-mail traffic between Germany and Pakistan.[352]

---

[346] Ellen Nakashima and Jerry Markon, 'NSA director says dozens of attacks were stopped by surveillance programmes' *The Washington Post* 12 June, 2013.
[347] ibid.
[348] ibid.
[349] ibid.
[350] The German Prism: Germany Wants to spy Too' *Spiegel Online* 17 June 2013. Available at: <http://www.spiegel.de/international/germany/berlin-profits-from-us-spying-program-and-is-planning-its-own-a-906129-2.html> Accessed 23 May 2015.
[351] Nicholas Kulish, 'Germany Sentences 4 in Terror Case' *The New York Times* March 4 2010.
[352] The German Prism: Germany Wants to spy Too' *Spiegel Online* 17 June 2013. Available at: <http://www.spiegel.de/international/germany/berlin-profits-from-us-spying-program-and-is-planning-its-own-a-906129-2.html> Accessed 23 May 2015.

14.1 EU Commission Report

The EU Commission acknowledges that certain types of crime cannot be investigated or prevented without recourse to retained telecommunications data. The Commission's 2011 Evaluation Report provides instances of this. Based on examples from Belgium, Ireland and the United Kingdom, the report comments that certain crimes involving communication over the internet can be investigated **only** via data retention[353] and where identification was made possible only by means of retained telecommunications data.[354]

The Commission's Evidence Dossier provides a valuable insight into the investigation of crimes and related activities, which could not have been conducted in the absence of 'mandatory communications data retention,' as opposed to 'communications data per se.'[355] In this regard, the Commission comments that the former offers 'the guarantee that potentially valuable data will be available for a given amount of time.'[356] It cautions that other retention measures including data preservation, also referred to as quick freeze, although possessing other capabilities, cannot provide law enforcement agencies with the same certainty of the availability of retained communications data, instead relying 'wholly on the need or willingness of operators to store these data for their own commercial purposes, and to do so in such a way as to render these data accessible in time to be valuable to investigations and prosecution'.[357]

In instances involving the exchange of retained telecommunications data between Member States, the underlying principle is that of mutual assistance. With regard to the investigation of serious crime throughout the EU, approximately 40,000 requests or half the total data requests pertain to retained telecommunications data.[358] One of the major challenges facing law enforcement agencies in the EU is the length of time taken to process cross-

[353] European Commission, (2011) Report from the Commission to the Council and the European Parliament. Evaluation Report on the Data Retention Directive (Directive 2006/24/EC) COM 225 final. 14. 1. 24. Henceforth cited as Commission Report 2011.
[354] ibid.
[355] EU Commission Dossier 'Evidence for necessity of data retention in the EU' March 2013. 1. 5. Available at 5.<http://ec.europa.eu/dgs/home-affairs/pdf/policies/police_cooperation/evidence_en.pdf> Henceforth cited as Dossier.
[356] ibid.
[357] ibid, at 5.
[358] Workshop with police on future options for data retention in the EU, 17 June 2011. 'Serious crime' is defined in Council Decision 2009/371/JHA establishing the European Police Office (Europol).

border requests for traffic data, as a consequence of mutual assistance requirements. A major obstacle to the swift commencement of criminal investigations is the potential for the individual or individuals being targeted as part of an investigation, to replace their SIM card or IP addresses while a request for retained traffic is being considered.[359] The procedural difficulties facing law enforcement have been exacerbated by the ECtHR's finding that the Data Retention Directive breached the privacy rights of European citizens.[360]

However, where such requests are processed in a relatively speedy manner, and when 'a good level of trust'[361] exists between Member States, as in the example of cooperation between France and Spain to combat the terrorist threat posed by ETA, it is noted 'that data are exchanged more easily.'[362] Cross-border data sharing is an invaluable tool of European law enforcement agencies, as evidenced by the example of a United Kingdom law enforcement agency which required retained telecommunications data during the course of a six-month period in 2009-10.[363] The retained traffic data obtained were used in the course of five operations and as a consequence fourteen cases were brought before courts in other EU Member States or courts outside the EU, with each resulting in a conviction. Statistics supplied by Lithuania showed that in 2010, from a total of approximately 136,000 cases where retained traffic data were requested, 23,000 involved requests for legal assistance from other Member States in relation to high-volume and high-value mobile telephone theft.[364]

The Emmerson Report, which considers the balance between retention and surveillance obligations on the one hand, and human rights considerations on the other, acknowledges that increased mechanisms now available to Sates have enabled law enforcement and intelligence agencies to conduct 'targeted

[359] EU Commission Dossier 'Evidence for necessity of data retention in the EU' March 2013. 1. 5. Available at 5.<http://ec.europa.eu/dgs/home-affairs/pdf/policies/police_cooperation/evidence_en.pdf> at 6.
[360] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others*. Grand Chamber CJEU, 8 April 2014.
[361] EU Commission Dossier 'Evidence for necessity of data retention in the EU' March 2013. 1. 5. Available at 5.<http://ec.europa.eu/dgs/home-affairs/pdf/policies/police_cooperation/evidence_en.pdf> at 6.
[362] ibid.
[363] ibid.
[364] ibid.

surveillance of suspected individuals and organisations,'[365] and recognises that '[t]he interception of communications provides a valuable source of information by which States can investigate, forestall and prosecute acts of terrorism and other serious crime.'[366] Although the Emmerson Report cautions against the lack of proportionality attaching to the blanket mass retention of communications,[367] it offers a normative warrant for the use of mass surveillance in keeping with principles of proportionality.

The Report notes the capacity of states to conduct targeted surveillance of a given individual, with a view to tracking their location and movements, through the interception of landline or mobile telephone communications, in addition to online activities and information contained on databases and on cloud facilities. Emmerson remarks that from the standpoint of law enforcement objectives, technologies which advance mass surveillance initiatives have the additional value of enabling 'the surveillance of the communications of individuals and organisations that have not previously come to the attention of the authorities.'[368] This perspective on one of the capabilities of mass surveillance accompanied by data retention comports with comments made by General Keith Alexander, former Director of the NSA, at this point, when musing over investigative surveillance approaches: 'You might ask, ‘What’s the best way to figure out who the bad guys are? What would you start with? You’d say, Well, I need to know who his network of friends are, because chances are many of them are bad, too.'[369]

The Emmerson Report places emphasis on the monitoring of Internet traffic and communications as a key counter-terrorism initiative, particularly with regard to the 'financing and perpetration of acts of international terrorism,' owing to the use of the Internet 'for the purpose of recruitment to terrorist organisations,' in addition to the advance identification 'of those involved in the

[365] United Nations General Assembly, 'Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism' 23 September 2014 at para 6. Available at:<http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519.pdf?OpenElement> Accessed 17 April 2015. Henceforth cited as A/69/397.
[366] ibid, at para 6.
[367] ibid, at para 7.
[368] ibid, at para 10.
[369] Matthias Schwartz, The Whole Haystack' *The New Yorker*, 26 January 2015.

planning or instigation of acts of terrorism' which 'may otherwise be hampered by intelligence limitations.'[370] Emmerson critically emphasises that as terrorism 'is a global activity,' the quest to locate terrorists, necessarily 'must extend beyond national borders.'[371] From a normative perspective, Emmerson contends that the 'prevention and suppression of terrorism' has become 'a public interest imperative of the highest importance and may in principle form the basis of an arguable justification for mass surveillance of the Internet.'[372]

Emmerson's Report highlights the fundamental societal threats posed by terrorism, particularly the potential to destabilize communities, threaten social and economic development, fracture the territorial integrity of States, and undermine international peace and security.' Moreover, Article 6 of The United Nations Convention for the Suppression of the Financing of Terrorism, enshrines that:

> Each State Party shall adopt such measures as may be necessary, including, where appropriate, domestic legislation, to ensure that criminal acts within the scope of this Convention are under no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature.[373]

In this regard, Emmerson highlights that signatory states to the Convention are bound by a 'positive obligation to protect citizens and others within their jurisdiction against acts of terrorism.'[374] The Report focuses on an aspect of the obligation, the 'duty to establish effective mechanisms for identifying potential terrorist threats before they have materialized.'[375] Such a pre-emptive project would necessarily involve data retention.

14.2 Future Developments?

The quest to find a balance between the retention of telecommunications data which fulfils national security objectives and the right to data privacy, is likely

[370] A/69/397, at 34.
[371] ibid.
[372] ibid.
[373] Adopted by the General Assembly of the United Nations in resolution 54/109 of 9 December 1999.
[374] A/69/397 at 33.
[375] ibid.

to ensure for the foreseeable future, in the same fashion as has the technological joust for supremacy between cryptographers and de-cryptographers.

For law enforcement agencies, legislators and the judiciary, the relentless and rapid pace of technological evolution, development and innovation has proven difficult, if not impossible to evaluate and respond to with commensurate rapidity. This, coupled with transborder transfers of digital communications and data, makes the task of upholding national security and serious crime objectives difficult. Moreover, the increasing use of retention circumvention methods in the form of encryption, unregistered SIM cards and phone handsets, in addition to the relative anonymity offered by the Darkweb, illustrates the ever increasing potential for acts to terrorism to be perpetrated with a corresponding absence of any certainty that those engaged in such acts will be detected.

Those seeking greater levels of privacy in the digital era face inevitable obstacles which impact upon the practical implementation of normative attempts to enhance levels of privacy. 'Deleted' data, whether telecommunications data or other forms of data, are not always deleted, but can be transferred from one server to another, while 'matters for momentary embarrassment, can now become immortalized on web servers.'[376] Law enforcement objectives are cited to explain the need to ensure that certain forms of information are not deleted to ensure that evidence cannot be tampered with.[377]

From the standpoint of preserving or enhancing privacy rights and guarantees in the digital age, it seems likely that legislative instruments such as the Fourth Amendment in the United States and Article 8 of the European Convention On Human Rights, in addition to domestic statutes, require evolution to capture the nuances of rapidly advancing technologies and how these can impact whether positively or negatively on privacy rights. This appears necessary, as the Fourth Amendment and Article 8 ECHR were envisioned and promulgated during the Twentieth Century, when digital age concerns such as the balance

[376] Alexander Tsesis, 'The Rights To Erasure: Privacy, Data Brokers And The Indefinite Retention of Data' 49 (2014) *Wake Forrest Law Review* 442.
[377] ibid, 478.

between telecommunications data retention and privacy rights were yet to manifest.

The transborder dimension of data flows and exchanges poses challenges for those advocating privacy and law enforcement standpoints. Due to the borderless nature of communications in the digital age, it is likely that an International treaty or protocol, administered by the United Nations, might be necessary to establish what constitute privacy and national security aims and objectives and under what circumstances the balances between the two can be altered. This development of Cloud Computing, where data can be stored in many territories, poses difficulties for those on both sides of the balancing paradigm.

A recurring question which emerges in the discourse relating to the balance between the retention of telecommunications and other data to uphold national security objectives and privacy and data privacy rights, concerns whether such retained data contribute to efforts to prevent and combat serious crime and terrorism. To date, there is little evidence to support this proposition, aside from contentions by Governments that data retention measures have prevented instances of terrorism from taking place.

Those who advocate that the absence of the mass retention of telecommunications, Internet and other forms of communications data is necessary to uphold privacy rights, might consider the possibility that as increasing acts of terror are perpetrated, the absence of retention mechanisms could confer an advantage on the enemies of a particular nation, state or continent.

It is now widely accepted that five arenas exists where conflict and warfare have the potential to occur; land, sea, air, outer space and within cyberspace, However potential responses to ongoing acts of terror and hacking, perpetrated through and with direct effects on cyberspace itself and beyond continue to evolve, but have yet to crystallise.[378] Perhaps it is valid to draw an analogy between the privacy/data retention balancing paradigm and the question

[378] Gary D. Solis, 'Cyber Warfare' *Military Law Review* 219 (2014), 1, 40.

regarding the merits and demerits regarding nuclear weapons and their role in global conflict. Amis sums up the rationale of those who seek to justify the necessity of nuclear weapons as a means of preventing their use:

> What is the only provocation that could bring about the use of nuclear weapons? Nuclear weapons. What is the priority target for nuclear weapons? Nuclear weapons. What is the only established defense against nuclear weapons? Nuclear weapons. How do we prevent the use of nuclear weapons? By threatening to use nuclear weapons. And we can't get rid of nuclear weapons, because of nuclear weapons.[379]

Perhaps telecommunications data retention is necessary to ensure that its use cannot be monopolised by any nation, state or continent to the detriment of another.

15.0 The U.S.A. Freedom Act, 2015. Adjusting the Data Privacy/National Security Balance in favour of Privacy?

15.1 Background

When Edward Snowden began releasing classified information in June 2013 about NSA surveillance activities, he helped to initiate a widespread discussion of the U.S. Government's secret surveillance practices. One of Snowden's most damaging revelations was a sweeping FISC opinion, in which it ordered Verizon Communications Inc to furnish all telephone data to the NSA once a day under the auspices of Section 215 of the Patriot Act.[380] Snowden's revelations and the reactions they provoked among the general public, the political class and the media[381] proved to be the catalyst which ultimately led to the enactment of the Freedom Act. The FISC order was originally requested by the FBI. The data which had to be supplied by Verizon involved 'all call records or telephony metadata,' for communications made via its systems, both within the United States and between the United States and other countries.[382]

---

[379] Martin Amis, *Einstein's Monsters* (Jonathan Cape, 1987) "Introduction: Thinkability" (Jonathan Cape, 1987), 2.
[380] See Glenn Greenwald, 'NSA Collecting Phone records of Millions of Americans Daily' *The Guardian* June 6, 2013.
[381] See Ian Black, 'NSA Spying Scandal: What We Have Learned,' *The Guardian* June 10 2013.
[382] See 'Verizon forced to hand over telephone data - fall Court Ruling' *The Guardian* June 5, 2013.

The telephony metadata' in question included the number of both parties on a call, unique identifiers, and the time and duration of all calls. The order gave the government the authority to obtain these call detail records or telephony metadata for a three month period, ending on July 19, 2013.[383]

The Snowden revelations spurred a national conversation about government intelligence collection and surveillance.[384] On March 27, 2014, President Obama announced several changes to the conduct of foreign intelligence activities in response to Snowden's unauthorised disclosure of classified information. The President announced changes that imposed a substantive limit on the scope of the NSA's access to telephony metadata, and a procedural limit on when the NSA might access the data in the first place. The procedural limit also required that the FISC approved queries of telephony metadata on a case by case basis and before the query was conducted, whereas under the bulk metadata programme the NSA was permitted to query the data without court approval. A further response to the Snowden revelations came from the House Judiciary Committee, which conducted aggressive oversight of the surveillance programmes. In July 2013, the Committee held a public hearing at which testimony was received from officials with the Justice Department, the Office of the Director of National Intelligence, the NSA, the FBI and civil liberties groups. The Committee held a comprehensive hearing to examine the various recommendations to reform the surveillance programmes. The proceedings eventuated in the emergence of the USA Freedom Bill with unanimous support. The Bill was passed by the House of Representatives on May 22, 2014. What emerged was compromise legislation that neither privacy nor intelligence interests considered perfect. Nevertheless, the White House endorsed the Bill in an official policy statement:

[383] ibid.

[384] See David Cole, 'Can Privacy Be Saved?' *New York Review of Books* March 6 2014 (discussing concerns about privacy); Laura K. Donohue, 'Section 702 and the Collection of International Telephone and Internet Content' 38(1) (2015) *Harvard Journal of Law and Public Policy* 117 (expressing caution about the risks attaching to foreign surveillance); Laura K. Donohue, 'Bulk Metadata Collection: Statutory and Constitutional Considerations' 37 (2013) *Harvard Journal of Law and Public Policy* 757 (warning about the risks of domestic surveillance); Shayana Kadidal, 'NSA Surveillance: The Implications for Civil Liberties' 10(1) (2014) *Journal of Law and Policy for the Information Society* 433.

> The bill ensures our intelligence and law enforcement professionals have the authorities they need to protect the Nation, while further ensuring that individuals' privacy is appropriately protected when these authorities are employed. Among other provisions, the bill prohibits bulk collection through the use of Section 215, FISA pen registers, and National Security Letters.[385]

When the Bill came before the Senate, it failed to garner enough votes to become law.[386] However, because these surveillance provisions of the Patriot Act were due to expire on June 1 2015, there was a need to address privacy concerns stemming from government surveillance. Several amendments designed to weaken the civil liberties protections of the Freedom Bill were voted down by the Senate, which then passed the House of Representatives version of the Bill, thus enacting the Freedom Act into law.

15.2 Provisions of the U.S.A. Freedom Act

The full title of the Act is 'Uniting and Strengthening America by Fulfilling Rights and ensuring effective Discipline over Monitoring Act of 2015.' The Act extends three expiring provisions of the Patriot Act, but overhauls its most controversial provision, the use of the pen register and trap and trace authority,[387] which U.S. Governments had interpreted to permit the NSA to engage in the bulk collection of the phone records and Internet metadata of American citizens.[388] It limits the government's data collection to the 'greatest extent reasonably practical': this means that the government cannot collect all data pertaining to a particular service provider or broad geographical region, such as a city or area code. It enables the phone records collection to resume for six months, provided that the Foreign Intelligence Surveillance Court orders phone companies to hand over their records, and that no Court stops this

[385] Statement of Administration Policy: H.R. 3361 - USA FREEDOM Act May 21, 2014 <http://www.presidency.ucsb.edu/ws/?pid=105338> accessed 21 December 2016.

[386] Adi Robertson and Nathan Ingraham, 'USA Freedom Act for NSA reform is voted down in the Senate' *The Verge*, November 18, 2014 <http://www.theverge.com/2014/11/18/7241967/usa-freedom-act-for-nsa-reform-is-voted-down-in-the-senate> accessed 23 December 2016.

[387] *See* 18 U.S.C. *§* 3127(3)-(4). A pen register records outgoing addressing information. 18 U.S.C. *§* 3127(3). A trap and trace device records incoming addressing information. 18 U.S.C. *§* 3127(4). Cited in Jeremy J. Broggi, 'Building On Executive Order 13,686 To Encourage Information Sharing For Cybersecurity Purposes' 37 (2014) *Harvard Journal of Law and Public Policy* 653, 672, fn 127.

[388] For a detailed section-by-section analysis of the Freedom Act, See Report of the House of Representatives Committee on the Judiciary, May 8 2015.

under various pending lawsuits. During those six months, the NSA will try to collaborate with providers to devise a method of querying their records expeditiously, against known terrorist phone numbers, pursuant to a Court order.[389] It will be possible for the NSA to collect data for all the numbers in contact with the subject number, and all the numbers in contact with these numbers. In other words, instead of permitting bulk collection, the Freedom Act authorises the government to collect from phone companies up to 'two hops' of call records, [390] provided that it can prove that it has 'reasonable' suspicion that the suspect is linked to a terrorist organisation.[391] As a result the NSA will still be enabled to collect the phone records of Americans, but not all of these. The Act does not provide guidance on what government may do with the American calling records it has been collecting over the years, or whether it will continue to search them.

A significant provision of the Freedom Act is that it extends the date of expiration of *three* Patriot Act provisions - Section 215, roving wiretaps and the lone wolf surveillance authority - to December 2019. But for this extension, these provisions would otherwise have expired. [392] The roving wiretap provision, which allows the FBI to eavesdrop on espionage and terror suspects who regularly change their communication devices, will go back into effect. The Freedom Act expands the definition of an 'agent of a foreign power'[393] with a view to helping security forces to monitor 'lone wolf' operators, such as those who carried out the Boston Marathon bombings. The Freedom Act gives providers greater scope to publish information about the number of National Security Surveillance demands they receive. More importantly, it requires declassification of FISA Court opinions containing significant legal decisions, hitherto secret - or a summary of these if declassification is not possible.[394] This provision of the Freedom Act is designed to prevent secret interpretations, which facilitated the bulk collection of U.S. telephone records.

[389] The Act also requires the FISC to publish opinions in certain circumstances.
[390] The call data records (CRDs) associated with the initial seed telephone number and call detail records associated with the CDRs identified in an initial 'hop.'
[391] USA Freedom Act H.R. 2048 Section 101.
[392] ibid, Section 705.
[393] ibid, Section 702.
[394] ibid, Section 402.

The legislation embodied in the Act addresses the most serious privacy concern raised by the disclosures of Edward Snowden: the bulk collection of domestic phone records. However, it does nothing to address another of Snowden's revelations: the collection by the NSA of foreign Internet content from U.S. technology companies, a programme that collects a considerable volume of U.S. communications. Furthermore, the Act does not address most of Snowden's disclosures about foreign intelligence gathering, nor does it address the NSA's attempts to exploit technologies such as encryption for the benefit of U.S. intelligence.

Finally, The Freedom Act also introduces a number of FISA Court reforms. The Act directs the presiding judges of the FISA Court and the FISA Court of Review to designate at least five individuals to serve as friends of the Court 'to assist in the consideration of any application for an order or review that presents novel or significant interpretation of the law.'[395] The same Section 'permits FISA Courts to appoint an individual or organisation to serve as *amicus curia* including to provide technical expertise.'[396] Such amici curiae are required to provide (1) legal arguments that advance protection of individual privacy and civil liberties or (2) other legal arguments or information related to intelligence collection or communications technology.[397]

15.3 Responses to the Freedom Act

The Electronic Frontier Foundation, a digital privacy lobby group, while expressing some concerns about the provisions of the Freedom Act, welcomed its passage as 'marking the first time in over thirty years that both Houses of Congress have approved a Bill placing real restrictions and oversight on the National Security Agency's surveillance powers.'[398] The Foundation isolated two aspects of the Act which should give technology users everywhere cause to celebrate: that the NSA 'will be a little more hampered in its surveillance overreach, and that both the NSA and the FISA Court will be more transparent

[395] ibid, Section 401.
[396] ibid.
[397] ibid.
[398] Cindy Cohn and Mark Jaycox, 'USA Freedom Act Passes: What We Celebrate, What We Mourn, and Where We Go From Here' *Electronic Frontier Foundation* (June 2, 2015) <https://www.eff.org/deeplinks/2015/05/usa-freedom-act-passes-what-we-celebrate-what-we-mourn-and-where-we-go-here> accessed 5 June, 2015.

and accountable than it was before'[399] However, 'while the Freedom Act represents a significant step in the Foundation's campaign to end overbroad surveillance of the digital lives of Americans, much still remains to be done.'[400]

While the Freedom Act might have neutered the phone records surveillance programme and provided a degree of transparency to the secretive FISA Court overseeing the surveillance, the broader digital surveillance problem remains to be solved. This is the problem of over-classification, a function of government use of secrecy and the claims of national security interests to ward off public oversight. The Freedom Act reforms cannot be fully effective unless more light is thrown on how government and its surveillance agencies are interpreting the law, and unless abuses of state secrets privilege are addressed.

Some responses to the Freedom Act were positive. The House Judiciary Report acknowledged what the Act had achieved in taking account of the needs of national security and the protection of citizens' privacy:

> H.R. 2048, the ‘‘USA FREEDOM Act of 2015,’’ prohibits bulk collection of records under Section 215 of the USA PATRIOT Act (Section 501 of the Foreign Intelligence Surveillance Act (FISA)), under the FISA Pen Register and Trap and Trace Device statute, and under National Security Letter (NSL) authorities. The Act creates a new program for the targeted collection of telephone metadata, provides greater privacy and civil liberties protections for Americans, expands existing congressional oversight provisions, and creates greater transparency of national security programs operated pursuant to FISA.[401]

However, in their comment on the claims made in the House Judiciary Report, Mondale, Stein and Fisher remark that while 'the Freedom Act does accomplish each of the aforementioned goals,' given 'the status quo before its enactment, saying that it improves liberty protections and Congressional

[399] ibid.
[400] ibid.
[401] House Judiciary Report, 2.

oversight is not, by itself, saying too much.' [402] Looking at the Freedom Act as a triumph for the U.S. political process, Forsyth was satisfied that:

> The USA FREEDOM Act represents a clear political product, drafted as an honest attempt to equip the intelligence community with the tools it needs without unnecessarily compromising privacy or civil liberties. There is no perfect place to draw the line between privacy and national security. The Constitution does, however, establish that the political process is the perfect way to draw it.[403]

15.4 Problems Concerning the Freedom Act

Most critiques of the Freedom Act tend to focus on its failure to make the significant modifications to the existing surveillance structure under FISA rules necessary to bring about meaningful change. There was a general consensus among the critics of the Act that three significant changes were required. The first was to remedy the FISA Court's non-adversarial nature, which meant that FISA judges were not able to hear countervailing arguments to the Government's position. The second was that there was no institutionalised method of challenging the initial analysis of the FISA judges, who operated on the system that their opinions would be the final word on issues arising, and that their opinions would remain secret. The third was to address the FISA Court's lack of transparency. The failure of the Freedom Act to facilitate decisive change in those three areas may be partially attributed to the fact that the Act, like the Foreign Intelligence Surveillance Act (FISA), was the outcome of a compromise. In the course of the evolution of the Freedom Act, it was originally envisaged that a truly independent Special Advocate's role would be created. This met with significant resistance from the intelligence community, with the result that the original proposal was diluted. Berman notes that 'a version of the Freedom Act that did not include an independent special advocate was the result of a 'series of hard-fought compromises' among stakeholders, including *inter alia*, the intelligence community.'[404] The diluted

[402] Walter R Mondale., Robert A. Stein and Caitlinrose Fisher, 'No Longer a Neutral Magistrate: The Foreign Intelligence Surveillance Court in the Wake of the War on Terror' 100(6) (2016) *Minnesota Law Review* 2251, 2262.
[403] Bart Forsyth, 'Banning Bulk: Passage of the USA Freedom Act and Ending Bulk Collection 72 (2015) *Washington and Lee Law Review* 1307, 1351.
[404] Emily Berman, 'Two Faces of the Foreign Intelligence Surveillance Court' 91(4) (2016) *Indiana Law Journal* 1191.

version of the Special Advocate proposal that was enacted involved the idea that FISA judges should be *encouraged* to appoint *amici curiae* rather than creating independent advocates. The Freedom Act of 2015 stipulated that the FISA Court:

> [S]hall appoint an individual who has been designated under paragraph (1) to serve as amicus curiae to assist such court in the consideration of any application for an order or review that, in the opinion of the court, presents a novel or significant interpretation of the law, unless the court issues a finding that such appointment is not appropriate.[405]

As a gesture towards the interests of privacy and civil liberties generally, the Act provided that any amicus appointed pursuant to Section 401 would provide the Court with legal arguments that 'advance the protection of individual civil liberties,' information 'related to intelligence collection or communications technology, or any other arguments or information.' The Court was also permitted to appoint an *amicus* to provide technical expertise, or to approve a motion by an individual or organisation to file an amicus brief. These were the only gestures contained in the Freedom Act which included some adversarial elements.

This *amici* provision is a feeble step in the direction of remedying FISA's post-9/11 underlying defects involving independent advocacy. This provision raises a number of troubling issues, the main one being that the FISA Court has the discretion to appoint, or not to appoint an *amicus*, and can decide that such an appointment is not appropriate. Secondly, if an *amicus* is appointed by the Court, he or she is not obliged to present a view that is adversarial to the government. Thirdly, the *amicus*, as a mere 'friend of the Court,' as opposed to being a party to the action, cannot appeal any losing decisions to the FISA Court of Review, as an adverse party could in any other individual lawsuit. As Mondale, Stein and Fischer point out, '[t]he amici provision thus provides only

[405] USA Freedom Act of 2015, Pub. L. No. 114-23, 129 Stat. 268, Section 401 2(A), Appointment of Amicus Curiae.

a surface level adversity to FISC proceedings, but does not change the underlying issues that limit FISC's ability to provide meaningful oversight.'[406]

The Freedom Act does not have due regard for the fact that the strength of the adversarial process derives from 'the guarantee it provides that each side will be presented in its most convincing form.'[407] Instead, the Act's nearest approach to an adversarial process is to empower the FISA Courts to *request* the services of an amicus curiae unless they deem that such a request is not appropriate. Berman points out that it should be 'for the FISA Court to decide whether an opposing party might have something to add. Instead, it should be an advocate's job to determine when a government raises a privacy or civil liberty concern to which it wants to respond. The power to determine when to intervene should rest with the advocate, not with the Court.[408] Had the Freedom Act incorporated the provisions suggested above, it would have addressed some of the serious defects implicit in the FISA process. As for the claim that an *amicus* appointed by the Court would provide it with legal arguments that advance the protection of individuals' liberties, this might have more substance in the context of the re-adjustment of the data privacy/national security balance had the Freedom Act given the *amicus curiae* the full authority and rights of an adverse party, with the capacity to appear in his or her own right, without having to be invited by the Court, to affirm the data privacy rights of citizens when, for example, mass surveillance of personal data is in question.

A further problem arises in connection with the *amicus* provision. This is the ambiguity of the terminology used to describe the role of the *amicus* should he or she be appointed by the Court. It is not made clear, for example, what 'a novel or significant interpretation of the law' means on which the *amicus* might be asked to comment. The Act provides no definition, or example of either the meaning of 'the law' on which comment might be appropriate. As might be expected from a piece of legislation which has resulted from a compromise between the conflicting views of privacy advocates and the intelligence

[406] Walter R Mondale., Robert A. Stein and Caitlinrose Fisher, 'No Longer a Neutral Magistrate: The Foreign Intelligence Surveillance Court in the Wake of the War on Terror' 100(6) (2016) *Minnesota Law Review* 2251, 2296.
[407] Emily Berman, 'Two Faces of the Foreign Intelligence Surveillance Court' 91(4) (2016) *Indiana Law Journal* 1243.
[408] ibid.

community, the Freedom Act, as Mondale, Stein and Fisher point out, 'contains an escape clause for the Court'[409] since the FISC does not need to appoint an *amicus* 'even if the case involves novel or significant issues, of such appointment is not appropriate.'[410]

Mondale et al also observe that on the question 'what would render such an appointment inappropriate?' Congress provided absolutely no guidance. They also pointed out that this is exactly the kind of ambiguous language that can be used to further the intelligence community's preference for 'operating in a cloak of secrecy at the expense of personal liberties,' and that the members of the FISA Court who are hostile to the Freedom Act's amici provision will use the Act's ambiguity to preclude the appointment of an amicus.'[411] It is worth noting that a FISC opinion delivered on June 17, 2015 suggested that it may be unnecessary to appoint an amicus if 'the Court concludes [that] the legal question is relatively simple or is capable of only a single reasonable or rational outcome,' or if the appointment would result in 'some degree of additional expense and delay.'[412]

To put the deficiencies of the Freedom Act's provision for an *amicus curiae* into perspective, it is useful to consider what a 2013 Congressional Research Service Report had in mind as a measure to reform the current national surveillance regime. This measure would involve the creation of a Special Advocate to counter the Government's arguments before the FISA Court.[413] The Congress Report centred on the idea that the Special Advocate would have a range of possibilities including the right to intervene in ongoing cases, to brief the FISC on relevant matters, conduct some forms of discovery, or appeal an adverse ruling. A common theme of the Report was an increase in the

[409] Walter R Mondale., Robert A. Stein and Caitlinrose Fisher, 'No Longer a Neutral Magistrate: The Foreign Intelligence Surveillance Court in the Wake of the War on Terror' 100(6) (2016) *Minnesota Law Review* 2251, 2296.
[410] USA Freedom Act of 2015, Pub. L. No. 114-23, 129 Stat. 268, Section 401.
[411] Walter R Mondale., Robert A. Stein and Caitlinrose Fisher, 'No Longer a Neutral Magistrate: The Foreign Intelligence Surveillance Court in the Wake of the War on Terror' 100(6) (2016) *Minnesota Law Review* 2251, 2296-2297.
[412] Elizabeth Goitein, 'The FISC's Newest Opinion: Proof of the Need for an *Amicus*' *Just Security* (June 23,2015) <https://www.justsecurity.org/24134/fiscs-newest-opinion-proof-amicus/> accessed 23 December 2016.
[413] Andrew Nolan, Richard M. Thompson II and Vivian S. Chu, 'Reform of the Foreign Intelligence Surveillance Courts: Introducing a Public Advocate' *Congressional Research Service* 7-5700, at 5, fn 35 <https://fas.org/sgp/crs/intel/R43260.pdf> accessed 27 December 2016.

opportunities for adversarial litigation before both the FISC and the Foreign intelligence Court of Review (FISCR), to ensure that even behind the closed doors of the Court, the Government's legal positions could be subjected to vigorous debate. If these proposals were to have effect, the Special Advocate would need to be properly equipped to act as an equal counter-party to the Government lawyer presenting his or her case before the FISC. The general idea was to allow the FISC to hear arguments both for and against each Government request for a surveillance warrant, this replicating the adversarial proceedings common in other United States courtrooms. The case for appointing such a Special Advocate on a statutory basis was reinforced when it became widely known that the FISC had seldom turned down a government request.[414] Squitieri's account of the emergence of the Freedom Act as a response to the patent inadequacy of the FISA Court is plausible:

> Feeling political pressure to do *something to improve* an increasingly unpopular national surveillance regime, Congress halfheartedly answered the calls for a special advocate by passing the USA FREEDOM Act..... the Freedom Act's *amicus curiae* is essentially a watered-down version of the type of special advocate.[415]

16.0 Recent Developments: Reconsideration by the Courts of the Constitutionality of Mass Data Mining and Long-Term Surveillance. Implications for the Data Privacy/National Security Balance.

The decisions in *United States v Miller* [416] and in *Smith v Maryland* [417] did not represent the Supreme Court's final word on the subject. The Court's 2012 decision in *United States v Jones* raised serious doubts about the constitutionality of mass data mining and long-term surveillance, an issue with major implications for the data privacy/national security balance. Here, the majority of justices were of the view that the collection of sufficiently large

[414] Dina Temple-Raston, 'FISA Court Appears To Be Rubber Stamp For Government Requests' *NPR* (June 13, 2013) <http://www.npr.org/2013/06/13/191226106/fisa-court-appears-to-be-rubberstamp-for-government-requests> accessed 28 December 2016.
[415] Chad Squitieri, 'The Limits Of The Freedom Act's Amicus Curiae' 11(3) (2015) *Washington Journal Of Law, Technology and Arts* 197, 199.
[416] 425 U.S. 435 (1976).
[417] 442 U.S. 735 (1979).

amounts of information might amount to a search, thus implicating the Fourth Amendment, regardless of physical trespass.[418]

The finding in *Jones* that metadata collection and analysis can raise Fourth Amendment concerns, despite these data having been voluntarily disclosed to a third party, is significant. Grey and Citron[419] observe that 'five Justices joined concurring opinions in *Jones* expressing sympathy for some version of the 'mosaic theory' of Fourth Amendment privacy.'[420] The Mosaic theory of the Fourth Amendment suggests that the government can learn a lot more from a given piece of information if it can put that information in the context of a broader pattern, a mosaic. This insight, that the incremental privacy threat posed by the government's acquisition of information increases as more information is obtained was articulated by Judge Ginsburg in the District of Colombia Court in 2010:

> Prolonged surveillance reveals types of information not revealed by short term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynaecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story.[421]

Prior to *U.S. v Maynard*, a controlling precedent, *United States v Knotts*, had held that an individual driving a car on a public roads had no expectation of privacy in his or her whereabouts.[422] In *Maynard* however, Judge Ginsberg was

[418] 132 S.Ct., 945, at 956-7.
[419] David Gray, and Danielle Keats Citron, 'A Shattered Looking Glass. The Pitfalls and Potential of the Mosaic theory of Fourth Amendment Privacy' 14(2) (2013) *North Carolina Journal of Law and Technology* 381.
[420] ibid, 381-82.
[421] *United States v Maynard*, 615 F.3d 544, 558 (D.C. Cir. 2010) ("[T]he whole of one's movements is not exposed *constructively* even though each individual movement is exposed, because that whole reveals more – sometimes a great deal more – than the sum of its parts.").
[422] 460 US 276. For Knotts see Richard H. McAdams Privacy in *Knotts*. Beeper Privacy and Collective Fourth Amendment "Tying Rights' 7 (1985) *Virginia Law Review* 297.

arguing that, in the context of Fourth Amendment protection, the long-term monitoring of an individual had different consequences for protection under the Amendment than had a single instance of monitoring. The core of his argument was that the lack of Fourth Amendment protection when the driver of a car was seen in public at any given moment in time did not preclude the possibility that the police would need to obtain a warrant to record someone's movements over several weeks. In *Jones*, which soon followed, a Supreme Court majority held that warrantless geolocation surveillance conducted over four weeks was unconstitutional, being a contravention of the Fourth Amendment, even though surveillance for a short period of time was not.[423] Mornin observes in relation to *Jones* that:

> NSA's large-scale metadata collection raises a familiar Fourth Amendment dilemma: as new technology makes it easier for the government to detect and apprehend criminals, it also deepens threats to personal privacy and disrupts the balance of power between citizens and government. Jones signals the possibility that the [Supreme] Court is willing to revisit the third-party doctrine under new technological circumstances.[424]

Mornin further observes that under the theory of the five justices, 'the NSA's surveillance program tests the limits of current Fourth Amendment doctrine.'[425] In *Jones*, Justice Sotomayor, concurring in the majority verdict and having in mind the holding in *Miller* that there is no 'legitimate expectation of privacy' in information provided to a third party, raised the question 'whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will, their practical and religious beliefs, sexual habits and so on,' adding 'more fundamentally, it may be necessary to reconsider the premise [of the third-party doctrine] that an individual has no reasonable expectation of privacy in

[423] *United States v Jones*, 132 S. Ct. 945, at 964 (2012). See also David Gray et al., *Fighting Cybercrime After* United States v. Jones' 103 (2013) *Journal of Criminal Law and Criminology* 745, 760.
[424] ibid.
[425] ibid.

information voluntarily disclosed to third parties.'[426] Reidenberg observes that 'the lack of constitutional standards for access to data [as a consequence of the debilitation of Fourth Amendment protection] appears in flux in the wake of *Jones*.'[427]

In its defence of the NSA surveillance programme, the government has given two reasons, in the light of *Jones* why it believes mass metadata collection is not a Fourth Amendment search. Firstly, NSA collection of telephony metadata does not involve *trespass*, whereas the holding in *Jones* turned on the officer's physical intrusion.[428] Second, all call records do not include location information (except trunk data, which reveals approximate locations), whereas *Jones* addressed *precise location* data specifically.[429] The Government's reading of the Fourth Amendment doctrine is consistent with the Court's development of the *third party doctrine* in *Smith*.[430] However, as Benkler has noted, 'there is no question that all three *Jones* opinions offer a very strong argument that the dramatically lower cost of pervasive, sustained surveillance of publicly observable data implicates the Fourth Amendment.'[431] The FISC endorsed the government's reading in *Jones*. Judge McLaughlin wrote for the FISC Court that the five concurring justices in *Jones* recognised that 'precise, pervasive monitoring by the government of a person's location could trigger Fourth Amendment protection……However, NSA telephony metadata collection

[426] *United States v Jones* 132 S.Ct., 945, at 961 (2012). A GPS tracking device had been attached to Jones's car by the police in order to monitor his movements over a twenty-eight day period. During Jones's trial evidence was adduced by the prosecution based on his movements as captured by the GPS device. The prosecution relied on Jones's movements to and from a stash house to implicate him in a drugs conspiracy. Jones was convicted by the trial Court and received a life sentence. The Court of Appeals for the District of Colombia overturned the trial Court's verdict on the basis that the placing of a GPS device under Jones's car constituted a violation of his Fourth Amendment rights and represented a physical intrusion under the Constitution. The Court held that the evidence which flowed from the GPS device had been unlawfully obtained. A majority of the Supreme Court agreed and held, per Scalia J, that in instances where a physical intrusion into a constitutionally protected zone (in the instant case Jones's car) in tandem with the aim of gathering information in the form of evidence takes place, the Fourth Amendment is violated.

[427] Joel R. Ridenberg, 'The Data Surveillance State in the United States and Europe' 49 (2014) *Lake Forrest Law Review* 583, 588.

[428] Administration White Paper. Bulk Collection of Telephony Metadata Under Section 215 of the Patriot Act 9 August 2013<http://big.assets.huffingtonpost.com/Section215.pdf> accessed 1 January 2016, note 9, 20.

[429] ibid.

[430] *Smith v Maryland* 442 U.S. para 735 (1979).

[431] Yochai Benkler, 'In secret, Fisa court contradicted US Supreme Court on constitutional rights' *The Guardian* 22 September 2013 <https://www.theguardian.com/commentisfree/2013/sep/22/secret-fisa-court-constitutional-rights> accessed 1 January 2017.

'concerns the acquisition of non-content metadata other than location information.'[432]

An earlier Supreme Court decision in *Kyllo v United States*[433] anticipated the direction taken by the majority in *Jones* in relation to Fourth Amendment protection of privacy in that it was not grounded in the assumption that the government and its agencies had the inherent power to adopt and utilise new technologies subject only to narrow Fourth Amendment protections of privacy, these narrow protections being based on the doctrine that unless a search involves a recognisable privacy interest, the Fourth Amendment places no limits upon government's ability to conduct that search. *Kyllo v United States*[434] dealt with the question whether the government's use of thermal imaging equipment without a warrant was lawful. The Court's finding was that such warrantless use was unlawful. Justice Scalia, speaking for the Court, concluded that when a technology was not 'in general public use,' the Courts should 'assume preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'[435]

In other words, instead of framing the question at issue in terms of whether the Founders would have regarded the act of surveillance involving thermal imaging a search, the Court should ask whether the Founders enjoyed this level of security from government surveillance and harassment. The significance of this approach is that by grounding its analysis in the level of privacy enjoyed by the Founders, *Kyllo* points the way to a less restricted role for the Fourth Amendment, because it would subject all searches assisted by new technologies to the Fourth Amendment's restraints. If the finding in *Kyllo* were to become the general standard for Supreme Court jurisprudence in privacy/security cases, the government use of technologies would invariably be subject to a warrant requirement unless they were in general public use. As a further consequence, government surveillance agencies would need to show

[432] In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13-158 (FISA Ct. Oct. 11, 2013), *available at* http://www.uscourts.gov/uscourts/courts/fisc/br13-158-memo-131018.pdf> Cited in Joseph D. Mornin, 'NSA Metadata Collection and the Fourth Amendment' 29(4) (2014) *Berkley Technology Law Journal* 985, 1005.
[433] 553 U.S. 27, 2001.
[434] ibid.
[435] ibid, 34.

probable cause and obtain a warrant before it could deploy such privacy-invasive technologies as Magic Lantern, Carnivore or decryption. From a constitutional perspective, the principles outlined in *Kyllo*, if adopted generally, would arrest the decline of the Fourth Amendment's role in the protection of privacy rights and affirm its function as a limiting influence on executive power in the context of the Constitution's separation of powers.

In a more recent case, *Riley v California*,[436] the Supreme Court has broadened its vision of Fourth Amendment rights, and as in *Kyllo* and *Jones*, departed from the tendency of previous Courts to narrow their vision of Fourth Amendment rights to an opaque privacy rationale, avoiding the difficult issues involving technological progress. In *Riley*, the Court faced up to these issues by recognising that the Fourth Amendment was the founding generation's response to the privacy-invasive practices of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity.[437]

The petitioner, Riley, was stopped for a traffic violation. An officer searching Riley, incidental to the arrest, seized Riley's cell phone, accessed information on the phone and noticed the repeated use of a term associated with a street gang. Later, at the police station, a detective specialising in gangs further examined the phone's digital contents. Based on information the detective found, the State of California charged Riley in connection with a shooting that had occurred a few weeks earlier and sought an enhanced sentence based on Riley's gang membership.[438] Riley moved to suppress all evidence the police had obtained from his cell phone. The Court denied the motion, and Riley was convicted. The California Court of Appeal affirmed. The Supreme Court reversed the judgment of the California Court of Appeal.

In the course of its judgment, the Court focused particularly on one of the most notable distinguishing features of modern cell-phones: their immense storage capacity.[439] Many of these devices are, in fact, minicomputers that also have the

[436] 573 U.S. No. 13-132 (2014).
[437] ibid, at 27.
[438] ibid, at 1.
[439] ibid, at 17.

capacity to be used as telephones. They could just as easily be called cameras, video players, calendars, tape recorders, libraries, diaries, albums, televisions, maps or newspapers.[440] The implications of this fact for privacy rights were clear to the Court. A cell phone collects in one place many distinct types of information: an address, a note, a prescription, a bank statement, a video, that reveal much more in combination than any isolated record.[441] Further, a cell phone's capacity allows even one type of information to convey far more than previously possible, since the sum of an individual's private life can be reconstructed through a thousand photographs labelled with dates, locations and descriptions.[442]

The Court also emphasised the qualitative and quantitative contrast between the information gathering capacity of searches and seizures the Founders had in mind in framing the Fourth Amendment, and that available to modern governments and their agencies when, for example, as in *Riley* they explore a cell phone's digital contents.[443] In the former, even the most exhaustive search of a house for everything that might incriminate its owner was limited by physical realities, and tended as a general matter to constitute a narrow intrusion on privacy. In the latter case, a cell phone may contain in digital form many sensitive records previously found in the home, but it also contains a broad array of private information never found in a home in any form - unless there is a cell phone.[444]

The essence of the finding in *Riley* was not that information on a cell phone is immune from search, but that a warrant is generally required before such a search, even when a cell phone is seized incidental to arrest. The use of 'generally required' indicates an exception, for example, the need to prevent the imminent destruction of evidence in individual cases.[445] In summing up, Judge Roberts on behalf of the Court declared, in reversing the judgment of the California Court of Appeal:

---

[440] ibid.
[441] ibid, at 18.
[442] ibid.
[443] *Riley v California* 573 U.S. No. 13-132 (2014).
[444] ibid, at 20-21.
[445] ibid, at 12.

> Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life,"[446] The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple - get a warrant.[447]

The Court's decision in *Kyllo v United States* (2001), *United States v Jones* (2012) and *Riley v California* (2014) have moved in the direction of inhibiting 'the power of technology to shrink the realm of guaranteed privacy' [448] and restoring the Fourth Amendment to the role, envisaged for it by those who framed the Constitution, of preserving the authority of the people to limit unfettered government power to restrict their privacy rights. Findings such as those in *Kyllo*, *Jones* and *Riley* should not be seen as tending to deny to government the power to use technologies to conduct surveillance in the interests of national security or crime prevention. Instead they limit the exercise of that power to circumstances in which government can show probable cause. Ku points out that the Fourth Amendment 'does not prohibit the government from benefiting from new technologies; it merely defines when these technologies may be used.' [449]

Given the obvious weakness in current Supreme Court Fourth Amendment doctrine, and the freedom of government from so many Fourth Amendment restrictions, a number of legal scholars believe that enhanced protection of privacy rights can be achieved partly by remedying some of the deficiencies in the application of Fourth Amendment doctrine, and partly through the implementation of legislative, administrative and technological solutions. Balkin, for example, argues that new laws and technologies 'will probably do more to enforce the constitutional values underlying the Fourth Amendment

[446] *Boyd* v *United States*, 116 U.S. 616, 625 (1886) at 630.
[447] *Riley v California* 573 U.S. No. 13-132 (2014) at 2495.
[448] *Kyllo v United States* 553 U.S. 27, 2001 at 34.
[449] Shin Ray Ku, 'The Founder's Privacy: The Fourth Amendment and the Power of Technological Surveillance' 86 (2002) *Minnesota Law Review* 1325, 1366.

and the Due Process Clause.'[450] The Due Process Clause is part of the Fifth Amendment, which provides that:

> No person…….shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.[451]

At least four Supreme Court Justices in *United States v Jones* suggested that the proper scope of some privacy protection might be better left to Legislatures than to Courts. Justice Alito, writing for himself and three others, endorsed an approach taken by Kerr, who had argued that technological change is 'best regulated by legislative, not constitutional, pronouncements.'[452] The premise of Kerr's argument was that Courts tend to meet technological advances with a relatively modest and deferential Fourth Amendment.'[453] Murphy observes that Criminal Justice and Courts 'increasingly look to statutory resolutions of Fourth Amendment questions.'[454] Murphy points out that the U.S. code contains over 20 separate statutes that restrict both the acquisition and release of covered information. These statutes, largely enacted in the twentieth century, address matters vital to modern living, among them telephone calls and e-mail messages, and enlist a variety of procedural tools to serve as safeguards, ranging from requirements such as warrants and Court orders to subpoenas and demand letters. However, the problem from the perspective of privacy and the privacy/security balance is that one feature that all these statutes have in common is that each contains a provision exempting law enforcement from its general terms. Murphy notes that although 'these law enforcement exceptions appear in every generally applicable privacy statute on the federal books,' they have gained 'virtually no scholarly attention.' [455] More and more executive action is excluded from judicial review on the twin grounds of secrecy and

[450] Jack M. Balkin, 'The Constitution in the National Surveillance State, 93 (2008) *Minnesota Law Review* 1, 21.
[451] U.S. 5th Amendment.
[452] Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for* Caution' 102 (2004) *Michigan Law Review* 801, 805.
[453] ibid, 828.
[454] Erin Murphy, 'The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment and Statutory Law Enforcement Exemptions' 111(4) (2013) *Michigan Law Review* 485.
[455] ibid, 487.

efficiency. The Bush administration's secret NSA programme is one example; the explosion in the use of administrative warrants that require no judicial oversight is another.'[456]

The steady erosion of Fourth Amendment safeguards has come at an inauspicious time for privacy protection. Coinciding with this erosion, Executive surveillance activity has radically undermined the separation of powers doctrine: Executive branch decisions to adopt and implement advanced surveillance technologies are frequently made without either legislative or constitutional authorisation. The Snowden disclosures in 2013 that the NSA, the major U.S. surveillance agency, had long been secretly eroding the privacy rights of millions of U.S. citizens with government authorisation shows that government was prepared to render Fourth Amendment privacy protections redundant. What the public discovered from what Snowden revealed was that since 2006 the NSA had been collecting details of almost all domestic phone call records and other telephony metadata on foot of a dubious classified interpretation of Section 215 of the Patriot Act. Until 2013, the existence of this activity had been concealed from the general public. However, at least some members of Congress were aware of its existence and of the government's justification of it. Because it was classified, these legislators were prevented from disclosing it.

In the same year that Snowden disclosed details of the NSA programme, two technology experts, Pell and Soghoian, drew attention to another unregulated surveillance technology, commonly called StingRay, which had been in use for more than two decades, without attracting direct Congressional scrutiny.[457] This surveillance device 'enables the government, directly and in real time, to intercept communications data and detailed location information of cellular phone data which it would otherwise be unable to obtain without the assistance of a wireless carrier.'[458] This is clearly the kind of surveillance - never explicitly authorised by Congress - which, if regulated, would be subject to Fourth

[456] Jack M. Balkin, 'The Constitution in the National Surveillance State' 93 (2008) *Minnesota Law Review* 1, 23.
[457] Stephanie K. Pell and Christopher Soghoian, 'A Lot more than a Pen Register and Less than a Wiretap: What the Stingray teaches us about How Congress should approach the Reform of Law Enforcement Surveillance Authorities' 16 (2016) *Yale Journal of Law and Technology* 134, 134-137.
[458] ibid, 135.

Amendment scrutiny and implicate the rights of cell phone users. Given the unregulated use of surveillance technologies such as StingRay, based on 'problematic interpretations of existing statutes,' for years before they came to the attention of Congress, Pell and Sogohian argue that:

> [A]n authoritative, reliable procedure must be established to put Congress on notice about the functions, capabilities and historical use, if any, of new surveillance technologies and methods if the law is ever to keep pace with technological change.[459]

Experience suggests that the diminishing capacity of the Fourth Amendment to limit government recourse to warrantless surveillance of suspicious citizens at home and abroad is unlikely to be compensated for by a statutory regulation of such activity, as some commentators have suggested. The legislative response to the extensive abuse of privacy rights by the Nixon administration in the 1970s should stand as a warning that even well-intentioned reforming legislation designed to address privacy abuses by government can facilitate further privacy abuses. The history of FISA and its adjunct, the Foreign Intelligence Court, (FISC), provides ample evidence of this. Among the abuses perpetrated by FISC was its transmission of a compulsory order to a major telecommunications company to release all its telephone records.[460] It is reasonable to argue that the FISA legislation has created more problems for privacy than it has solved. Other efforts regulate mass breaches of privacy by government by means of legislation based on Fourth Amendment principles have proved ineffective or abortive, as shown earlier in this chapter.

However, the landmark Supreme Court decision in *Riley v California*[461] suggests that the Court is still prepared to affirm the central role the Fourth Amendment can play in privacy cases. In *Riley* the Court ruled, in an unanimous judgment, that cell phones are so vital to people's lives that the police must get a warrant to search them, just as they would need to do to search a person's home, a fundamental Fourth Amendment requirement. In the

---

[459] ibid, 169.
[460] The text of the leaked Order is available at: <https://epic.org/privacy/nsa/Section-215-Order-to-Verizon.pdf> accessed 26 March 2015.
[461] 573 U.S. 2014.

case of Riley, lower courts had been in dispute as to whether the Fourth Amendment allows the police to search the digital contents of such a phone. The verdict in *Riley* offers an interesting illustration of how courts take account of the way in which evolving technologies - in this case cell phone technology- require adjustment of, for example, Fourth Amendment rules to take account of the implications of new technologies. Many of these new technologies can radically change the balance between government surveillance power and the privacy rights of citizens. The Supreme Court's response to this situation is illustrated in the contrast between the finding in *United States v Robinson* [462] and that in *Riley v California*.[463] Both cases involved searches of a person on arrest. The verdict in *Robinson* was that the police were always entitled to conduct a complete search of a person on arrest.[464] In *Riley* the Court had to decide whether *Robinson* allowed police to search the contents of a cell phone that an arrestee had in his possession at the time of arrest. The *Riley* Court held that it did not. The reasoning of the Court was that searching a cell phone is much more invasive than searching for physical evidence that an arrestee might have on his or her person, for example, letters, pictures and books.[465] In *Riley*, the Court adjusted the Fourth Amendment rule in keeping with new technological facts. As Kerr points out, the equilibrium adjustment implicit in the *Riley* judgment 'recognizes that new technologies can change the balance between government power and civil liberties struck in an earlier age, and it allows courts to adopt rules in the light of technological changes or maintain that balance.'[466]

It still remains to be seen how Fourth Amendment law should adapt to the global nature of Internet surveillance. This is a particularly important issue in the light of the fact that the two decades since the mid-nineties have witnessed the globalisation of the Internet: at the end of 2013, less than 10% of the world's Internet traffic was attributable to U.S.-based users.[467] This raises significant questions about how the Fourth Amendment can apply to

[462] 414 U.S. 218 (1973).
[463] 134 S.Ct. 2473 (2014).
[464] *United States v Robinson* 414 U.S. 218 (1973).
[465] *Riley v California* 573 U.S. No. 13-132 (2014) at 2495.
[466] See Orin S. Kerr, 'An Equilibrium-Adjustment Theory of the Fourth Amendment' 125 (2011) *Harvard Law Review* 476, 487-88.
[467] Orin S. Kerr, 'The Fourth Amendment and the Global Internet' 67 (2015) *Stanford Law Review* 285, 286.

monitoring on a worldwide network where many users lack Fourth Amendment rights, and how Fourth Amendment law is to be applied to the monitoring of communications between people who have Fourth Amendment rights and those who do not. Kerr points out that almost all the cases and scholarship applying the Fourth Amendment to the Internet have been grounded on the assumption of domestic territoriality: in other words that all of the people, data and computers are physically located in the United States. Since that assumption no longer applies, the question must be framed in terms of how existing Fourth Amendment doctrine applied outside the borders of the U.S. The most important Supreme Court case applying the Fourth Amendment outside the U.S. is *United States v Verdugo Urquidez.*[468]

This case involved the search by U.S. law enforcement officials of two houses in Mexico owned by a Mexican drug baron, Verdugo Urquidez. The purpose of the search was to establish the defendant's involvement in a drug-trafficking conspiracy as well as the murder of a U.S. agent. By the time of the searches, the defendant had already been arrested in Mexico and transported to the U.S. to face charges in a U.S. Court. The defendant moved to suppress the evidence from the searches of his Mexican properties on the ground that these searches violated his Fourth Amendment rights.[469] The Court ruled that the defendant could not invoke the Fourth Amendment, which protects 'the right of the people,' a term which 'refers to a class of persons who are part of a national community' rather than to the world at large. This ruling was bolstered by historical evidence showing that 'the purpose of the Fourth Amendment was to protect the people of the United States against arbitrary action by their own government; it was never suggested that the provision was intended to restrain the actions of the Federal Government against aliens [such as Urquidez] outside of the United States territory.'[470] Thus the defendant was not one of 'the people' that the Fourth Amendment protects.[471]

17.0 Conclusion

When two major American cities became targets of terrorist acts on September 11, 2001, the Executive and public responses ensured that in the context of the

[468] 494 U.S. 259, 271 (1990).
[469] ibid, at 263.
[470] ibid, at 266.
[471] ibid, at 271-2.

data privacy/national security balance, the U.S. authorities would adjust the balance in favour of national security and lead to the adoption of legislation, including complex changes to laws governing intelligence surveillance and government guidelines, overriding previous checks and balances and intensifying the levels of secrecy surrounding surveillance practices. In particular, the passage of the Patriot Act in 2001 and of the FISA Amendment Act of 2008 ushered in an era of ambiguity and a further expression of Executive authority into the FISA framework. These were two of the factors that the Church Committee identified in 1976 as having contributed to Executive surveillance overreach, to the detriment of privacy.

The U.S. Administration may well have felt justified, in the immediate aftermath of the 9/11 attacks in acting on the principle that in times of national emergency, especially when there was no assurance that further terrorist events might not have been imminent, privacy protectors and the protection of national security were incompatible, or at least that restrictions on intelligence surveillance in the interest of privacy had to give way to whatever privacy-invasive measures the Administration deemed necessary for the protection of national security. Nevertheless, a question addressed in this chapter is whether the intensive surveillance measures undertaken post-9/11 proved effective in pre-empting terrorist attacks or identifying terrorist plots. The evidence adduced in the chapter leads to the conclusion that these measures had little, if any, influence on the defence of national security.

During the post-9/11 period, attempts by privacy advocates in Congress to moderate overbroad surveillance were frustrated, even after 2007, by which time the FISA Court and Congress had combined, in secret, to broaden FISA into a bulk surveillance statute. It was only after Edward Snowden exposed the extent of NSA activities that civil society and Congress, to a lesser degree, took the initiative in opposing bulk surveillance. The post-9/11 changes to FISA, embodied in the Patriot Act and the FISA Amendments Act, which undid the reforms of overbroad surveillance practices following the Church Committee Report, reforms which were incorporated in the original version of FISA, were finally addressed in the Freedom Act of 2015. As the analysis of the Freedom Act in this chapter suggests, it was an ambiguous statutory directive, based on

compromise, which failed to address adequately the inherent defects of the revised FISA, for example, the absence of an independent advocate with the role of presenting the case for privacy rights, and having a statutory right to question the basis for government requests for surveillance warrants, thus giving balance to the deliberations of the FISA Court (the FISC), whose proceedings are unduly influenced by Government. Further, the Freedom Act fails to address such significant problems as the NSA's practice of collecting enormous quantities of personal data on, and communications of, foreigners overseas, even when these are communicating with Americans. As the final section of the chapter suggests, the US Supreme Court's recent commentary on the legal problems posed by continuous, long-term surveillance in the context of the mosaic theory may indicate a lesser degree of reluctance on the part of the Court to become involved when national security is in question.

Chapter Four

Contrasting Europe and the United States. Perspectives on the Balance between Data Privacy and National Security

1.0 Contrasting Europe and the United States. Perspectives on the Balance Between Data Privacy and National Security.

When the protection of data privacy rights is at issue, as Sievert remarks, 'many legal commentators have written favourably about the European approach to data privacy protection as opposed to what they consider more intrusive U.S. laws.'[1] The general trend of this line of commentary is to suggest stark contrasts between the U.S. and European approaches to data protection. On the one hand, European privacy provisions and enforcement measures are regarded as constituting the 'most comprehensive and effective system [for the protection of human rights] in the world.'[2] The commentary contrasting the protective European approach to data privacy with the invasive U.S. approach fails to take account of the complexities of European law on the balancing of data privacy rights with the need for protecting the security of the state. In the wake of the 9/11 terrorist attacks in the U.S. and similar attacks in various states in Europe, the European Union's Data Retention Directive of 2006 mandated that internet, telecommunications and content providers retained metadata recording the identity, source, time, duration and destination of all communications [3] for six to twenty-four months [4] to assist intelligence services to combat serious crime and terrorism. This meant that every EU citizen, whether under suspicion of terrorist offences or not, was liable to have the privacy of his or her communications retained and surveilled without knowing that this was being done.

Another aspect of European security law should be taken into account when comparisons are being made between European and United States laws and

[1] Ronald J. Sievert, 'Time To Rewrite The Ill-Conceived And Dangerous Foreign Intelligence Surveillance Act of 1978' 31 (2014) *National Security Law Journal* 47, 82.
[2] Jeffrey A. Brauch, 'Human Rights Protections In The Post-9/11 World' *Quinnipiac Law Review* 31 (2013) 339.
[3] Directive 2006/24/EC Of The European Parliament And Of The Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC O.J. (L 105/54), Article 5(1) 2(c)
[4] ibid, Article 5(b), 2(c).

practices relating to balancing data protection and national security. This is that each European State is responsible for the maintenance of law and order and safeguarding its own national security,[5] at the same time complying with the privacy safeguards embodied in Article 8 of the European Convention on Human Rights. A margin of appreciation is afforded to the competent national authorities in assessing what is necessary, particularly in relation to matters of national security, although each State's laws may be challenged before, and ruled upon, by the European Court of Human Rights.

Even apologists for U.S. surveillance practices concede that U.S. Intelligence collects bulk metadata, bulk content of Internet messages outside the U.S. and various other communications. They also acknowledge that the degree of NSA surveillance may also vastly exceed that of any other free world intelligence agency and in addition that the same agency resorts to the covert use of 'back doors' in communications products to facilitate interception and code-breaking.[6] A *Washington Post* article, written in the immediate aftermath of the Snowden revelations, details the findings of an international audit of the NSA's domestic surveillance activities. The findings revealed that the NSA had broken privacy rules or exceeded its legal authority thousands of times per year since Congress granted the agency new powers in 2008, according to an internal audit and top-secret documents. Most of the breaches related to unauthorized surveillance of Americans or foreign intelligence targets in the United States, both of which are restricted by statute and executive order. They ranged from significant violations of law to typographical errors that resulted in unintended interception of U.S. e-mails and telephone calls.[7]

A Report by the Electronic Frontier Foundation revealed that the NSA had been at the forefront of American technical efforts relating to operations designed to combat international terrorism and other U.S. national security

[5] Kaatlo Tuori, 'A European Security Constitution' in Massimo Fichera and Jens Kremer, *Law and Security in Europe: Reconsidering the Security Constitution* (Intersentia, 2013) 39-84, 59.
[6] David Bender, 'E.U. or U.S. : which has more actual privacy? 21(1) (2015) *Computer Law and Security Review* 18.
[7] Barton Gellman, 'NSA Broke Privacy Rules Thousands of Times Per Year, Audit Finds' *The Washington Post* (August 15, 2013) <https://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html?utm_term=.65c406d3aadf> accessed 10 January 2017.

objectives as early as 2001. The Report noted that the NSA, with assistance from major telecommunications carriers, 'has engaged in a massive illegal dragnet surveillance of domestic communications and communications records of millions of Americans.'[8]

2.0 Conflicting Views on overall privacy protection levels in the U.S. and Europe

In a comparative analysis of privacy rights in the U.S., Canada and Europe, James, in 'the light of the intrusiveness and obvious potential for abuse by agencies such as the NSA,' argues that 'a reconsideration of nationwide privacy policy is in order if there remains any desire to protect the private data of citizens.'[9] The reconsideration of U.S. privacy policy favoured by James is one involving the entrenchment of the right of privacy into American law. It is significant that the way chosen by James to accomplish this goal is 'by carefully drafting a proposed amendment to the U.S. Constitution which unambiguously proclaims the right to privacy *à la Article 8* of the ECHR.'[10] This suggestion implies that existing U.S. Constitutional law does not provide adequate protection for privacy rights, data privacy included, since the principal legal document in this context, the U.S. Constitution, makes no express mention of a right to privacy, and as a consequence of this, 'the U.S. concept of an assertable and substantive right to privacy continues to be divided and extracted by the Supreme Court in particular from a number of constitutional amendments, the most relevant of these, in the context of data privacy, being the Fourth Amendment, which affirms that

> The right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures, shall not be violated and no warrants shall issue, but upon probable cause, supported by Oath

[8] 'NSA Spying on Americans' *Electronic Frontier Foundation* <https://www.eff.org/nsa-spying> accessed 9 January 2017.

[9] Michael C. James, 'A Comparative Analysis of the right to Privacy in the United States, Canada and Europe' 29 (2014) *Connecticut Journal of International of Internal Law* 259, 297.

[10] ibid. Amending the U.S. Constitution via an Amendment would be a challenging process. The authority to amend the Constitution is derived from Article V of the Constitution. This Article provides that an Amendment may be proposed either by the Congress with a two-thirds majority vote in both the House of Representatives and the Senate or by a Constitutional Convention called for by two-thirds of the State legislatures. The U.S. President does not have a conational role in the amendment process. A proposed Amendment becomes part of the Constitution as soon as it is ratified by three-quarters of the Senate.

> or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

However, as interpreted by the Courts, the Fourth Amendment does not offer the kind of protection to data privacy that would be necessary to prevent the massive, often illegal, intrusiveness on the part of government entities identified in the reports referred to above. This issue will be dealt with in the next section of this chapter.

Bender, in his paper on whether the citizens of the EU or the U.S. have more 'actual privacy,' cited above, refers to a detailed comparison of actual EU and U.S. privacy levels reported in April 2006 by the Ponemon Institute and sponsored by the author's law firm, which found overall privacy levels to be somewhat higher in the U.S. than in the EU.[11]

There have been changes in both the U.S. and the EU since 2006. For example, the 2006 EU Data Retention Directive had the effect of tilting the data protection/national security balance in Europe in favour of the latter. During the same period, the data breach notification laws which took hold in the U.S. had the opposite effect on the balance in that jurisdiction. Bender, seeking to defend the U.S. privacy regime, and to present a positive view of privacy in the U.S. compared to that in the EU, points out that in the EU, national security matters are dealt with at Member State level.[12] This gives him an opportunity to draw attention to what he terms 'the extensive judicial approval and legislative oversight procedures built into the [U.S.] Foreign Intelligence Surveillance Act.' This provided him with a basis for saying that few countries provide for the kind of judicial authorisation and oversight of foreign intelligence counterterrorism investigations built into the American framework.[13]

---

[11] David Bender, 'E.U. or U.S. : which has more actual privacy? 21(1) (2015) *Computer Law and Security Review* 18.

[12] ibid, 19. Article 3(2) of Directive 95/46EC reads: 'This Directive shall not apply….. to processing operations concerning public security, defence, state security.'

[13] ibid. For a contrary view of FISA see Chapter 2, Section 7.0 of this thesis (The Problems with FISA).

Bender relied on the Maxwell and Wolf Reports, cited below, in support of the claim that '[t]he EU critics of U.S. privacy protections would be well-advised to take stock of their own countries' national security access to personal data.'[14] On this issue, Peltz takes a similar line, in the context of European responses to the Snowden revelations. Peltz claims that 'when European arguments turn to Snowden, they smack of disingenuity'……it strains credulity to imagine that European security officials are not engaged in their own vigorous intelligence gathering.'[15] As an example, he mentions a report in *Der Spiegel* that the U.S. National Security Agency 'shared its questionably gotten gains with the German intelligence service.'[16]

In two studies, the key national security surveillance law provisions and practices in the major European powers and in a number of non-European powers, including the U.S., Maxwell and Wolf provide a useful corrective to some of the more extravagant comparisons frequently drawn between U.S. and European surveillance practices. These studies were based on an examination of contributions from Privacy International, law review articles and instructive court decisions.[17]

Maxwell and Wolf's 2012 survey dispelled the notion that the U.S. Government had greater powers of access to personal data in the cloud than governments elsewhere, finding that 'even European countries with strict privacy laws also have anti-terrorism laws that allow expedited government

[14] ibid.
[15] Richard J. Peltz-Steele, 'The Pond Between: Differences In The US-EU Data Protection/Safe Harbour Negotiation' 19(1) (2015) *Journal of Internet Law* 14, 23.
[16] ibid, 21, fn 123, citing: 'Prolific Partner': German Intelligence Used NSA Spy Program," Spiegel, July 20, 2013, <http://www.spiegel.de/international/germany/german-intelligence-agencies-used-nsa-spying-program-a-912173.html.>
[17] The first study was: Winston Maxwell and Christopher Wolf, 'A Global Reality: Government Access to Data in the Cloud: A Comparative analysis of ten international jurisdictions' (23 May, 2012) *A Hogan Lovells White Paper* 1 <http://www.hldataprotection.com/uploads/file/Revised%20Government%20Access%20to%20Cloud%20Data%20Paper%20(18%20July%2012).pdf> accessed 7 January 2017. The second study was Winston Maxwell and Christopher Wolf, 'A Sober Look at National Security Access to Data in the Cloud. Extravagant Claims About U.S. Access That Ignore Access by Foreign Jurisdictions' (May 22, 2013) *A Hogan Lovells White Paper* 1 <http://www.hldataprotection.com/files/2013/05/A-Sober-Look-at-National-Security-Access-to-Data-in-the-Cloud.pdf> accessed 7 January 2017.

access to Cloud data.'[18] The same survey also found that it is not possible 'to isolate data in the Cloud from government access based on the physical location of the Cloud services provider or its facilities,' and that it is incorrect 'to assume that in the United States government's access to data in the Cloud is greater than that of other advanced economies.'[19] The report of Maxwell and Wolf's 2012 survey drew attention to the fact that in addition to domestic legal frameworks facilitating governmental access to data within a country, Mutual Assistance Treaties are in effect 'between and among countries around the world' which 'provide governments with the ability to access data stored in one jurisdiction but needed for lawful investigative purposes in another.'[20]

3.0 National Security Surveillance in Germany, the U.K. and the U.S.

Maxwell and Wolf's survey of key national security surveillance law provisions and practices in two major European States, Germany and the United Kingdom yield interesting results when comparisons and contrasts between U.S. and European attitudes to data privacy and national security protections are being discussed. In national security cases, German intelligence agencies are allowed to monitor letters, telecommunications and conversations, with targeted collection of personal data to investigate serious threats to the security of the Sate.[21] They are also permitted to gather relevant information about other countries that are considered important to the national security policy of Germany.[22]

Germany does not require judicial review before surveillance is authorised, as the U.S. does under FISA and does not demand that the government should show probable cause. Instead, the responsible Federal Ministry or Federal State

[18] Data in the Cloud: A Comparative analysis of ten international jurisdictions' (23 May, 2012) *A Hogan Lovells White Paper* 1<http://www.hldataprotection.com/uploads/file/Revised%20Government%20Access%20to%20Cloud% 20Data%20Paper%20(18%20July%2012).pdf> accessed 7 January 2017.
[19] ibid, 2.
[20] ibid.
[21] Winston Maxwell and Christopher Wolf, 'A Sober Look at National Security Access to Data in the Cloud. Extravagant Claims About U.S. Access That Ignore Access by Foreign Jurisdictions' (May 22, 2013) *A Hogan Lovells White Paper* 1, 7-8 <www.hldataprotection.com/files/2013/05/A-Sober-Look-at-National-Security-Access-to-Data-in-the-Cloud.pdf> accessed 7 January 2017. See also Paul M. Schwartz, 'Systematic government access to private-sector data in Germany' *International Data Privacy Law* (2) 4 (2012) 289, 291.
[22] Winston Maxwell and Christopher Wolf, 'A Sober Look at National Security Access to Data in the Cloud. Extravagant Claims About U.S. Access That Ignore Access by Foreign Jurisdictions' (May 22, 2013) *A Hogan Lovells White Paper* 1, 8.

Authority orders the surveillance measures. Furthermore, if German intelligence agencies request data from Cloud service providers, these providers are prohibited from disclosing to their customers that they provided such information to the government.[23] The Federal office of Criminal Investigation (BKA) has broad authority in investigations concerning national security or terrorism. The BKA, for example, is permitted to use a computer virus, the so-called *Bundestrojaner* (the 'Federal Trojan') to search IT systems, monitor ongoing communications and collect communication traffic data without the knowledge of data subjects or service providers.[24] While the BKA must obtain a court order to use the 'Federal Trojan,' systems on which this is deployed, which include Cloud service providers, are not aware of its deployment.[25] In the U.S. by contrast, parallel provisions are more restrictive: under the terms of the FISA Amendment Act, Cloud service providers receive notice of acquisition orders handed down by the FISC and are given an opportunity to contest these orders. On the other hand, there are similarities between German and U.S. oversight of the activities of their respective intelligence agencies. In Germany, intelligence agencies must report to a Parliamentary Control Panel on their activities and provide documentation on these. In this way, the Panel occupies a similar role to U.S. Government Oversight.[26] Schwartz points out that the German Parliamentary Control Panel appoints a non-judicial body called the G-10 Committee, which supervises the processing of personal data and decides on the 'permissibility and necessity' of surveillance conducted by the intelligence agencies.[27]

In the United Kingdom, the Regulation of Investigatory Powers Act, 2000 (RIPA) allows a Secretary of State to authorise the interception of communications in the interests of national security.[28] Interception warrants relating to foreign intelligence are generally issued by the Foreign Secretary.

[23] ibid.
[24] ibid, 8. See also John Leyden, 'German States defend use of 'Federal Trojan' (12 October, 2011) *The Register* <http://www.theregister.co.uk/2011/10/12/bundestrojaner/> accessed 8 January 2017.
[25] Winston Maxwell and Christopher Wolf, 'A Sober Look at National Security Access to Data in the Cloud. Extravagant Claims About U.S. Access That Ignore Access by Foreign Jurisdictions' (May 22, 2013) *A Hogan Lovells White Paper* 1, 8.
[26] ibid, 8; See also Paul M. Schwartz, 'Systematic government access to private-sector data in Germany' *International Data Privacy Law* (2) 4 (2012) 289, 297.
[27] Paul M. Schwartz, 'Systematic government access to private-sector data in Germany' 2(4) (2012) *International Data Privacy Law* 289, 298.
[28] Regulation of Investigatory Powers Act, 2000 (RIPA), Section 5(3).

Although a warrant issued under these provisions must be 'proportionate' to the intended purpose, intercepted information is expressly excluded from legal proceedings to prevent interception methods from being revealed. The fact that the U.K. courts take no part in the authorisation or review of such interceptions contrasts with U.S. practices: in the U.S., under the terms of FISA, the authorisation or review of such interceptions is left to the FISC a judicial body and to another judicial body, the FISA Court of Review (the FISCR). While in the U.K. there is an Investigatory Powers Tribunal to hear complaints under RIPA, composed of five senior members of the legal profession, the absence of a requirement to provide *post facto* notification to those who have been placed under surveillance, suggests that those who might have cause to bring claims to the Tribunal will not in practice do so.[29] Under the provisions of RIPA, Cloud Computing service providers are likely to meet the definition of 'telecommunications operator.'[30]

In addition to providing for the interception of communications, RIPA also establishes mechanisms through which law enforcement entities may require the disclosure of 'communications data' (traffic, usage and subscriber data) from public and private telecommunications operators in the interest of national security.[31] In these circumstances, telecommunications operators receiving a disclosure request are obliged to comply or risk being subject to civil enforcement proceedings.[32] There is also provision for government access to private-sector data through voluntary agreements with operators of databases and other companies. Sections 28 to 29 of the Data Protection Act 1998 authorise such agreements for national security purposes. Section 19 of the Counter-Terrorism Act of 2008 authorises communications operators to disclose information to any of the Intelligence services for the purposes of the

[29] Winston Maxwell and Christopher Wolf, 'A Global Reality: Government Access to Data in the Cloud: A Comparative analysis of ten international jurisdictions' (23 May, 2012) *A Hogan Lovells White Paper* 1, 8. <http://www.hldataprotection.com/uploads/file/Revised%20Government%20Access%20to%20Cloud%20Data%20Paper%20(18%20July%2012).pdf> accessed 7 January 2017. See also Ian Brown, 'Systematic government access to private-sector data in the United Kingdom' 4(2) (2012) 230, 235.

[30] Section 25 of RIPA defines 'telecommunications operator' as 'a person who provides a telecommunications service,' while Section 2(1) defines 'telecommunications service as 'any system (including the apparatus comprised in it) which exists (whether wholly or partly in the United Kingdom or elsewhere) for the purpose of facilitating the transmission of communications by any means involving the use of electrical or electro-magnetic energy.'

[31] RIPA, Section 22.

[32] RIPA, Section 22(6), (8).

exercise by those services of any of their functions. This removes any obligation of confidentiality or other restriction on disclosure to the intelligence agencies.[33]

The authors of the 2012 White Paper - A Sober Look - claim, on the basis of their research findings, that the premise that the U.S. law enforcement agencies are likely to violate their own laws, or are more likely to do so than their counterparts in Europe, including Germany and the U.K., is unsubstantiated.[34] The first claim, however, is questionable. For one thing, the findings of the Church Committee, based as these are on credible evidence, have established that U.S. law enforcement agencies, in particular, the NSA, consistently violated the laws governing their operations, violating the privacy rights of U.S. citizens at a fundamental level, albeit under Presidential direction, and in the case of its controversial programmes its Deputy Director considered its legality irrelevant.[35] It is also true that, based on the evidence adduced in the White Paper, that German, U.K. and French Intelligence Agencies have exploited their formidable counterterrorism capabilities,[36] sometimes using legally-dubious surveillance methods, for example, monitoring ongoing communications, without the knowledge of data subjects or service providers, without judicial oversight or judicial review and in the case of Germany, spying on their own head of government.[37]

Based on the evidence discussed so far, the significant contrasts between U.S. and European principles and practices relating to balancing data privacy protection against the demands of national security, the most significant contrasts are exhibited in two areas: the constitutional and the judicial. Taking

[33] Ian Brown, 'Systematic government access to private-sector data in the United Kingdom' 4(2) (2012) 230, 235.
[34] Winston Maxwell and Christopher Wolf, 'A Sober Look at National Security Access to Data in the Cloud. Extravagant Claims About U.S. Access That Ignore Access by Foreign Jurisdictions' (May 22, 2013) *A Hogan Lovells White Paper* 1, 9. <www.hldataprotection.com/files/2013/05/A-Sober-Look-at-National-Security-Access-to-Data-in-the-Cloud.pdf> accessed 7 January 2017.
[35] See Chapter of this thesis dealing with The Privacy/Security Balance in the U.S. pre-9/11, in particular the section headed 'Two Data/Privacy/National Security Balancing Systems Pre-9/11: The Influence of NSA Surveillance Activity. The Legal and Actual Balances, page 38 onwards.
[36] See Steven Erlanger, 'Fighting Terrorism, French-style (*The New York Times*, March 30, 2013).
[37] 'Germany Spied on Friends and Vatican' *Spiegel Online* (November 7, 2015) <http://www.spiegel.de/international/germany/german-bnd-intelligence-spied-on-friends-and-vatican-a-1061588.html> accessed 9 January 2017.

the constitutional area first, it is clear that in both European systems, the Council of Europe and the European Union, and in many European states, the right to privacy protection has a firm Constitutional foundation. In contrast, the U.S. Constitution provides an extremely limited foundation for this right. In the judicial area, a similar degree of contrast applies. When national security is in question, and especially when U.S. Intelligence agencies interfere with citizens' data privacy by implementing overbroad surveillance measures, the Courts have exhibited a reluctance to intervene to affirm privacy rights. On the other hand, the major European Courts, the ECtHR and the CJEU, have shown no such reluctance. A recent example is the striking down by the CJEU of the EU Data Retention Directive of 2006 for being excessively privacy-invasive.

When it comes to the activities of the intelligence services in the two jurisdictions, whatever evidence there is suggests that the practices of these services are largely similar in both jurisdictions. Whatever distinction there is, is one of degree rather than of kind. What distinguishes the U.S. from Europe in this regard is that U.S. intelligence services such as the NSA enjoy vastly greater scope for privacy-invasive activities than do their European counterparts. No European State Intelligence services are as well-funded or as technologically sophisticated as the NSA; its nearest competitor in Europe is the British GCHQ, with which it shares intelligence data. According to Bamford, the leading authority on the NSA, it has tens of thousands of employees and a budget in the billions and 'is the largest, most costly spy organisation the world has ever known.'[38] However, differing models of government in the U.S. and Europe have a major bearing on surveillance practices for the purposes of privacy rights analysis. In the U.S., post-9/11, it was possible for the President to issue a secret directive to the NSA to undertake a programme of mass surveillance and for the President to claim that any disclosure of the NSA database constituted a threat to national security. This database is protected by the 'State Secrets' privilege, which bars information that would adversely affect national security.[39] Bignami points out that under U.S. law the NSA antiterrorism database might very well be legal,

[38] James Bamford, 'The Shadow Factory: the NSA from 9/11 to the Eavesdropping on America' (Anchor Book, 2009) 1; Siobhan Gorman, 'NSA's Domestic Spying Grows as Agency Sweeps Up Data,' (Wall Street Journal, March 10, 2008).

[39] See Francesca Bignami, 'European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining,' 48 3(3) (2007) *Boston College Law Review* 609, 650.

particularly in the light of the President's claim that post-9/11 he enjoyed absolute discretion in employing whatever measures he chose to fight terrorist threats, but under European law such a database would clearly be illegal.[40] In France and Germany, by contrast to the U.S., 'a government proposal for data mining, even intelligence-related data mining, would have to be submitted to an independent regulator for review.'[41]

Bignami has drawn attention to German länder case involving data mining by police forces in the State of North-Rhine Westphalia in the aftermath of the 9/11 attacks which underlines the nature of the contrast mentioned above.[42] The context of this case is that in Germany, the police have 'preventive' powers to thwart future threats to state security. In North-Rhine Westphalia, the police forces, acting on foot of these powers, undertook a co-ordinated effort to collect and search data sets based on a common terrorist profile: male, aged between eighteen and forty, student or former student, Islamic faith, and citizenship or birthplace in a country with a predominantly Islamic population. The results of these searches were transmitted to the German Federal Police Office which matched the names against other data sets on other characteristics associated with terrorism, thereby narrowing the pool of possible suspects, and sent the names of suspects back to the Länder police for possible surveillance and questioning.[43] A complaint brought against the state of North-Rhine Westphalia resulted in a finding by the German Constitutional Court (the Bundesverfassungsgericht) that the data-mining programme in question was unconstitutional.[44] The Court found that the national security purpose of the programme was legitimate and that the data mining was an appropriate and necessary means of achieving that purpose.[45] However, the Court concluded that the burden on the right of informational self-determination (i.e the right to informational privacy) was not proportionate to the public ends being pursued (i.e the need to thwart terrorist threats to national security).[46] The data-mining

[40] ibid, 609.
[41] ibid, 655.
[42] Fransesca Bignami, 'European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining,' 48 3(3) (2007) *Boston College Law Review* 609, 654, fn 285.
[43] Bundesverfassungsgericht [BVerfC], Apr. 4, 2006, 1 BVerfGE <http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2006/04/rs20060404_1bvr051802.html> at para. 63.
[44] ibid, paras 68-75.
[45] ibid, paras 81-86.
[46] ibid, at para 68.

in question in this case would be acceptable only if there were concrete facts demonstrating an immediate and concrete risk (concrete 'gefahr') of a terrorist attack.[47] The fact that the police data-mining had been prompted by a widespread fear of a terrorist attack following September 11 did not, according to the Court, constitute a sufficient reason to intrude on the privacy right. In the U.S., a widespread fear of a terrorist attack post-9/11 was considered sufficient for the President to launch a massive surveillance programme which intruded on an ongoing basis on the privacy rights of millions of Americans.

4.0 The Role of the Fourth Amendment in Protecting the Data Privacy Rights of Americans

In U.S. law. the Fourth Amendment is the critical constitutional provision regarding telecommunications surveillance, for controlling and preventing abuses of privacy rights by government and its agents. Over time, however, the role of the Fourth Amendment as protector of the privacy rights of citizens has been significantly reduced, as government collection and use of personal data is now deemed to fall outside the limits of its protection. The U.S. Supreme Court, for example, when confronted with new practices and new technologies, has limited Fourth Amendment privacy protections, while at the same time Congress has neglected to develop an appropriate legal framework of data protection to compensate for this limitation.[48] Other factors limiting Fourth Amendment protections have been the rise of a powerful administrative state increasingly preoccupied with the mass surveillance of its citizens, and the centralisation of mass surveillance powers in the hands of a largely unaccountable Executive invoking the pre-eminence of State security as a national imperative and proclaiming an ongoing state of war as a justification for the inevitable restriction of privacy rights. Strong privacy protections require strict limits on the powers of government to gather personal data; the Presidential assumption of power to engage in warrantless surveillance inevitably limits Fourth Amendment protections of privacy.

[47] ibid, at para 158.

[48] See Daniel J. Solove, *The Digital Person: Technology and Privacy in the Information Age* (New York University Press, 2004) 202; Solove notes that the Supreme Court has limited Fourth Amendment protections when faced with new practices and new technologies. Paul Schwartz, 'Data Processing and Government Administration: The Failure of the American Legal Response to the Computer' (1992) 43 *Hastings Law Journal* 1321; Jack M. Balkin, 'The Constitution in the National Surveillance State,' 93 (2008) *Minnesota Law Review* 1.

In 1803, Chief Justice Marshall declared the basic principle that the federal judiciary 'is supreme in the exposition of the law of the Constitution.'[49] In contemporary U.S.A., constitutional decisions of the Supreme Court are accepted as final.[50] The finality of the Supreme Court's authority has been affirmed in a variety of versions. Justice Jackson declared that 'We [the Supreme Court] are not final because we are infallible, but we are infallible only because we are final.' [51] A more demotic version is that of Charles Evans Hughes, later Chief Justice, in an address given in 1908: 'We are under a Constitution, but the Constitution is what the judges say it is.'[52] If it is accepted that the Constitutional decisions of the Supreme Court are final, then current Fourth Amendment doctrine is what the Supreme Court says it is. This means that much government collection and use of personal data is now outside the protection of the Fourth Amendment, as the Supreme Court construes it.[53]

5.0 The Fourth Amendment: An Inadequate Defender of Privacy

The weakness of the Fourth Amendment as a privacy-defensive mechanism resides in the large number of exceptions to its application when data protection is in question. Many of these exceptions have been developed as part of Supreme Court jurisprudence. One of these, the third-party doctrine, was first developed by the Court in *United States v Miller*,[54] which held that there are no Fourth Amendment protections for data voluntarily disclosed to third parties, or stored in the control of third parties.[55] In a further elaboration of the third-party doctrine, the Court in *Smith v Maryland*[56] held that callers lack a Fourth Amendment interest in the numbers they dial because they voluntarily turn over those data to their telephone providers.[57] The government has placed particular reliance on *Smith v Maryland*[58] in defence of the constitutionality of its unfettered metadata collection and analysis. The basis of

[49] William W. Van Alstyne, 'A Critical Guide to Marbury v Madison' 1(1) (1969) *Duke Law Journal* 1, 2.
[50] Robert W. Bennett, 'Objectivity in Constitutional Law' 132 (1984) *University of Pennsylvania Law Review* 445.
[51] *Brown v Allen* 344 U.S. 443, 540 (1953).
[52] Cited by William W. Van Alstyne, 'A Critical Guide to Marbury v Madison,' 1(1) (1969) *Duke Law Journal* 1, 2.
[53] Jack M. Balkin, 'The Constitution in the National Surveillance State,' 93 (2008) *Minnesota Law Review* 1, 19.
[54] 425 U.S. 435, 446 (1976).
[55] ibid.
[56] 422 U.S. 735 (1979).
[57] ibid.
[58] ibid.

this defence is that since callers have no right to privacy in their metadata (information about a phone-call - giving the who, what, when and how long), the National Security Agency enjoys a constitutional right to gather, store and analyse any amount of telephony metadata over any period of time.

Additionally in *United States v Miller*,[59] the Supreme Court has held that there is no expectation of privacy in business records and information that people give to banks and other businesses.[60] In the digital age, as Balkin points out, this amounts to a vast amount of personal information not protected by the Fourth Amendment.[61] Furthermore, since most e-mail messages are copied onto privately held servers, the third-party doctrine deprives them of the protection of the Fourth Amendment. In the technological era, the Supreme Court doctrine that one cannot have a reasonable expectation of privacy in information given to third parties, 'or made accessible to the public,'[62] covers a huge range of activity. For example, commercial interactions are known to credit card companies, financial records are in the possession of banks; telephone calls and e-mails involve giving telecommunications companies the numbers and e-mail addresses necessary to route the information appropriately, and the location of a cell phone may be known to the phone company at all times. If the Courts decide that all this information falls outside the scope of the Fourth Amendment protection, then Government is free to compile and analyse it free from Constitutional scrutiny.[63] Alphran elaborates on the way in which the U.S. Courts have progressively weakened the force of the Fourth Amendment as the principal foundation upon which the protection of personal data is based: 'As Courts expand the special needs doctrine in support of the government's interests in combating terrorism, the Fourth Amendment's privacy interests of the American public continue to diminish.'[64] Alphran notes that post-9/11 in particular, the Federal Courts have embraced an unprecedented expansionist approach in Fourth Amendment cases with regard

[59] 425 U.S. 435, 446 (1976).
[60] ibid.
[61] Jack M. Balkin, 'The Constitution in the National Surveillance State,' 93 (2008) *Minnesota Law Review* 1, 19.
[62] *California v Greenwood* 486 U.S. 35, 40-41 (1988).
[63] See (----------) 'Data Mining, Dog Sniffs and the Fourth Amendment' *Harvard Law Review* 128 (2014) 691, 691-2.
[64] Derek M. Alphran, 'Changing Tides: A Lesser Expectation of Privacy in a Post-9/11 World' 13(1) (2009) *Richmond Journal and The Public Interest* 89, 120.

to many exceptional doctrines such as 'exigent circumstances' and 'special needs' in national security matters.'[65] Krotosznski is pessimistic about the prospects of privacy protection in the U.S.; remarking that the notion of privacy generally runs against the federal government, he points to a consequence of this, that 'very little data privacy protection - even of a sort that would probably not implicate the First Amendment - exists at either the federal or State level,' and that instead, 'to a remarkable - indeed unwise - degree, in the United States, we rely almost entirely on market competition to ensure a modicum of privacy protection for our personal information, data and Internet browsing habits.'[66]

In his seminal article on the Fourth Amendment, Armstrong observes that 'for clarity and consistency, the law of the Fourth Amendment is not the Supreme Court's most successful product.'[67] However, Amsterdam was careful to add that 'the Fourth Amendment is not clear. The work of giving concrete and contemporary meaning to that brief, vague, general, unilluminating text written two centuries ago is inescapably judgemental'.[68] Numerous scholars have complained that 'the Court has produced a series of inconsistent and bizarre results that it has left entirely undefended.'[69] Wassterstrom and Seidman also draw attention to 'the remarkable divergence' between two separate lines of Fourth Amendment jurisprudence. On some occasions, 'the Court uses a rigid, formal structure for Fourth Amendment analysis,' and makes no effort to 'weigh or assess the underlying interests at stake,' while on other occasions, 'for reasons that are never made clear, the Court abandons this formal approach and instead employs a free-wheeling, fact-specific balancing of costs and benefits.'[70]

It is not surprising that legal scholars have been highly critical both of the way in which the Fourth Amendment is formulated and the way in which the Supreme Court had dealt with it. One line of criticism is that the Amendment is

[65] ibid, 120-21.
[66] R.J. Krotoszynski, 'The Polysemy of Privacy' 88(3) (2013) *Indiana Law Journal* 881.
[67] Anthony G. Amsterdam, 'Perspectives on the Fourth Amendment' *Minnesota Law Review* 58 (1974) 4(3) 349-477, 349.
[68] ibid, 353-4.
[69] Silas J Wasserstrom and Louis Michael Seidman, 'The Fourth Amendment as Constitutional Theory' 77 (1988-89) *Georgetown Law Journal* 19, 29.
[70] ibid, 22.

a mass of contradictions and obscurities that has so ensnared the judges of the Supreme Court that every effort they make to extract themselves finds them more profoundly perplexed.[71] While seemingly ignoring the issues posed by the text of the Fourth Amendment, the Court has been preoccupied with resolving problems about which the text is silent.[72] The Supreme Court's view of what is open and what is closed under the Amendment is difficult to comprehend. For example, in its view, what one takes upon the public roads is deemed private, and protected by the Fourth Amendment, to the extent that is not exposed to view, but what one does on private property that is fenced, posted (and presumably guarded) is not protected by the Fourth Amendment because it is 'open.' Also, that people should receive more protection in a taxi than on land they own, care for and seek to keep private for themselves is a proposition difficult to defend.[73]

6.0 The Courts and the Interpretation of the Fourth Amendment

Since the 1960s, as Barr points out, the Fourth Amendment has been consistently whittled down in favour of the government in a variety of ways.[74] Balkin, who believes that the Fourth Amendment should function as the most important constitutional provision for controlling and preventing abuse of power in the national surveillance state, observes that 'Courts have largely debilitated the Fourth Amendment to meet the demands of the National Security State.'[75] In *Katz v U.S.* [76] the Supreme Court formulated both a subjective and objective 'reasonable expectation of privacy' and in so doing mandated that 'the privacy exception be one that society is prepared to regard as reasonable.'[77] Barr observes that less than a generation after *Katz*, the Supreme Court, employing the 'reasonable expectation of privacy' formula in a

[71] Craig M. Bradley, 'Two Models of the Fourth Amendment,' *Michigan Law Review* 83 (1985) 1468.
[72] Silas J Wasserstrom and Louis Michael Seidman, 'The Fourth Amendment as Constitutional Theory,' 77 (1988-89) *Georgetown Law Journal* 19, 26.
[73] Stephen Allan Saltzburg, 'Another Victim of Illegal Narcotics: The Fourth Amendment (As Illustrated by the Open Fields Doctrine) 48 (1986) *University of Pittsburgh Law Review* 1 20. See also 'Court fails to accept the opportunity this case presents……. to develop a clear [Fourth Amendment] doctrine' - Blackmun dissenting in *United States v Chadwick*, 433, U.S. 1, 17 (1977); 'Courts are destined to create absurdities in search warrant law as long as they contribute to build upon absurdity' - Joseph D. Grano, 'Rethinking the Fourth Amendment Warrant Requirement' *American Criminal Law Review 19* (1982) 1603, 605.
[74] Bob Barr, 'Post 9/11 Electronic Surveillance Society Severely Undermining Freedom' 41(4) (2007) *Valparaiso University Law Review* 1383-1412, 1385.
[75] J. M. Balkin, 'The Constitution in the National Surveillance State' 93 (2008) *Minnesota Law Review* 1, 19.
[76] 389 U.S. 347 (1967).
[77] ibid, at para 361.

trilogy of cases, set in motion 'a true loosening of the strictures of the Fourth Amendment.' [78] What the decisions in these cases 'did, in practical terms, was to limit the "persons and places searched" provision to an ever-shrinking number of people and circumstances.'[79] 'It is,' as La Leve remarks in reference to cases such as these, 'almost as of a majority of the Court was hell-bent to seize any viable opportunity to define more expansively the constitutional authority of law enforcement officials.'[80]

Maclin makes a similar point: 'In effect, the Court has adopted the outlook of a fox in defining the rules that will govern the hen-house.' [81] The findings of the Court in the cases considered by Barr sound new depths of triviality: *Salvucci* holding that the Fourth Amendment rights should be analysed by asking not merely whether the defendant had a possessory interest in the items seized, but whether he had an expectation of privacy in the area searched; and *Raskas* holding that there was no showing that mere passengers in a car had any legitimate expectation of privacy in the glove compartment or area under the seat of the car.

The Supreme Court deems that citizens have a lesser 'expectation of privacy' if they communicate by e-mail as opposed to telephone, simply because e-mail transmissions travel through an ISP over which they have no control. It had also held that people's private medical records are less private because they are kept in a doctor's office, and that private financial records cannot be considered private because they are held in a bank. A commonsense response to those situations is that they may be considered to be just as 'private' as the letters that were the most common mode of communication in the eighteenth century when the Fourth Amendment was drafted. However, because of the artificial 'expectation of privacy' test, which the government has exploited, the

[78] Bob Barr, 'Post 9/11 Electronic Surveillance Society Severely Undermining Freedom' 41(4) (2007) *Valparaiso University Law Review* 1383, 1385. The three cases were *Raskas v Illinois* 439, U.S. 128 (1978), *Rawlings v Kentucky* 448. U.S. 98, 1980 and *United States v Salvucci* 448 U.S., 83 (1980).

[79] Bob Barr, 'Post 9/11 Electronic Surveillance Society Severely Undermining Freedom' 41(4) (2007) *Valparaiso University Law Review* 1383-1412 1385

[80] Wayne R. LaFave 'Fourth Amendment Vagaries of Probable Cause, Imperceptible Plain View, Notorious Privacy and Balancing Askew' *Journal of Criminal Law and Criminology* 74 (1983) 1171, 1222.

[81] Murray T. Maclin, 'Constructing Fourth Amendment principles from the Government Perspective: Whose Amendment Is It Anyway?' *American Criminal Law Review* 25(4) (1988) 669, 675.

understanding of privacy, and data privacy, on which the Amendment was based, has been cast aside.[82]

Even garbage no longer enjoys the protection of the Fourth Amendment. In *California v Greenwood* [83] a government agent, following a tip-off that Greenwood was involved in drug-trafficking, asked the garbage collector to turn over Greenwood's trash bags to her. Having searched these, the agent found traces of narcotics in them. Greenwood challenged the searches of his trash, contending that they violated his Fourth Amendment Rights. The Supreme Court explained that the search of the trash would have violated the Fourth Amendment only if Greenwood manifested on subjective expectation of privacy in his garbage that society accepts as objectively reasonable. However, the Court found that Greenwood had sufficiently exposed his garbage to the public as to defeat any claim to Fourth Amendment protection. [84] Bradley, writing in 1985, observed that the overhaul called for by Harlan had still not occurred: instead, the Supreme Court 'has simply continued with the same problems, finding "solutions" which saw ever more litigation and confusion.'[85]

7.0 The Need to Reform Fourth Amendment Jurisprudence

In 1971 Justice Harlan called for an 'overhauling of Fourth Amendment law.[86] In 1974, Weinreb cited the fact that between 1968 and 1973, the Supreme Court had rendered sixteen major opinions interpreting the Fourth Amendment, illustrating that the body of Fourth Amendment [Supreme Court] doctrine 'is unstable and unconvincing.'[87] Bradley observes that between 1979 and 1984, the Court had decided 35 cases involving the Fourth Amendment:

> In seven of these, there was no majority opinion. In the seventeen cases decided [between 1983 and 1985] the Court has never reached the same result as all lower Courts, and has usually reversed the highest Court below, rendering a total of sixty-one separate opinions in the process.

[82] Bob Barr, 'Post 9/11 Electronic Surveillance Society Severely Undermining Freedom' *Valparaiso University Law Review* 41(4) (2007) 1383-1412, 1386.
[83] 486 U.S. 35 (1988).
[84] ibid, at para 40.
[85] Craig M. Bradley, 'Two Models of the Fourth Amendment' 83 (1985) *Michigan Law Review* 1468.
[86] *Coolidge v New Hampshire*, 403, U.S. 443 (1971) 490-1.
[87] Lloyd L. Weintrub, 'Generalities of the Fourth Amendment' 42 (1974) *University of Chicago Law Review* 47, 49.

> Thus it is apparent that not only do the police not understand Fourth Amendment law, but that even the Courts, after briefing, argument and calm reflection, cannot agree as to what police behaviour is appropriate in a particular case. [88]

The problems associated with Supreme Court jurisprudence on the Fourth Amendment are illustrated in its unanimous opinion in *United States v Ross* [89] in which it affirmed its commitment to the need for a search warrant:

> The Fourth Amendment proscribes all unreasonable searches and seizures, and it is a cardinal principle that 'searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment - subject only to a few specifically established and well-delineated exceptions.[90]

The comment at the end of this description of what the Fourth Amendment requires - probable cause and a search warrant - that this requirement is subject only to a few specifically established and well-delineated exceptions is not justified. As Bradley points out, there are 'over twenty exceptions to the probable cause or the warrant requirement, or both.'[91] These exceptions, listed by Bradley, and later cited by Justice Scalia in *California v Acevedo*,[92] include searches incidental to arrest, automobile searches, searches incidental to non-arrest where there is 'probable cause' to arrest, driver's licence and vehicle registration checks, airport searches and searches at courthouse doors.[93]

Ku, writing in 2002 and approaching the issued discussed above from the point of view of those who framed the Fourth Amendment, argues that the Founders were more concerned about limiting government's power to invade any aspect of life without sufficient cause than with defining what aspects of life should

---

[88] ibid. In one of the cases heard by the Supreme Court in 1982, centred on whether the Fourth Amendment prohibited the warrantless search of a leather pouch, but not the search of a paper bag.
[89] 458 U.S., 798, 825 (1982).
[90] 456 U.S. 798 (1982) at para 825.
[91] Craig M. Bradley, 'Two Models of the Fourth Amendment,' 83 (1985) *Michigan Law Review* 1468, 1473-4.
[92] *California v Acevedo* 500 U.S. 565 (1991)
[93] ibid, at paras 582-3.

be off limits to government, and that the Founders also believed that the people should play a sufficient role in making this determination.[94] The logic of Ku's approach is that the Fourth Amendment should play an important role in 'preserving the people's authority over government - the people's sovereign right to determine how and when government may intrude into their lives, and influence the behaviour of its citizens.' [95] However, as Ku sees it:

> [T]he Supreme Court's approach does more than ignore these concerns- it undermines them. As it stands, the Supreme Court has transferred the Fourth Amendment from a Constitutional provision delineating the scope of government power generally as determined by the people into a provision that protects only isolated pockets of interests as determined by Judges.[96]

According to the Supreme Court in *Katz* [97] the Fourth Amendment establishes a general rule that for a search to be considered reasonable, it must be authorised by warrant. However, as Ku and others see it, '[a]lthough the Court has never seriously questioned this Rule, it has spent over a quarter of a Century creating exceptions to it.'[98] Reading a warrant requirement into the Amendment, and hence 'reading an elaborate set of exceptions into that warrant requirement, seems more like rewriting the Amendment than reading it as it was written.'[99] The dispiriting conclusion reached by Ku is that 'either the Supreme Court considers the use of technology a search requiring a warrant, or the government's use of technology is absolutely unrestrained by the Constitution.'[100]

Taylor had already reached a similar conclusion when he suggested that '[f]ar from looking at the warrant as a protection against unreasonable searches, [the

---

[94] Raymond Shih Ray Ku, 'The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance' 86 (2002) *Minnesota Law Review* 1325,1327.
[95] ibid, 1326.
[96] ibid, 1357.
[97] 389 U.S. at 357 (1967).
[98] Raymond Shih Ray Ku, 'The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance,' *Minnesota Law Review* 86 (2002) 1325, 1357.
[99] Akhil Reed Amar, '*The Bill Of Rights: Creation And Reconstruction* (Yale University Press, 1998) 68-69.
[100] Raymond Shih Ray Ku, 'The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance,' *Minnesota Law Review* 86 (2002) 1325, 1358-59.

Supreme Court] saw it as an authority for unreasonable and oppressive searches, and sought to confine its issuance and execution in line with the stringent requirements applicable to common - law warrants for stolen goods.'[101] In cases where the Supreme Court considers the government's use of privacy-invasive technology as a search not requiring a warrant, as it does in the numerous exceptions it has created to the warrant requirement, the government's use of the technology is unrestrained by the Constitution. The consequence of this is that the Supreme Court has interpreted the Fourth Amendment to vest the authority to determine the appropriate level of privacy and security the citizen may enjoy to an institution [the government] whose power the Founders who framed the First Amendment sought to restrain, and thus, as Taylor puts it, the Courts has 'stood the Fourth Amendment on its head.'[102]

8.0 Conclusion

The closest European approach to the U.S. surveillance systems was the EU Data Retention Directive of 2006. Both the EU Directive and the NSA programme involved the retention and storage of metadata (but not the data) of citizens' telephone calls, text messages or e-mails for future law enforcement and counter-terrorist purposes. When, in the *Digital Rights Ireland* [103] case, the CJEU held that the vast metadata collection programme mandated by the Data Retention Directive violated the EU Charter of Fundamental Rights and stipulated that interference with data privacy rights be subject to strict scrutiny of its necessity and proportionality, even when that interference was carried out for national security purposes, the contrast between U.S. and EU jurisprudence in the context of the data privacy/national security balance was thrown into sharp focus. The question then arises: could the decision of the CJEU represent a model for the U.S. Supreme Court to adopt in adjudication mechanisms governing data protection in the context of the challenges posed to these by the sophisticated surveillance technologies of the digital age. This kind of adjustment was already foreshadowed in *Kyllo v The United States* [104] when the Supreme Court discerned a need to adopt Fourth Amendment doctrine to

[101] Telford Taylor, *Two Studies in Constitutional Interpretation* (Ohio State University Press, 1969) 41.
[102] ibid.
[103] Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland and Seitlinger and Others*. Grand Chamber CJEU, 8 April 2014.
[104] 533 U.S. 27 (2001).

protect traditional expectations of privacy from advances in technology. However, in *United States v Jones*[105] Justice Alito in his concurring opinion that digital change may lower the expectations of privacy and further suggesting that counter-terrorism investigations may justify sacrificing privacy for security needs.[106]

Nevertheless in the *U.S. v Jones* case Supreme Court Justice Sotomayor described the third-party doctrine approach, limiting the scope of Fourth Amendment protection as being 'ill suited to the digital age,'[107] on the basis that large amounts of information are disclosed by people 'in the course of carrying out mundane tasks,'[108] such as disclosing 'the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers.'[109] Justice Sotomayor observed that a search, as captured within the meaning of the Fourth Amendment, occurs, at a minimum, '[w]here, as here, the Government obtains information by physically intruding on a constitutionally protected area.'[110] Moreover, Judge Sotomayor also warned against 'entrusting to the executive, in the absence of any oversight from a co-ordinated branch (either the Courts or Congress) against a tool (such as modern technology) so amenable to misuse….'.[111]

While both of the major European Courts have emphasised the role of courts to act as protectors of privacy rights in the face of the challenges presented by government surveillance, U.S. jurisprudence, particularly in relation to the Fourth Amendment, has weakened, not strengthened, the comparatively fragile safeguards for privacy that the Amendment might have offered, compared with the robust safeguards offered by the two European Constitutional systems. Very recent U.S. Supreme Court decisions seem to offer tentative indications that the Court may in future tend to confront privacy-invasive technological advances with more than the traditional and relatively restrictive and

[105] 132 S. Ct. 945 (2012).
[106] ibid, at 955.
[107] ibid, at 957.
[108] ibid, at 957.
[109] ibid, at 957.
[110] ibid, at 954.
[111] ibid, at 956.

deferential interpretations of Fourth Amendment.[112] Cuccinelli and Fitzgibbons make the point that the 'third-party doctrine' has been rejected 'by at least seven states with no negative effort on their law enforcement,' and that:

> The Fourth Amendment 'is now subject to more than 225 years of experience and hindsight, and thousands of pages of case-law that is too frequently misinterpreted by government officials, and too inconsistently construed by lawyers and judges. People deserve better clarity about their fundamental rights to security and privacy of their property.[113]

This difficulty might be overcome by recourse to renewed emphasis on judicial activism, with a view to determining each case relating to an interpretation of the Fourth Amendment on its own merits. Ohm observes that the Fourth Amendment's background rules attaching to surveillance 'tend to operate in the middle,' between the polarities of unbridled surveillance and unbridled privacy and further contends that this due to 'a feature of its jurisprudence that is never celebrated by scholars - its lack of clarity.'[114]

With regard to the nuances of digital age technologies and the warrantless interception of communications data, Ferguson advocates the adoption of the 'informational curtilage' theory, which would define the threshold of a protected data trail the interception (and/or use) of which is a search.'[115] Ferguson additionally contends that the 'informational curtilage' theory would provide a 'workable test' to 'distinguish the types of data that should be protected,' and which would emphasize 'security over privacy and *ex ante* individual notice over *ex post* judicial review,' and provide 'a flexible balancing framework to allow for judicial discretion.'[116]

---

[112] For evidence of this, see the final section of the U.S. post-9/11 Chapter.
[113] Ken Cuccinelli and Mark Fitzgibbons, 'A Much-Needed Facelift for the fourth Amendment' *Washington Examiner* (20 January, 2015) <http://www.washingtonexaminer.com/a-much-needed-facelift-for-the-fourth-amendment/article/2558889> accessed 16 January 2017.
[114] Paul Ohm, 'The Argument Against Technology-Neutral Surveillance Laws' 88 (2010) *Texas Law Review* 1685, 1703.
[115] Andrew Guthrie Ferguson, 'The "Smart" Fourth Amendment' 102 (2017) *Cornell Law Review* 547, 618.
[116] ibid, 631.

While theorists such as Kerr have argued that the regime of existing Fourth Amendment protection provides an adequate framework wherein privacy and security can be balanced,[117] greater and ongoing levels of consistency regarding judicial interpretations of Fourth Amendment privacy rights in relation to communications will be essential, if a reasonable data privacy/national security balance is to be achieved. There would seem to be one obvious method of dealing with the obscurities inherent in the text of the Fourth Amendment, and at the same time with the multiplicity of problems posed by the inconsistent canons of construction applied by the judiciary in the interpretation of the privacy rights afforded by the Fourth Amendment and the restriction on these. This method would involve the replacement of the present text of the Fourth Amendment with a new version clearly setting out the precise nature of the privacy rights covered and the circumstances in which these rights apply and in which they are liable to restriction. Such a new version would also need to take into account the implications for privacy of technological developments.

Replacing the present version of the Fourth Amendment with a new one would be a complex process. There are two methods of bringing about an amendment, both of which are captured by Article 5 of the U.S. Constitution. The first, and most common one, requires that any amendment must receive two-thirds ratification in both the Senate and House of Representatives, and following this, the amendment must be ratified by three-quarters of the States.[118]

The second, and to date an unused method of amending the U.S. Constitution, involves the convening of a constitutional convention. This is brought about by means of a call, ratified by two-thirds of State legislatures, for the holding of such a convention. For an amendment to be successfully ratified, it must hence

[117] Orin S. Kerr, 'Do We Need A New Fourth Amendment' 107(6) (2009) *Michigan Law Review* 951,966.

[118] Article 5 states: The Congress, whenever two thirds of both houses shall deem it necessary, shall propose amendments to this Constitution, or, on the application of the legislatures of two thirds of the several states, shall call a convention for proposing amendments, which, in either case, shall be valid to all intents and purposes, as part of this Constitution, when ratified by the legislatures of three fourths of the several states, or by conventions in three fourths thereof, as the one or the other mode of ratification may be proposed by the Congress; provided that no amendment which may be made prior to the year one thousand eight hundred and eight shall in any manner affect the first and fourth clauses in the ninth section of the first article; and that no state, without its consent, shall be deprived of its equal suffrage in the Senate.

enjoy the three-quarters majority support of the States at a convention.[119] In this regard, Congress is not involved in the process and its approval of an amendment in the ambit of a constitutional convention is not required. The latter method has never been used, and in relation to the former method, it is doubtful whether a supermajority of both houses of Congress would ratify an amendment which limits the interpretative role of the judiciary and places restrictions upon themselves.[120]

[119] ibid.
[120] Gaines B. Jackson, *Rape of the American Constitution By Its Own Government* (Mill City Press, 2016) 87.

Overall Conclusion

Throughout the period reviewed in this thesis, the quality and variety of personal data accessed, processed and exchanged by Government intelligence agencies has been steadily escalating. During the decades ahead, should present trends continue, U.S. Presidents are likely to inherit extensive knowledge about almost every U.S. citizen's beliefs, concerns, attitudes, interests, fears, activities and associates. The mass of information involved here will also be subject to electronic search, storage, and cross-reference. This process will generate increasingly reliable conclusions about citizens' past in addition to predictions about their future activities.[1] Defenders of the privacy rights of citizens tend to regard the possible ramifications of this situation for democracy and for civil society as dangerous. For example, law enforcement agencies, without any showing of a compelling social need or of a judicial warrant, can demand, with the assistance of a federal prosecutor, records that *might* be useful to a Grand Jury. This procedure has been vindicated by the U.S. Supreme Court.[2]

This phenomenon has largely been a function of more sophisticated surveillance technologies and the readiness of governments and intelligence agencies to deploy these in the service of national security, particularly when state authorities considered that this was under immediate threat by terrorist elements. From the beginning of the post-World War II period, the authorities had been active in developing the surveillance capacities of its intelligence services, the CIA, the FBI and the NSA, the latter playing the most prominent role in the protection of national security. In the pre-digital age, the world had yet to experience the proliferation of digital technologies with their more and more sophisticated surveillance tools, and their expanding role in intelligence-gathering which marked the beginning of the twenty-first century. The deployment by the U.S. intelligence agencies, and predominantly by the NSA,

[1] Philip B. Heymann, 'An Essay on Domestic Surveillance' *Journal of Security Law and Policy* 8 (2016) 241.

[2] See *United States v Williams*, 505 U.S. 36 (1992), para 48: 'The grand jury can investigate merely on suspicion that the law is being violated, or even because it wants assurance that it is not. It need not identify the offender it suspects or even the precise nature of the offence it is investigating.' The government is also empowered to demand access to any records possessed by third parties, including the vast quantity of electronic records now kept by businesses about their customers. See *Smith v Maryland* 442, U.S., 735 (1979) in which the third party doctrine is articulated.

of programmes of mass collection and retention of U.S. citizens' personal data in response to the terrorist attacks on two American cities on September 11, 2001, inaugurated a new phase in the history of the data privacy/national security balance.

Different interests came into conflict in this field. One the one hand, the U.S. Executive, with the support of the legislature, felt that its primary obligation, in time of emerging threats to the security of the State, was to engage its intelligence agencies in virtually unrestricted covert surveillance programmes, which inevitably involved interference on a wide scale with the data privacy of U.S. citizens. This brought the data privacy/national security balancing paradigm into sharp focus, with two different interests in conflict with each other: the Executive and the intelligence agencies engaging a comprehensive data collection programme, and private individuals, with the support of privacy advocates, arguing for a legitimate, adequate use of personal data, and a safeguarding of their privacy rights.

The tension between the two societal interests, privacy of personal data and the security of the State was not as marked in the U.S. as it was in Europe where it was first addressed by the Data Protection Directive (95/46/EC). This measure embodied a set of principles to be complied with by data controllers and processors, in public as well as in private organisations, along with a statement of the rights of data subjects. However, the significance of this measure for these rights is diminished by a key provision in the Directive that the processing of personal data for the purposes of national security is explicitly excluded from its scope. EU security-defensive policies were progressively tightened when the post-9/11 'war on terror' reached Europe and the EU Data Retention Directive led to the establishment of vast databases of citizens' telecommunications and Internet metadata. The data privacy/national security balance fluctuated again when on 8 April 2014, the European Court of Justice declared that the Data Retention Directive was invalid, due to the provisions of the EU Charter of Fundamental Rights which upgraded the right to the protection of personal data to the status of a human right.

Such fluctuations in the data privacy/national security balance illustrate the principle that the meaning and scope of values such as national security and data privacy evolve with time and circumstances, as well as with the relative weight attached to other principles, rights and values that may enter into conflict with them. The changes in the equilibrium between data privacy and national security imperatives as recorded in the thesis are predominantly reactive, whether they are responding to developing situations such as terrorist events, legislative enactments, judicial decisions or public revelations by whistleblowers about interference with privacy rights by intelligence agencies. Thus, for example, in Europe, twenty-first-century terrorist attacks followed by blanket data retention measures in 2006 moved the balance firmly towards security, while the *Digital Rights* judgment of 2014 moved the balance firmly towards privacy, and as a result of the judgment in *Tele 2 and Watson*, the balance rested firmly on the side of data privacy. In the U.S.A., pre-9/11, surveillance and data retention flourished at the expense of data privacy, and in reaction to this overbalancing, the Foreign Intelligence Surveillance Amendment Act was introduced in 2008 to restore a balance more favourable to privacy, while security defensive measures taken post-9/11 represented an extreme rebalancing in favour of national security.

When U.S. and European practices in maintaining a balance between data privacy and national security are being compared, the most significant influences at play are contrasting understandings of the status of data privacy as a fundamental right. The European understanding on this issue is that any interference with this right, even in the interest of national security, must be subject to a number of strict conditions. This understanding is reflected in the EU Charter of Fundamental Rights, in Article 17 of the International Covenant on Civil and Political Rights, (the ICCPR) and the U.N. Human Rights Committee's Interpretation of the ICCPR. By those standards, European privacy advocates, revisiting U.S. surveillance practices in the light of the Snowden revelations, felt able to argue that the U.S. authorities violated their international obligations and the right to individual privacy granted by Article 17 of ICCPR to all those whose communications were intercepted by the NSA without judicial supervision. This interpretation is not acceptable to U.S. international lawyers who support the U.S. understanding of privacy. The U.S.

position is that no right to privacy can be discerned in contemporary international law.

In 1890, Warren and Brandeis cautioned that threats to conceptions of privacy abounded, stemming from the fact that '[I]nstantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life,' in addition to 'numerous mechanical devices.'[3] Furthermore, as a consequence of '[r]ecent inventions and business methods,' they contend that 'attention to the next step must be taken for the protection of the person.'[4] In this regard, they refer to Judge Cooley's doctrine of the right "to be let alone."[5] It is worth observing that initiatives leading to a 'Right to be Forgotten,' could be viewed as representing a logical new-age evolution of Cooley's right to be let alone.

Another problem arises when legal and policy decisions involving privacy rights have been made on the basis of a commitment to privacy such as might be inspired, for example, by the pronouncement of U.S. Supreme Court Justice Louis Brandeis, who characterised it as 'the most comprehensive of rights and the right most valued by civilized men.'[6] The practical problem is that no matter what aspect of privacy a society chooses to protect in its laws, such protection as is afforded will often tend to compromise, sacrifice or occult interests of importance to large numbers of people in the same society. Such interests may include: freedom of speech, freedom of the press, economic and social benefits, access to information online or otherwise, while also inhibiting law enforcement and endangering national security. Suppose, for instance, that legislators decided to frame a statute protecting privacy and defining it without further qualification as 'the right to be left alone,' a notion given currency in the nineteenth century as a legal term of art, [7] also taken up by Brandeis and Warren[8] and recently included by Solove in his list of general types of privacy.[9]

[3] Samuel D. Warren and Louis D. Brandeis, 'The Right To Privacy.' *Harvard Law Review*. (1890). IV (5) 193. 195.
[4] ibid.
[5] ibid. See *Cooley on Torts*, 2d ed., 29.
[6] *Olmstead v United States* 277 U.S. 438, 478 (1928).
[7] Thomas Cooley, *The Elements of Torts* [1895] 9.
[8] Louis Brandeis and Samuel Warren, 'The Right to Privacy' (1890-91) *Harvard Law Review* 4(5) 193 195.
[9] Daniel Solove, *Understanding Privacy* (Harvard 2008) 1, fn 23.

Attempts to make such a statute take practical effect would face the same obstacles as would all other incomplete or over-general definitions. Legalising the right to be left alone would leave the way open to ill-intentioned people to plan and perpetrate offences against the state, to frustrate aspects of law enforcement, to commit crimes against family members, and to avoid obligations to society.

The significant feature of this case was not the judgment, but the dissenting opinion of Judge Brandeis, who argued for a broader interpretation of the right guaranteed by the Fourth Amendment, and in effect for a constitutional right to privacy disjoined from property. He made the case that the makers of the Constitution, in formulating the Fourth Amendment, had conferred, 'as against the government, the right to be let alone- the most comprehensive of rights and the right most valued by civilised men.'[10] The view of privacy as autonomy advanced by Brandeis did not become influential in U.S. jurisprudence until the mid-nineteen sixties. Already in 1890, Warren and Brandeis, invoking the Common Law principle that a man's home was his castle, used this principle as a basis for implying a right to personal privacy. Starting from the premise that the Common Law has always recognised that a man's house is impregnable even to officers of the law 'engaged in the execution of its commands,' they asked rhetorically: 'Shall the Courts now close the front entrance to constituted authority, and open the back door to prurient curiosity.'[11] Consequently, no State or authority is obliged to respect such a right. Relying on the U.S. doctrine of national sovereignty, lawyers such as E.A. Posner hold that this doctrine implies a 'right to surveillance' for each State, which may be legitimately exercised by European, as well as U.S. authorities.[12] When Posner invokes a 'right to surveillance,' he is referring to the mass surveillance practices of the NSA as revealed by Edward Snowden.

The relative strength of European data protection provisions, constitutional, legislative and judicial, gives rise to the question whether, or to what degree,

[10] ibid, at 478.
[11] Samuel Warren and Louis Brandeis, 'The Right to Privacy,' (1890) 4 *Harvard Law Review* 193.
[12] E.A. Posner, S*tatement to the Privacy & Civil Liberties Oversight Board*, 14 March 2014, available online at <pclob.gov/Library/20140319-Testimony-Posner.pdf> accessed 19 January, 2017).

these provisions offer protection to European citizens against undue interference with their personal data. The relevant material reviewed in this thesis points to the conclusion that neither the EU nor the Council of Europe data protection provisions during the period up to April 2016 had the capacity to impose meaningful limitations on government surveillance. Prior to the passage of the EU Data Regulation (2016/679/EU) the EU had limited jurisdiction over the foreign intelligence activities of its Member States, the great majority of which were also members of the Council of Europe. Under the terms of the Treaty on the Functioning of the European Union, each Member State maintains its own policies and laws on domestic intelligence gathering, with various degrees of privacy protection offered to its own citizens.[13] States could enforce their privacy protection laws only within their own territory.

The privacy of European citizens' data is further compromised by the transnational nature of data-flows. Much European personal data are stored and processed by foreign companies outside the EU, with diminishing amounts are stored in the EU, thus not allowing local state authorities to enforce EU and national privacy laws effectively. These developments prompted the EU to initiate a programme of comprehensive data protection reform in 2014. The vital element in this reform programme was the decision of the EU Commission to adopt a Data Protection Regulation, directly applicable to every state in the Union, rather than a Directive, which would have led to the perpetuation of discrepancies between the privacy protections afforded in different states. The Regulation recognises that flows of personal data to and from countries outside the EU are necessary for the expansion of international trade, for example, but also that the increase in such flows has raised challenges and concerns with regard to the protection of such data. To allay these fears and meet these challenges, the Regulation has been designed to ensure that when personal data are transferred from the EU to controllers, processors or other recipients in third countries, the level of protection of natural persons ensured in the Union by the Regulation should not be undermined. Thus, under the terms set out in the Regulation, transfers of data

[13] Article 4.2 of the Treaty on European Union (1992) reads: 'National Security remains the sole responsibility of each member state.'

can take place only if the privacy-protective measures prescribed in the Regulation relating to the transfer of personal data to third countries are complied with by the controller or processor. It is for the EU Commission to decide, with effect for the entire European Union, that a third country, or a specified sector within a third country, or an international organisation, offers a level of data protection in conformity with EU standards, thus providing legal certainty and uniformity throughout the Union, as regards that third country or organisation.[14]

The materials surveyed in this thesis relating to data protection/national security balancing and the prospect of devising a principled legal solution to the ongoing problem of achieving a system of balancing that might win acceptance on both sides of the Atlantic and perhaps further afield, suggest that the major obstacle to such an outcome is still the transnational nature of data flows. It is apparent that a data privacy/national security balancing regime, limited to either the United States or to Europe, will not suffice to inhibit or deter the dissemination of private data in the wider world. One solution would be to devise systems enjoying transnational, as distinct from local, acceptance, based perhaps on principles embodied in Article 17 of the ICCPR. The feasibility of this kind of solution is questionable in the light of the U.S. government view that the ICCPR did not apply to the U.S., and the U.S. position, mentioned above, that no right to privacy is affirmed in international law. The creation of a global consensus on an appropriate data privacy/national security balancing paradigm in the age of the borderless internet seems a remote prospect, at time when it is unrealistic to expect effective protection from foreign cyber spying under U.S. law, when U.S. law, while offering some degree of protection to U.S. citizens against spying by their own government, does not impose significant limitations on foreign intelligence gathering by U.S. governments on foreign territory. Another factor inhibiting a global consensus is that the U.S. government has no incentive to limit or halt the mass surveillance programmes of its intelligence agencies, firstly because the 'war on terror' declared in 2001 is still being waged, and secondly, there is no assurance that even if the government desisted from, or moderated its programmes, other governments or groups would follow suit. Again, the U.S.

[14] Regulation 2016/679/EC, Articles 101 and 103.

government, having set up and greatly expanded the reach and sophistication of agencies such as the NSA, is most unlikely to diminish their capacities. At the same time, in common with other state-funded bureaucratic systems, these agencies feel the need to justify their existence, the vast number of operatives they employ and their huge budgets, while supporters of surveillance equipment are incentivised to supply them with more and more sophisticated surveillance tools.

An issue examined in the thesis is whether one can validly assume that as a consequence of the mass data retention and surveillance practices of agencies such as the NSA and GCHQ, the transatlantic world has been spared greater levels of terrorism, or whether it is the case that the activities of these agencies have little or no bearing on national security, despite their vast resources in manpower, money and technological expertise. An analysis of the claims made by and on behalf of these agencies by their executives and by governments that they have succeeded in thwarting further terrorist attacks post-9/11 suggests that such claims may be unjustified. If the claims are in fact unjustified, those who persist in making them might be compared to the man who was asked by his psychiatrist why he kept waving his arms about. 'To ward off the killer elephants ' the man replied. 'But there aren't any killer elephants around here' said the psychiatrist. 'That's rights,' his patient replied. 'Effective, isn't it.'

The Snowden revelations of multiple aspects of the NSA's surveillance activities demonstrate that the most secretive of secret intelligence agencies was incapable of safeguarding the extremely sensitive data it had gathered over a long period of time. This exposes the futility of these activities, a side-effect of which was to compromise the data privacy of millions of people, at the same time compromising its own valuable intelligence data. In an important sense, government and the intelligence community were fortunate that it was Snowden who revealed the truth about U.S. surveillance practices. If another intelligence operative with expertise similar to Snowden's had been a terrorist agent and had secretly passed the data on to a terrorist group, the consequences for national security might have been far worse. One of the ironies associated with the policies of the agency specifically tasked with the defence of national security was its weakening of the encryption and other Internet safety standards

for the purposes of facilitating mass surveillance. This calculated weakening poses a danger for national security, since the weaknesses are open to exploitation by terrorists and cyber terrorists, who can take advantage of the schemes implemented by the National Security Agency in order to compromise national security.

In the context of arriving at a principled legal solution to the problem of achieving a data privacy/national security balancing solution that might win approval in both Europe and the U.S., one major obstacle identified in this thesis is the transnational nature of data flows. There are other obstacles. Attempting to reconcile the fundamentally different cultural and legal understandings in Europe on the one hand and in the U.S. on the other, of what privacy means, and should mean, constitutes another major obstacle. Furthermore, the differing attitudes in the two jurisdictions to the relative importance of privacy, and in particular, in the context of the research question dealt with in this thesis, to the significance of data privacy as a fundamental right, are significant barriers to the achievement of a data privacy/national security balancing solution. As has been indicated above, a balancing solution such as the acceptance by the U.S. of the principles enshrined in the EU Charter of Fundamental Rights, particularly that interferences with data privacy must be subject to a number of strict conditions, or of those enshrined in the International Covenant and Political Rights (the ICCPR) as interpreted by the U.N. Human Rights Committee, would conflict with the standard U.S. position that no right to privacy can be discerned in international law, that no state is obliged to respect such a right, and that each state enjoys an unrestricted right to surveillance.

Further considerations, pragmatic rather than theoretical or philosophical, come into play when one is responding to, or passing judgment on, the wholesale intrusion into the data privacy rights of innumerable people throughout the world by intelligence agencies in the case of protecting national security, a process facilitated by the exponential development of privacy-invasive technologies. The detailed, authoritative revelations of Edward Snowden have given us a new perspective on the nature and scope of government surveillance of citizens in times of peace and war and the collection by intelligence agencies

throughout the world of vast amounts of information on Internet communications and international phone calls, including those involving diplomats and government.

What Snowden has revealed suggests that no European government is in a position to condemn the NSA and other U.S. Intelligence agencies for their systematic, unrelenting data gathering activities. Snowden has shown that European governments operate data-gathering programmes similar in kind, if not in degree, to those of the NSA, and regularly share these data with the NSA, an outstanding example being the British GCHQ. Sweden passed a law in 2008 allowing its intelligence agencies to monitor cross-border e-mail and phone communications without any court order.[15] A loose alliance exists between British, Swedish, German, French and Spanish intelligence agencies. Data transfers from Germany aid U.S. surveillance, while U.S. intelligence agents have intercepted the phone calls of the German Chancellor, Angela Merkel, whose phone calls were also intercepted by the NSA.[16] Data gathering is endemic. Most countries conduct foreign intelligence data gathering programmes, and even allies spy on each other. In this scenario, it seems futile and illusory to expect governments to desist from data gathering. As has been pointed out above, no government is incentivised to moderate or halt its data-collection programmes, there being no assurance that other governments will reciprocate.

The countries mentioned above are engaged in compiling economic. political and military foreign intelligence data. The motivations behind data-gathering remain largely the same: to acquire the capacity to protect and defend national security. The extent to which this activity is legal is another matter. Intercepting foreign communications data is usually prohibited under the domestic laws of the country being spied upon. On the other hand, simply because one country's foreign intelligence data-gathering programmes may violate another county's domestic laws governing interference with data privacy does not mean that these programmes are illegal under the domestic

[15] Gregory F. Treverton, *Intelligence for an Age of Terror* (Cambridge University Press, 2009) 249.
[16] Philip Sherwell and Louise Barnett, "Barack Obama approved tapping Angela Merkel's phone 3 years ago' *The Telegraph* (27 October, 2013).

law of the cyberspying country. For example, the German Foreign Intelligence Service (BND) describes its mission as compiling foreign intelligence data 'in secret and clandestine ways but always in compliance with applicable [German] law and in the interest of national security.'[17]

As a response to the massive worldwide expansion of government data surveillance activities, privacy advocates' instinctive response tends to take the form of the demand that governments discontinue or limit surveillance. However, at a time when the transatlantic world is enduring a dangerous terrorist phase, it is unlikely that governments will accede to such a demand. On the contrary, many European countries are bolstering their surveillance resources in an effort to match those of the United States. It is reasonable to argue that limiting U.S. surveillance capacities might well reduce the security of people in the U.S. and its allied countries, increase their exposure to surveillance by other countries, and not increase anybody's net privacy protections.

There have been suggestions that increased government transparency should be the basis of further discussions and cost-benefit analyses regarding intelligence-gathering programme reform. The possibility of achieving this goal seems limited given the potential adverse effect transparency could have on successful intelligence gathering. As Determann and Guttenberg suggest, '[a] turn in the opposite direction may be more promising. Secret services should be kept more secret.' [18] It seems likely that citizens would be less concerned by foreign intelligence gathering if the information derived from this were kept secret, safe and secure. However, at a time when terrorist incidents constitute an ever-present threat, it is alarming that the U.S. Government had proved unable to keep massive amounts of sensitive data secure and secret. Bradley Manning, a low-level intelligence analyst in the U.S. Army and Edward Snowden, a civilian computer technician working for a private

[17] Lothar Determann and Karl T. Guttenberg, 'On War and Peace in Cyberspace - Security, Privacy, Jurisdiction' *Hastings Constitutional Law Quarterly* 41(4) (2014) 875, 881.
[18] ibid, 890.

government contractor, leaked top-secret intelligence data to the media for publication.[19]

Future Developments

The quest to find a balance between the retention of telecommunications data which fulfils national security objectives and the right to data privacy, is likely to endure for the foreseeable future, in the same fashion as has the technological joust for supremacy between cryptographers and de-cryptographers.

For law enforcement agencies, legislators and the judiciary, the relentless and rapid pace of technological evolution, development and innovation has proven difficult, if not impossible to evaluate and respond to with commensurate rapidity. This, coupled with transborder transfers of digital communications and data, makes the task of upholding national security and serious crime objectives difficult. Moreover, the increasing use of retention circumvention methods in the form of encryption, unregistered SIM cards and phone handsets, in addition to the relative anonymity offered by the Darkweb, illustrates the ever increasing potential for acts to terrorism to be perpetrated with a corresponding absence of any certainty that those engaged in such acts will be detected.

Those seeking greater levels of privacy in the digital era face inevitable obstacles which impact upon the practical implementation of legislative or other measures to enhance levels of privacy. 'Deleted' data, whether telecommunications data or other forms of data, are not always deleted, but can be transferred from one server to another, while 'matters for momentary embarrassment can now become immortalized on web servers.' [20] Law enforcement objectives are cited to explain the need to ensure that certain forms of information are not deleted to ensure that evidence cannot be tampered with.[21]

[19] Mark Mazzetto and Michael S. Schmidt, 'Ex-Worker at C.I.A. Says he leaked Data on Surveillance' *New York Times* (June 9, 2013).
[20] Alexander Tsesis, 'The Rights To Erasure: Privacy, Data Brokers And The Indefinite Retention of Data' *Wake Forrest Law Review* 49 (2014) 442.
[21] ibid, 478.

From the standpoint of preserving or enhancing privacy rights and guarantees in the digital age, it seems the Fourth Amendment in the United States and Article 8 of the European Convention On Human Rights, in addition to domestic statutes, require evolution to capture the nuances of rapidly advancing technologies and how these can impact, whether positively or negatively, on privacy rights. This is because the Fourth Amendment and Article 8 ECHR were formulated at a time when digital age concerns such as the balance between telecommunications data retention and privacy rights were yet to manifest.

While the achievement of a principled data protection/national security paradigm enjoying acceptance on both sides of the Atlantic and further afield may seem a remote prospect, some reforming measures, relating to both data protection and national security might be more easily achievable. Such measures might focus on enhancing governments' data security mechanisms with a view to reducing data leaks, thereby alleviating national security concerns. To strengthen data privacy protection, procedural and organisation safeguards at surveillance agencies might be enhanced, an example being the appointment of a Civil Liberties and Privacy Officer at the NSA in the aftermath of the Snowden revelations.[22] The rules for cooperation between intelligence and law enforcement agencies might be re-framed to permit information-sharing only in clearly enumerated cases of extreme and immediate threats to national security. Finally, in the interests of protecting data privacy, a closer monitoring of the compliance of law enforcement agencies with data privacy laws might be instituted.

The transborder dimension of data flows and exchanges poses challenges for those advocating privacy and law enforcement standpoints. Due to the borderless nature of communications in the digital age, it is likely that an International treaty or protocol, administered by the United Nations, might be necessary to establish what constitutes privacy and national security aims and objectives and under what circumstances the balances between the two can be altered. The development of Cloud Computing where data can be stored in

[22] Margo Schlanger, 'Intelligence Legalism and the National Security Agency's Civil Liberties Gap' *Harvard National Security Journal* 6 (2015) *Harvard National Security Journal* 112, 140, fn 116.

many territories, poses difficulties for those on both sides of the balancing paradigm.

A recurring question which emerges in the discourse relating to the balance between the retention of telecommunications and other data to uphold national security objectives and privacy and data privacy rights, concerns whether retained data contribute to efforts to prevent and combat serious crime and terrorism. To date, there is little evidence to support the proposition that they do, aside from contested contentions by Governments that data retention measures have prevented instances of terrorism.

Those who advocate that limitations on the mass retention of telecommunications, Internet and other forms of communications data is necessary to uphold privacy rights, might consider the possibility that as increasing acts of terror are perpetrated, limits on retention mechanisms could confer an advantage on the enemies of a particular nation, state or continent.

The biggest problem for data protection everywhere arises from foreign cyber surveillance. Even the most rigorous EU or ECHR data protection law cannot protect European citizens from this kind of surveillance. The same applies to U.S. data protection law. In the case of the EU Data Protection Regulation, the difficulty is that the current versions of this do not even attempt to regulate surveillance for national security purposes. Furthermore, the laws of each European country cannot offer meaningful protection from its own government intelligence agencies.

Assessing the trade-offs between data privacy tights and national security imperatives has always been a difficult task. One reason for this is that much is, and will, remain unknown and in dispute about the effectiveness of surveillance programmes in protecting national security. Further, there is little evidence for such simple correlations such as 'less surveillance means more privacy.' On the contrary less government surveillance, intelligence gathering and law enforcement have the potential to result in a loss of net privacy when one takes into account the fact that surveillance by foreign governments and cybercriminals will tend to increase. It is thus reasonable to conclude that less

surveillance does not automatically result in more privacy. It is also reasonable, given the evidence of security breaches and data leaks involving the intelligence services in the United States, that more surveillance does not automatically guarantee more security.

It is now widely accepted that five arenas exist where conflict and warfare have the potential to occur; land, sea, air, outer space and within cyberspace. However potential responses to ongoing acts of terror and hacking, perpetrated through and with direct effects on cyberspace itself and beyond continues to evolve, but has yet to crystallise.[23] Perhaps it is valid to draw and an analogy between the privacy/data retention balancing paradigm and the question regarding the merits and demerits of nuclear weapons and their role in global conflict. Amis sums up the rationale among those who seek to justify the necessity of nuclear weapons as a means of preventing their use:

> What is the only provocation that could bring about the use of nuclear weapons? Nuclear weapons. What is the priority target for nuclear weapons? Nuclear weapons. What is the only established defense against nuclear weapons? Nuclear weapons. How do we prevent the use of nuclear weapons? By threatening to use nuclear weapons. And we can't get rid of nuclear weapons, because of nuclear weapons.[24]

Similarly, robust telecommunications data retention may be necessary to ensure that its use can not be monopolised by any nation, state or continent to the detriment of another.

The Convergence of The Twain?

The emphasis so far has been on the formidable obstacles confronting attempts to devise a data privacy/national security balancing paradigm capable of commanding acceptance on both sides of the Atlantic. However, this negative outlook may not tell the entire story. Developments on both sides of the Atlantic in the twenty-first century may be part of a process of opening the way for a new trans-Atlantic standard governing law enforcement access to personal

[23] Gary D. Solis, 'Cyber Warfare' *Military Law Review* 219 (2014), 1, 40.
[24] Martin Amis, *Einstein's Monsters* (Jonathan Cape, 1987) "Introduction: Thinkability" (Jonathan Cape, 1987), 2.

data. Even in present circumstances it is clear that there is a tendency among commentators to overstate the extent of the disparity between European and U.S. privacy and surveillance regimes There is no doubt that the comprehensive privacy regime in the European Union contains many requirements that do not apply in the U.S. However, apologists for the U.S. privacy regime can argue that the U.S. also sets requirements that do not apply in the EU., for example, the Fourth Amendment requirement that a warrant be signed by a judge upon a finding of probable cause before surveillance may be undertaken.

If both of these standpoints are valid, the conclusion must be that both the EU and the U.S. are stricter than each other in some significant respects. There are two problems here. The first is that the data protective Fourth Amendment requirement has been inconsistently interpreted by the Courts and not always applied in the manner mentioned above. The second, more serious, problem is that in 2015, the highest EU Court, the CJEU, found that the U.S. did not provide a level of protection of fundamental rights and freedoms guaranteed in the EU by virtue of the EU Data Protection Directive read in the light of the EU Charter. Essentially, the CJEU found that the U.S. felt free to undermine the fundamental right to data privacy under Article 7 of the EU Charter when this right was in conflict with U.S. national security and law enforcement requirements.[25]

The EU has approved a General Data Protection Regulation that will be effective in 2018 and strengthen existing privacy protections, [26] in addition to a Police and Criminal Justice Directive which concerns government access to personal data.[27] Both of these EU instruments contain requirements for data transfers to third countries In light of this, it would appear that the U.S. will have to strengthen its privacy protection systems if a principled legal solution

[25] Case C-362/14, *Maximilian Schrems v Data Protection Commissioner*, 6 October, 2015.
[26] Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1.
[27] Directive 2016/680, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JIA, 2016 O.J. (L 119) 89.

to the problem of devising a data protection/national security balancing paradigm capable of winning acceptance on both sides of the Atlantic is to be solved.

Considerable progress needs to be made on the U.S. side to make this ideal a reality by developing forms of governance and law reform to address European privacy concerns. One of the key aspects of the 'War on Terror' has been the intensification of surveillance, aided by advances in technology. This new surveillance paradigm has now become globalised, since U.S. security imperatives transcend borders and have been duplicated in other parts of the world. Most scholars who have analysed and compared the extent and limits of privacy protection in the U.S. and the EU have concluded that EU law provides a higher level of constitutional protection of privacy than U.S. law.[28]

In the U.S., one of the significant obstacles to filling the void between U.S. and European protections of data privacy lies in the failure of the Courts to interpret Fourth Amendment privacy safeguards in a manner that takes account of the sophistication of modern information technology and the potential of the Amendment to become a more effective agent of privacy protection. The application of the third-party Fourth Amendment doctrine has whittled away privacy protections, and has created a privacy gap by denying Fourth Amendment protection to data processed by third parties, including communications information and data stored in the 'cloud.' The rapid advances in information technology and a proliferation of third-party records means that the gap in privacy protection continues to widen, and with it the gulf between privacy protections in the U.S. and in Europe.

If the gulf is to be narrowed, U.S. federal courts will need to be less reluctant to become involved in regulating electronic surveillance. However positive developments in this area have been a recurring feature of the jurisprudence concerning the Fourth Amendment in the new millennium, when Courts have responded to the implications of changing technology for Fourth Amendment interpretation, and in the process issued a series of Fourth Amendment rulings

[28] See, for example, Valsamis Mitsilegas, 'Surveillance and Digital Privacy in the Translantic "War On Terror": The Case For a Global Privacy Regime' *Columbia Human Rights Law Review* 47 3(1) (2015-16) 1.

to protect privacy. These included *Riley v California* [29] ; *United States v Jones* [30] and *United States v Warshak.*[31]

Elected branches of the U.S. government have also moved to set limits to surveillance. When its excessive use became known, these branches responded with legislative privacy safeguards. For example, gross interferences with privacy under President Nixon were followed by attempts at reform, including the Privacy Act of 1974, expansion of the Freedom of Information Act in the same year and the Foreign Intelligence Surveillance Act (FISA) in 1978. Following the Snowden revelations from 2013, the U.S. Government introduced over two dozen significant surveillance reforms, which included two notable statutes: the USA Freedom Act of 2015, which created multiple new limits on foreign intelligence surveillance. The Freedom Act abolished bulk collection of data which had been provided for under Section 215 of the Patriot Act. These limits on collection apply to both U.S. and non-U.S. persons. As a result, a far narrower authority now exists, based on individualised selectors associated with terrorism, and judicial review of each proposed selector.[32] Congress also enacted the Judicial Redress Act in 2016. These legislative and Executive safeguards setting limits on surveillance powers complemented the privacy protection afforded by the Constitution and the independent judiciary.[33] Although some of these legislative provisions, including FISA and the Freedom Act fell short of expectations, a group of independent researchers were sufficiently impressed to declare that 'the legal framework for foreign intelligence collection in the U.S. as enhanced by the Presidential Policy Directive of January 2014, contains much clearer rules on the authorisation and limits on the collection, use, sharing and oversight of data relating to foreign materials than the equivalent laws of almost all EU Member States.[34]

[29] 134 S. Ct. 2473 (2014) - warrant needed to search cell phones.
[30] 132 S. Ct. 495 (2012). - warrant needed for high technology search of home conducted from the street.
[31] 631F. 3rd, 266/6th Cir. (2010) - warrant required to access e-mail.
[32] These reforms are Codified at 50 U.S.C., Section 1881 a.
[33] See Peter Swire and De Brae Kennedy-Mayo, 'How Both the EU and the U.S. are 'Stricter' than Each Other For the Privacy of Government Requests for Information' 66 (2017) *Emory Law Journal* 617, 640-642.
[34] ibid, 652, fn 187.

The verdict of these independent researchers seems to indicate that U.S. reforms in the area of surveillance practices and privacy rights have laid the groundwork for the establishment of an agreed transatlantic data privacy/national security regime. In formulating the content of such a regime, the EU and the Council of Europe can provide key guiding principles, some of which are acknowledged in recent U.S. legislation and jurisprudence providing for improved privacy protection and more robust controls imposed on surveillance practices.

In the context of devising a data privacy/national security balancing paradigm commanding acceptance in both the U.S. and Europe, other developments are worth noting. In 2012, President Obama's Administration devised the Consumer Privacy Bill of Rights, designed to give Americans many of the privacy protections that the EU General Data Privacy Regulation affords.[35] Also in the U.S., State governments have also increased privacy standards, including California, Nevada and Massachusetts,[36] while Vermont, Minnesota and North Dakota have adopted legislation that embodies principles from the EU Data Protection Directive.[37] The Massachusetts privacy regulation incorporates the principles and policy in the EU Data Protection Directive and the EU General Data Protection Regulation.[38] To develop a U.S./European privacy standard, it will be necessary for the U.S. to resile from its self-regulatory approach to privacy regulation, and the Federal Government will have to intervene to provide an acceptable level of regulation.

Such a transition away from self-regulation on the part of the Federal Government would be made easier if a sufficient number of states followed the example of the six mentioned above and enforced European privacy standards, thus incentivising the Federal authorities to move in the same direction. If this were to happen, it is likely that third countries would replicate the U.S. privacy standards in order to conduct business in the U.S. In such a scenario, with two

[35] Natasha Singer, 'Data Protection Laws, an Ocean Apart' *The New York Times* February 2, 2013.
[36] Edward R Alo, 'EU Privacy Protection: A Step Towards Global Privacy' 22 (3) (2014) *Michigan State International Law Review* 1096.,1143-44.
[37] ibid, 1143, fn 225.
[38] ibid, 1144.

of the world's largest markets, the U.S. and Europe, establishing similar privacy standards, a global standard would ultimately exist.

Among the principles that could underpin a transatlantic or even a global privacy regime, a fundamental one would be that the right to data privacy should apply to all individuals, irrespective of nationality. This would have the effect of placing meaningful limits on foreign surveillance, and confront the challenge of addressing extraterritorial systems of surveillance with territorial laws. The right to data privacy should also cover not only the processing of personal data, but should limit the collection of such data, and its storage and transfer. A further requirement would be the provision of effective remedies and means of redress for individuals claiming to be affected by surveillance activities, but who do not necessarily have to demonstrate that they have been so affected. This requirement has been endorsed by the two major European Courts: by the CJEU in *Schrems* and the ECtHR in *Zakharov*. The use of independent privacy supervisors on both sides of the Atlantic with the purpose of providing rigorous scrutiny of compliance by the Executive and the legislature, would strengthen the right to an effective remedy by providing scope for affected individuals to being privacy complaints before independent supervisory authorities with investigative and decision-making powers.[39]

[39] Valsamis Mitsilegas, 'Surveillance and Digital Privacy in the Translantic "War On Terror": The Case For a Global Privacy Regime' *Columbia Human Rights Law Review* 47 3(1) (2015-16) 1, 75-77 and Edward R. Alo, 'EU Privacy Protection: A Step Towards Global Privacy' 22(3) (2014) *Michigan State International Law Review* 1195, 1131-48.

Bibliography

Books

Alexy R, *A Theory of Constitutional Rights* (Oxford University Press, 2002)

Amar, AR, '*The Bill Of Rights: Creation And Reconstruction* (Yale University Press, 1998)

Amis, M, Einstein's Monsters (Jonathan Cape, 1987) "Introduction: Thinkability" (Jonathan Cape, 1987)

Arnardóttir O.M, and Buyse A, (eds.), *Shifting Centres of Gravity in Human Rights Protection: Rethinking Relations between the ECHR, EU and National Legal Orders* (Routledge, London and New York, 2016).

Anderson D.A, *The Failure of American Privacy Law, in* Protecting Privacy 139 (Basil S. Markesinis ed., 1999.

Arai-Takahashi Y, *The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR*. (Intersentia, Antwerp, 2001).

Balkin J.M, and Siegel R.B, (eds), *The Constitution In 2020* (Oxford University Press, 2009).

Bamford J, *The Puzzle Palace: A Report on America's Most Secret Agency* (Penguin 1983).

Bamford J, *The Shadow Factory: The Ultra-Secret NSA from 9/11 to the Eavesdropping on America* (Anchor Books, 2009).

Beddard R, Human Rights and Europe (3rd edn, Cambridge University Press, 1993).

Bennett C.J, and Grant R, (eds.) *Visions of Privacy for the Digital Age* (University of Toronto Press, 1999).

Bennett C.J, and Raab C.D, *The Governance of Privacy: Policy Instruments in Global Perspectives* (MIT Press, Cambridge MA, 2nd edn, 2006).

Benvenisti E, 'Margin of Appreciation, Consensus and Universal Standards,' *New York University Journal of International Law and Practice* (1998-9) 31 843.

Bingham T, *The Rule of Law* (Penguin 2011).

Blanke, H-J, and Mangiameli S, (eds.) *The Treaty on European Union (TEU). A Commentary* (Springer, 2013).

Boehm F, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level*. (Springer 2012)

Bonnici M, and Pia J, Redefining the Relationship Between Security, Data Retention and Human Rights' in Ronald L. Holzhacker and Paul Luif, eds, *Freedom, Security and Justice in the European Union* (Springer, New York, 2014).

Brems E, and Gerards J, (eds), *Sharing Rights in the ECHR. The Role of the European Court of Human Rights in Determining the Scope of Human Rights* (Cambridge 2013).

Brin D, *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* (Addison-Wesley, Reading, MA, 1998).

Burkert H, 'Privacy-Data Protection: A German/European Perspective' in Governance of Global Networks in Christoph Engel and Kenneth H. Keller (eds) *Governance of Global Networks in the Light off Differing Local Values* (Baden-Baden, 2000).

Cambenisch J, Fischer-Hüber S, and Hansen M, (eds), *Privacy and Identity Management for the Future Internet in the Age of Globalisation* (Springer, 2015).

Campbell T, Ewing K.D., and Tomkins A, (eds), *The Legal Protection of Human Rights: Sceptical Essays* (Oxford University Press, 2011).

Campise P, (ed) *Security and Privacy in Biometrics* (Springer 2013).

Cate F.A, Privacy in the Information Age (Brookings Institution Press, 1997)

Chandler J, 'Privacy versus national security: Clarifying the Trade-off,' in Kerr I.R, Luckock C, and Steevess V.M, (eds.), *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society,* (Oxford University Press, Oxford, 2009).

Claes M, et al. (eds), Constitutional Conversations in Europe: Actors, Topics and Procedures (Cambridge: Intersentia, 2012)

Craig T, and Ludoff M.E., *Privacy and Big Data* (O'Reilly 2011).

Craig P, and de Búrca G, *EU Law: Texts, Cases and Materials* (Sixth edn, Oxford University Press, 2011).

De Hert P, and Gutwirth S, 'Privacy, data protection and law enforcement. Capacity of the individual and transparency of power,' in Claes, Erik, Duff et al. (eds.), *Privacy and the Criminal Law* (Intersentia, Antwerp, Oxford, Oxford, 2006).

Deibert R, et al (eds), *Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace'* (Massachusetts Institute of Technology, 2010),

Delany H, Carolan E, and Murphy C, *The Right to Privacy: A Doctrinal Comparative Analysis* (Round Hall 1998).

DeLondris F, 'Governance gaps in EU counter-terrorism: implications for democracy and constitutionalism' in De Londris F, and Doody J, (eds), *The Impact, Legitimacy and Effectiveness of EU Counter-Terrorism* (Routledge London, 2013).

Demaris O, *The Director* (New York, 1975).

DeVires S, Bernitz U, and Weatherill S, (eds.), *The Protection of Fundamental Rights After Lisbon* (Hart Publishing, Oxford and Portland, Oregon, 2013).

Deibert R, et al (eds), *Access Controlled: The Shaping of Power, Rights and Rule in Cyberspace'* (Massachusetts Institute of Technology, 2010).

Dworkin R, *Taking Rights Seriously* (Harvard University Press, 1977).

Egan S, (ed). *International Human Rights Perspectives from Ireland* (Dublin, Bloomsbury, 2015).

Fabbrini F, *Fundamental Rights in Europe. Challenges and Transformations in Comparative Perspective* (Oxford University Press, 2014).

Fichera M, and Jens Kremer, *Law and Security in Europe: Reconsidering the Security Constitution* (Intersentia, 2013).

Follesdal A, Peters B, and Ulfstein G, *Constituting Europe. The European Court of Human Rights in a National, European and Global Context* (Cambridge 2013).

Finn R, Wright D and Friedewald M, 'Seven Types of Privacy,' in Gutwirth, Serge,

Glendon, M.A, *Rights Talk. The Impoverishment of Political Discourse*, (New York 1991).

Fuller Lon L, *The Morality of Law* (Yale University Press, New Haven 1969).

George R.Z, and Kline R.D, *Intelligence And The National security Strategist. Enduring Issues and Challenges* (Bowman and Littlefield, New York, 2006).

Grabenwarter C, and Pabel K, ' Fundamental Rights - The Charter and the ECHR' in Blanke H-J, and Mangiameli S, (eds.) *The Treaty on European Union (TEU). A Commentary* (Springer, 2013) 287-348.

Greenwald G, *How would a Patriot Act? Defending American Values from a President Run Amok* (Working Assets Publishing, 2006).

Greenwald G, 'No place to hide: Edward Snowden, the NSA and the U.S. Surveillance State (Picador, London 2014).

Harding L, *The Snowden Files* (Random House, 2014).

Hijmans H, *The European Union as Guardian of Internet Privacy. The Story of Article 16 TFEU* (Springer, 2016).

Hofmann H.C.H, Rowe GC, and Türk A. H, *Administrative Law And Policy Of The European Union* (Oxford University Press, 2011).

(---- ---) *International Law at the Time of its Codification, Essays in Honour of Judge Roberto Ago* (Giuffrè, Milan 1987).

Jackson G.B., *Rape of the American Constitution By Its Own Government* (Mill City Press, 2016).

Jacobs F, *The European Convention on Human Rights* (Oxford, 1975).

Janis M.W, and Kay, R.S, *European Human Rights Law* (University of Connecticut Law School Foundation, 1990).

Johnson L.K, *A Season of Inquiry: The Senate Intelligence Investigation* (University of Kentucky Press, Lexington, 1985).

Johnson L.K, *American Secret Power: The CIA in a Democratic Society* (Oxford University Press, New York, 1989).

Kamlah R.B, 'The Invasion of privacy by Electronic Listening devices in the United States and Germany,' International Symposium on Comparative Law (University of Ottawa Press, 1970).

Kelleher D, *Privacy and Data Protection in Ireland* (Tottel 2006).

Keller H, and Sweet Stone A, (eds) *A Europe of Rights. The Impact of the ECHR on National Legal Systems* (Oxford University Press, 2008).

Kerr I, Lucock C, and Stevens V, (eds.) *Lessons from the Identity Trail: Anonymity, Privacy and Identity in a Networked Society* (Oxford University Press, 2009).

Knott S.F, *Secret and Sanctioned: Covert Operations and the American Presidency* (Oxford University Press, 1996).

Kommers D.P, and Finn J.E, *American Constitutional Law, Essays, Cases and Comparative Notes.* (Wadsworth Publishing Company 1998).

Kosta V, Skoutaris N, and Tzevekos V, (eds.), *The EU Accession To The ECHR* (Hart, Oxford And Portland, Oregon, 2004).

Kroes, Q.R., *E-Business Law of the European Union* (2nd edn, Wolters Lkuwer, Netherlands, 2010) .

Lambert P, *Data Protection Law in Ireland*. (Clarus Press 2013).

Leenes R, de Hert P, and Poullet Y, (eds.) *European Data Protection: Coming of Age* (Springer 2013).

Lynskey O, *The Foundations of EU Data Protection Law* (Oxford University Press, 2015).

Markesans B.S, (ed), *The Clifford Chance Lectures* (Oxford 1999).

Martinico G, and Pollicino O, 'Report on Italy' in Giuseppe Martinico and Oreste Pollicino (eds) *The National Judicial Treatment of the ECHR and EU Laws: A Comparative Perspective* (Europa Law Publishing, 2010).

Macdonald, R.J, 'The Margin of Appreciation in the Jurisprudence of the European Court of Human Rights', in Anon (ed), *International Law at the Time of its Codification, Essays in Honour of Judge Roberto Ago* (Giuffrè, Milan 1987).

Macdonald R. St. J, Natcher F and Petzold H., (eds.) *The European System for the Protection of Human Rights* (Dortrecht London: Martinus Nijhoff, 1993.

Martinico G and Pollicino O, 'Report on Italy' in Martinico G, and Pollicino O, (eds) *The National Judicial Treatment of the ECHR and EU Laws: A Comparative Perspective* (Europa Law Publishing, 2010).

(----- -----) *Mass surveillance. Who is watching the watchers?* (Council of Europe, 2016).

Medsger B, *The Burglary - the Discovery of J. Edgar Hoover's Secret FBI*. (Alfred Knopf 2014)

McIntyre T.J., 'Implementing Information Privacy Rights in Ireland' in Suzanne Egan, ed. *International Human Rights Perspectives from Ireland* (Dublin, Bloomsbury, 2015) 271-287.

David Frost *Frost/Nixon* (London, 2007).

Merrils J.G, The development of International Law by the European Court of Human Rights, (2nd edn, Manchester University Press, 1993).

Mjll A.O, and Buyse A, (eds.), *Shifting Centres of Gravity in Human Rights Protection: Rethinking Relations between the ECHR, EU and National Legal Orders* (Routledge, London and New York, 2016).

Morrisson C.C, 'Margin of Appreciation in European Human Rights Law.' *Human Rights Law Journal* (1973) 6 263.

Nardell G, 'Levelling Up: Data Privacy and the European Court of Human Rights,' in Gutwith S, Poullet Y, and De Hert P, (eds) *Data Protection in a Profiled World* (Springer 2010).

Nietzsche F, *Untimely meditations*. (Cambridge University Press, 1997).

Nissenbaum H, *'Privacy in Context: Technology, Policy, and the Integrity of Social Life*.' (Stanford University Press, 2010).

Nowak M, *U.N. Convention on Civil and Political Rights CCPR Commentary* (2nd revised edition) (Kehl an Rhein Engel 2005).

Oates S.B, *Let the Trumpet Sound. The Life of Martin Luther King, Jr.* (Search Press, London 1982).

Papacharissi, Z.L, and Gibson P.L, 'Fifteen Minutes of Privacy: Privacy, Sociality, and Publicity on Social Network Sites' in Trepte Sabine and Reinecke Leonard (eds), *Perspectives on Privacy and Self-Disclosure in the Social Web* (Springer 2011).

Peers S, and Ward A, *The European Union and Fundamental Rights* (Oxford, Hart, 2004).

Petzold H, 'The Convention and the Principle of Subsidiarity,' in *The European System For The Protection Of Human Rights* (Martinus Nijhoff, Dordrecht, 1993).

Post R.C, *The Social Foundation of Privacy in Constitutional Domains: Democracy, Community, Management*. (Harvard University Press, 1995)

Posner R.A, *The Economics of Justice.* (Harvard University Press, 1983).

Raab C.D, 'From Balancing to Steering: New Directions for Data Protection' in Bennett, C.J, and Grant R, (eds.) *Visions of Privacy for the Digital Age* (University of Toronto Press, 1999) 68-93.

Rengel, A, *Privacy in the 21st Century* (Hotei Publishing, Leiden, 2014).

Rodotà S, 'Data Protection as a Fundamental Right' in *Reinventing Data Protection*? Gutwith S, et al, (eds), (Springer, New York, 2009).

Rotunda R.D, and Nowak J.E, *Treatise on Constitutional Law: Substance and Procedure* (2nd edn West 1992).

Rudalevige A, 'The New Imperial Presidency' (University of Michigan Press, 2005).

Samaha J, *Criminal Procedure* (Cengage Learning 9th edition 2015).

Schlessinger, Jr, A., *The Imperial Presidency* (Houghton Mifflin, New York 1973).

Schneier B, *Beyond Fear. Thinking Sensibly About Security in an Uncertain World* (Copernicus Books, New York, 2003).

Schneier B, *Data And Goliath: The Hidden Battles to Collect Your Data and Control Your World* (W.W. Norton and Company, New York and London, 2015).

Schoenfeld G, *Necessary Secrets: National Security, The Media, and the Rule of Law* (Norton and Company 2010).

Douglas-Scott S, 'Fundamental Rights in the EU: The Ambiguity of Judicial Review,' 268-296 in Campbell T, Ewing K.D, and Tomkins A, (eds), *The Legal Protection of Human Rights: Sceptical Essays* (Oxford University Press, 2011).

Schwartz P.M., and Reidenbeg J.R., Data Privacy Law: A Study of United States Data Protection (Michie 1996).

(----- ----) *Spanish Yearbook Of International Law* Volume IV, 1995-1996, (Martinus Nijhoff Publishers, Netherlands, 2001).

Solove D.J, 'The Digital Person: Technology and Privacy in the Digital Age' (New York University Press, 2004).

Solove D, *Understanding Privacy* (Harvard 2008).

Summers A, *The Arrogance of Power. The Secret World of Richard Nixon.* (Gollancz, 2000).

Taylor T, *Two Studies in Constitutional Interpretation* (Ohio State University Press, 1969).

Theoharis AG, and Cox J.S, *The Boss: J. Edgar Hoover and the Great American Inquisition*. (Temple University Press 1988).

Toomey J, *Change You Can Really Believe In. The Obama Legacy Of Broken Policies and Failed Policies* (AuthorHouse, 2012).

Treverton G.F., *Intelligence for an Age of Terror* (Cambridge University Press, 2009) 249.

Tribe LH, *American Constitutional Law* (2nd edn, West Academic Publishing, 1988).

Trudel P, 'Privacy Protection on the Internet: Risk Management and Networked Normativity,' in Gutwirth S, Poullet Y, De Hert P, de Terwangne C and Nouwt S, (eds.), *Reinventing Data Protection?* (Springer 2009).

Tuori Kaatlo 'A European Security Constitution' in Massimo Fichera and Jens Kremer, *Law and Security in Europe: Reconsidering the Security Constitution* (Intersentia, 2013).

Van Dijk P and Van Hoof GJ.H., *Theory and Practice of the European Convention on Human Rights*. (3rd ed., The Hague 1998).

Van Dijk P, et al (eds.), *Theory and Practice of the European Convention on Human Rights* (Intersentia, 2006).

Waldron, J, *Security and Liberty: The image of a Balance* (Blackwell Publishing, 2003).

Westin A.F., *Privacy and Freedom* (Atheneum 1967).

Wise D, *The American Police State* (New York, 1976).

Wright D, and De Hert P, (eds), *Privacy Impact Assessment* (Springer 2012).

Wright D and Kreissl R, (eds) *Surveillance in Europe* (Routledge, Oxon and New York, 2015).

Zedner L, Security. Key Ideas in Criminology (Routledge, New York, 2009).

Zeegers K, *International Criminal Tribunals and Human Rights Law. Adherence and Continuance* (Springer, 2016.

Academic Journals

Aberbach J.D., 'What's Happened to the Watchful Eye?' 29(1) (2000) *Congress and the Presidency* 3.

Aleinikoff A.T, 'Constitutional Law in an Age of Balancing' 96(5) (1987) *The Yale Law Journal* 943.

Alo, Edward R., 'EU Privacy Protection: A Step Towards Global Privacy' 22 (3) (2014) *Michigan State International Law Review* 1096.

Alphran DM, 'Changing Tides: A Lesser Expectation of Privacy In A Post 9/11 World' 13(1) (2009) *Richmond Journal And The Public Interest* 89.

Amsterdam A.G. 'Perspectives on the Fourth Amendment' 58 (1973-74) *Minnesota Law Review* 349.

Amsterdam A.G, and Atkinson R.L, 'The Fourth Amendment's National Security Exception: Its History and Limits' 66 (5) (2013) *Vanderbilt Law Review* 1343.

Aquilina K, 'Public security versus privacy in technology law: A balancing act?' 26(2) (2010) *Computer Law and Security Review* 130.

Atkinson R.L, 'The Fourth Amendment's National Security Exception. Its History and Limits.' 66(5) (2013) *Vanderbilt Law Review* 1346.

Baghai K, 'Privacy as a Human Right: A Sociological Theory' 46(5) (2012) *Sociology* 951.

Balkin J.M. and Levinson S, 'The Process of Constitutional Change: From Partisan Entrenchment to the National Surveillance State' 75(2) (2006) *Fordham Law Review* 489.

Balkin J.M, 'The Constitution in the National Surveillance State' 93 (2008) *Minnesota Law Review* 1.

Balthasar A, 'Complete Independence' of National Data Protection Supervisory Authorities – Second Try: Comments on the Judgment of the CJEU of 16 October 2012, C-614/10 (*European Commission v. Austria*), with Due Regard to its Previous Judgment of 9 March 2010, C-518/07 (*European Commission v. Germany*)' 9(3) (2013) *Utrecht Law Review* 26.

Banks, W.C, 'Programatic Surveillance and FISA: of Needles and Haystacks' (2010) 88(7) *Texas* 1633.

Banks, C.P, 'Security and Freedom After September 11: Limits and Ethical Costs of Terrorism Prosecutions' 1(1) (2010-11) *Public Integrity* 5.

Barak A, 'Proportionality and Principled Balancing' 4 (2010) *Law and Ethics of Human Rights* 1

Bar-Gill O, and Friedman B, 'Taking Warrants Seriously,' 106(4) (2012) *Northwestern Law Review* 1609.

Barr B, 'Post 9/11 Electronic Surveillance Society Severely Undermining Freedom' 41(4) (2007) *Valparaiso University Law Review* 1383.

Benkler Y, 'A Public Accountability Defence for National Security Leakers and Whistelblowers' 8 (2014) *Harvard Law and Policy Review* 281.

Bennett R.W., 'Objectivity in Constitutional Law' 132 (1984) *University of Pennsylvania Law Review* 445.

Baumer D.I., Earp, J.B., and Poindexter J.C, 'Internet Privacy Law: a comparison between the United States and the European Union.' 23 (2004) *Computers and Security* 400.

Bender A, 'An Elementary Approach to the Rule of Law' 2 (2010) *Hague Journal on The Rule of Law* 48.

Bender D, 'E.U. or U.S. : which has more actual privacy? 21(1) 2015) *Computer Law and Security Review* 18.

Bennett S.C. 'The "Right to Be Forgotten" Reconciling EU and US Perspectives' 30(1) (2012) *Berkeley Journal of International Law* 161.

Benvenisti, E, 'Margin of Appreciation, Consensus and Universal Standards,' 31 (1998-99) *New York University Journal of International Law and Practice* 843.

Bernstein N.J., and Mann T.E, 'When Congress Checks Out' 85(6) (2006) *Foreign Affairs* 67.

Berman E, 'Two Faces of the Foreign Intelligence Surveillance Court' 91(4) (2016) *Indiana Law Journal* 1191.

Besselink L.F.M., 'National and constitutional identity before and after Lisbon' 6(3) (2010) *Utrecht Law Review* 36.

Besson S, 'The European Eunion and Human Rights: Towards A Post-National Human Rights Institution? 6(2) (2006) *Human Rights Law Review* 323.

Bignami F, European Versus American Liberty: 'A Comparative Privacy Analysis of Antiterrorism Data Mining,' 48 3(3) (2007) *Boston College Law Review* 609.

Bignami F, 'Privacy and Law Enforcement in the European Union: The Data Retention Directive.' 8(1) (2007) *Chicago Journal of International Law* 233.

Bignami F, 'The Case for Tolerant Constitutional Patriotism: The Right to Privacy Before the European Courts.' 41 (2008) *Cornell International Law Journal* 211.

Bigo D, et al, 'Mass Surveillance of personal Data by EU Member States and its Compatibility with EU Law' 61(1) (2013) CEPS Paper in Liberty and Security 39.

Birkenstock G.E., 'The Foreign Intelligence Surveillance Act and Standards of Probable Cause: An Alternative Analysis' 80 (1992) *Georgetown Law Journal* 843.

Blakeney S, 'The Data Retention Directive: Combating Terrorism or Invading Privacy? 13(5) (2007) *Computer and Telecommunications Law Review* 153.

Blanchette J.F, and Johnson D.G, 'Data Retention and the Panoptic Society: The Social Benefits of Forgetfulness.' 18(1) (2002) *The Information Society* 33.

Bloom R, and Dunn W.J, 'The Constitutional Infirmity of Warrantless NSA Surveillance: The Abuse of Presidential Power And The Injury To The Fourth Amendment' 15 (2006) *William and Mary Bill of Rights Journal* 147.

Blume, Peter, 'It Is Time For Tomorrow: EU Data Protection Reform And The Internet' 18(8) (2015) *Journal of Internet Law 3*

Bogdandy A, 'The EU as a Human Rights Organisation? - Human Rights and the Core of the European Union' 37(6) (2000) *Common Market Law Review* 1307.

Bradley C.M, 'Two Models of the Fourth Amendment,' 83 (1985) *Michigan Law Review* 1468.

Brand, J.S., 'Eavesdropping on our Founding Fathers: How a Return to the Republic's Core Democratic Values Can Help Us Resolve the Surveillance Crisis' 6(1) (2015) *Harvard National Security Journal* 1.

Brauch J.A, 'The Margin Of Appreciation And The Jurisprudence Of The European Court Of Human Rights: Threat To The Rule Of Law' 11 (2005) *Columbia Journal Of European Law* 113.

Brauch J.A, 'Human Rights Protections In The Post-9/11 World' *Quinnipiac Law Review* 31 (2013) 339.

Breglio N.K., 'Leaving FISA Behind: The Need To return to Warrantless Foreign Intelligence Surveillance' 113 (2003) *The Yale Law Journal* 179.

Brems E, 'The Margin of Appreciation Doctrine in the Case-Law of the European Court of Human Rights' 36 (1996) *Zeitschrift für Auslandisches Offentliches Recht und Volkrecht* 240.

Breyer P, 'Telecommunications Data Retention and Human Rights: The Compatibility of Blanket Traffic Data Retention with the ECHR.' 11(3) (2005) *European Law Journal* 365.

Broggi J.J., 'Building On Executive Order 13,686 To Encourage Information Sharing For Cybersecurity Purposes' 37 (2014) *Harvard Journal of Law and Public Policy* 653.

Bromwich D, 'Obama's Mental Bookkeeping,' (27 May, 2011) *London Review of Books.*

Brown I, 'Systematic government access to private-sector data in the United Kingdom' 4(2) (2012) 230.

Brown W.F. and Cinquerana A.R. 'Warrantless Physical Searches for Foreign Intelligence Purposes: Executive Order 12,333 and the Fourth Amendment' (35(1) (1985) *Catholic University Law Review* 97.

Brown I, 'Communications data retention in an evolving internet.' 19(2) (2011) *International Journal of Law and Information Technology* 95.

Bunn A, 'The curious case of the right to be forgotten' 31 (2015) *Computer Law and Security Review* 336 .

Burke K.C, 'Secret Surveillance and the European Convention on Human Rights' 33 (1981) *Stanford Law Review* 1113.

Burke C.A., 'Foreign Intelligence Surveillance Gathering of Prosecution? 6(3) (1982) *Fordham International Law Journal* 501.

Butler A, 'Standing Up to Clapper: How to Increase Transparency and Oversight of FISA Surveillance' 45 (2013) *New England Law Review* 55.

Byhrave L, 'Data Protection Pursuant to the Right to Privacy in Human Rights Treaties' 6(3) (1998) *International Journal of Law and information Technology* 247.

Byrne, A, 'European Data Protection Uncapped: A Critical Analysis of *Google Spain v. AEPD*' 38 (2016) *Loyola of Los Angeles International and Comparative Law Review* 115.

Casale D, 'EU Institutional and Legal Counter-Terrorism Framework.' 1(1) (2008) *Defence Against Terrorism Review* 49.

Cate F.H, and Litan R, 'Constitutional Issues in Information Privacy, Constitutional Issues in Information Privacy' 9 (2002) *Michigan Telecommunications and Technology Law Review* 35.

Chenault J, 'The Myth of Freedom of Information in the United States' 78(2) (2014) *University of Louisville* 32.

Civiletti B, 'Intelligence Gathering and the Law: Conflict or Compatibility?' 48(6) (1980) *Fordham Law Review* 883.

Clark B, 'Freedom of art v personality rights: ban upheld on the real life novel *Esra* 3(4) (2008) *Journal of Intellectual Property Law and Practice* 221.

Cohen J.E, 'Privacy, Visibility, Transparency and Exposure' 181 (2008) *The University of Chicago Law Review* 75.

Cohen J.E, 'What Privacy is For.' 126 (2013) *Harvard Law Review* 1904.

Cole D, 'Reviewing the Nixon Doctrine: NSA Spying, the Commander-In-Chief, and Executive Power in the War on Terror,' 13(1) (2006) *Washington and Lee Journal of Civil Rights and Social Justice* 17.

Cole D, and Lederman M, 'The National Security Agency's Domestic Spying Program: Framing the Debate.' 81(4) (2006) *Indiana Law Journal* 1355.

Cole D, 'Can Privacy Be Saved?' (March 6 2014) *New York Review of Books*

Costa L, and Poullet Y, 'Privacy and the regulation of 2012' 28 (2012) *Computer Law and Security Review* 254.

Costello R, 'The Right To Privacy, Clandestine Surveillance And International Trade in The United States And Europe' 17(1) (2014) *Trinity College Law Review* 37.

Crowther, Hannah, 'The draft data protection Regulation: can we start counting our chickens?' 14(5) (2014) *Privacy & Data Protection* 9.

Davis R.N, 'Striking the Balance: National Security vs. Civil Liberties' 29(1) (2004) *Brooklyn Journal of International Law* 175.

Davies G and Trigg G, 'Being data retentive: a knee jerk reaction?' 11(1) (2006) *Communications Law* 18.

De Búrca G, 'The drafting of the European Union Charter of Fundamental Rights' 26(2) (2001) *European Law Review* 126.

De Búrca G, 'The European Court of Justice and the International Legal Order After *Kadi'* 51(1) (2010) *Harvard International Law Journal* 1.

De Búrca G, 'After The EU Charter Of Fundamental Rights: The Court Of Justice As A Human Right Adjudicator? 20 (2013) *Maastricht Journal of European and Comparative Law* 168.

De Búrca G, 'The Domestic Impact of the EU Charter of Fundamental Rights' 49(1) (2013) *The Irish Jurist* 49.

Deflem M, and McDonough S, 'The Fear of Counterterrorism: Surveillance and Civil Liberties since 9/11' 52(1) (2015) *Global Society* 70.

Determann L, and Guttenberg K.T, 'On War and Peace in Cyberspace. Security, Jurisdiction' 41(4) (2014) *Hastings Constitutional Law Quarterly* 875.

De Hert P, 'Balancing security and liberty within the European human rights framework,' 1 (2005) *Utrecht Law Review* 74.

De Hert P, Gutwirth S, Moscibroda, Wright D, and González Fuster G, 'Legal safeguards for privacy and data protection in ambient intelligence' 13(6) (2009) *Personal and Ubiquitous Computing* 435.

De Hert P, and Papakonstantinou V, 'The Proposed data protection Regulation replacing Directive 95/46/EC. A sound system for the protection of individuals'. 28(2) (2012) *Computer Law and Security Review* 30.

Del Moral, I de la R, 'The Increasingly Marginal Appreciation of the Margin-of-Appreciation Doctrine,' 6(7) (2006) *German Law Journal* 611.

De Londras F, 'Accounting for Rights in EU Counter-Terrorism: Towards Effective Review' 22(2) (2016) *Columbia Journal of European Law* 237.

De Poorter J.C.A., 'Constitutional Review in the Netherlands: A Joint Responsibility' 9(2) (2013) *Utrecht Law Review* 89.

DeVos S, 'The Google-NSA Alliance: Developing Cybersecurity at Internet Speed" 21(1) (2010) *Fordham Intellectual Property, Media and Entertainment Law Journal* 173.

Donohue L.K, 'Bulk Metadata Collection: Statutory and Constitutional Considerations' 37 (2014) *Harvard Journal of Law and Public Policy* 757.

Donohue L.K, 'Section 702 and the Collection of International Telephone and Internet Content' 38(1) (2015) *Harvard Journal of Law and Public Policy* 117.

Douglas-Scott, 'The European Union's Fundamental Rights Myth' Journal of Common Market on and Human Rights after the Treaty of Lisbon,' 11(4) (2011) *Human Rights Law Review* 645.

Edwards G.M, and A.J.I, 'Security policies and the weakening of personal data protection in the European Union' 29 (2013) *Computer Law and Security Review* 255.

Egan S, 'The European Convention on Human Rights Act 2003: A Missed Opportunity for Domestic Human Rights Litigation,' 25(1) (2003) *Dublin University Law Journal* 230.

Eger J, "Emerging Restrictions on Transnational Data Flows: Privacy Protections or Non-Tariff Barriers? 10 (1978) *Law and Policy in International Business* 1065.

Etzioni A, 'Imperfections of Select New Technologies for Individual Rights and Public Safety' 15(2) (2002) *Harvard Journal of Law and Technology* 258.

Fabbrini F, 'Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and surveillance in the United States' 28 (2015) *Harvard Human Rights Journal* 67.

Feingold C.S, 'The Doctrine of Margin of Appreciation and the European Convention on Human Rights' 53 (1977) *Notre Dame Law Review* 90.

Ferguson J.R., 'Government Secrecy After The Cold War: The Role of Congress' 34(3) 1993) *Boston College Law Review* 541.

Ferguson A.G, 'The Big Data Jury' 91(3) 2016) *Notre Dame Law Review* 935.

Ferguson A.G, 'The Internet of Things and the Fourth Amendment' 104(4) (2016) *California Law Review* 805.

Guthrie Ferguson A.G., 'The "Smart" Fourth Amendment' 102 (2017) *Cornell Law Review* 547.

Fischer L.E, 'Guilt By Expressive Association: Political Profiling, Surveillance And The Privacy of Groups' 46(4) (2004) *Arizona Law Review* 621.

Ford, C.M, 'Intelligence Demands in a Democratic State: Congressional Intelligence Oversight' 81 (2007) *Tulane Law Review* 721.

Forsyth B, 'Banning Bulk: Passage of the USA Freedom Act and Ending Bulk Collection 72 (2015) *Washington and Lee Law Review* 1307.

Frantziou E, 'Further Developments in the Right to be Forgotten: The European Court of Justice's Judgement in case C-132/12, *Google Spain, SL, Google Inc v Agencia Espanola de Protection de Datos*' 14 (2014) *Human Rights Law Review* 761.

Fried C, 'Privacy' 77 (1968) *Yale Law Journal* 475.

Fromholz J.M, 'The European Union Data Privacy Directive.' 15 (2000) *Berkeley Technology Law Journal* 461.

Froomkin M.A, “The Death of Privacy?” 52 (2000) Stanford Law Review 1461.

Fuchs C, 'Towards an alternative concept of privacy.' 9(4) (2011) *Journal of Information, Communication and Ethics in Society* 220.

Fuld J.S, 'Data Mining and Privacy,' 11(1) (2000) *Albany Law Journal of Science and Technology* 105.

Funk W, 'Electronic Surveillance of terrorism: The Intelligence/Law Enforcement Dilemma - A History' 11(4) (2007) *Lewis and Clark Law Review* 1099.

Fuster G.G, and Gellert R, 'The Fundamental Right of data protection in the European Union: in search of an uncharted right' 26(1) 2012) *Review of Law, Computers and Technology* 73.

Gajda A, 'Judging Journalism: The Turn Toward Privacy and Judicial Regulation of the Press' 97 (2009) *California Law Review* 1039.

Gearty C, 'The State of Freedom in Europe' 21(6) (2015) *European Law Journal* 706.

Gibbs H.A, 'Reasoned 'Balance' in Europe's Area of Freedom, Security and Justice' 17(1) (2011) *European Law Journal* 121.

Gilbert F, 'Demystifying the United States Patriot Act' 16(8) (2013) *Journal of Internet Law* 1.

Gillespie A, 'Regulation of internet surveillance' 4 (2009) *European Human Rights Review* 552.

Gόmez-Arostegui H., 'Defining Private Life Under The European Convention On Human Rights By Referring To Reasonable Expectations' 35 (2005) *California Western International Law Journal* 153.

Gorman S, 'The Ashcroft Doctrine' 34(51/52) (2002) *National Journal* 3712.

Grano J.D, 'Rethinking the Fourth Amendment Warrant Requirement' 19 1982) *American Criminal Law Review* 603.

Greer S, "Balancing" and the European Court of Human Rights: a contribution to the Habermas-Aleexy Debate' 63(2) (2004) *Cambridge Law Journal* 1

Greer S, 'What's Wrong with the European Convention on Human Rights?' 30(3) (2008) *Human Rights Quarterly* 680.

Griswold E, 'The Right to be let alone' 55 (1960) *Northwestern Law Review* 216.

Granger M.P, and Irion K, 'The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection' 39(6) (2014) *European Law Review* 835.

Gray D, and Citron D.K, 'A Shattered Looking Glass. The Pitfalls and Potential of the Mosaic theory of Fourth Amendment Privacy' 14(2) (2013) *North Carolina Journal of Law and Technology* 381.

Gray D, 'Fourth Amendment Remedies As Rights: The Warrant Requirement' 96 (2016) *Boston University Law Review* 425.

Gross O, and Ní Aoláin F, 'From Discretion to Scrutiny: Revisiting the Application of the Margin of Appreciation Doctrine in the Context of Article 15 of the European Convention on Human Rights' 23(3) (2001) *Human Rights Quarterly* 625.

Guild E, and Carrera S, 'The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive' 65 (2014) *CEPS Paper in Liberty and Security in Europe* 1.

Gutierrez G, 'The Imbalance of Security and Privacy: What the Snowden Revelations Contribute to the Data Mining Debate' 19(2) (2015) *Intellectual Property Law Bulletin* 161.

Halberstam D, and Möllers C, 'The German Constitutional Court says 'Ja zu Deutschland' 10(8) (2009) *German Law Journal* 1241.

Halberstein D, 'It the Autonomy, Stupid!' A Modest Defence of *Opinion* 2/13 on EU Accession to the ECHR, and the Way Forward' 16(1) (2015) *German Law Journal* 105.

Harper J, 'Reforming Fourth Amendment Privacy Doctrine' 57 (2008) *American University Law Review* 1381.

Hartzog W, and Stutzman F, 'The Case for Online Obscurity' 101(1) (2013) *California Law Review* 1.

Helfer L.R, and Slaughter AM,, 'Toward a Theory of Effective Supranational Adjudication' 107 (1997) *The Yale Law Journal* 273.

Henkin L, 'Privacy and Autonomy' 74 (1974) *Columbia Law Review* 1410.

Heymann P.B, 'An essay on Domestic Surveillance' 8 (2016) *Journal of National Security Law and Policy* 421.

Higgins R, 'Derogations under Human Rights Treaties' 48(1) (1976) *British Yearbook of International* 281.

Hornung G, and Schnabel C, 'Data protection in Germany I: The population census decision and the right to informational self-determination' 25(1) 2009) *Computer Law and Security Review* 84.

Husovec M, 'Slovak Constitutional Court Annuls National Data Retention Provisions' 1 (2015) *European Data Protection Law Review* 227.

Huynh A, 'What Comes After Get A Warrant' 101 (2015) *Cornell Law Review* 187.

James M.C, 'A Comparative Analysis of the right to Privacy in the United States, Canada and Europe' 29 (2014) *Connecticut Journal of International of Internal Law* 259, 297.

Johnson L.K, 'Legislative Reform of Intelligence Policy' 17(5) (1985) *Polity* 49.

Johnson L.K, 'The CIA and the Question of Accountability' 12(1) (1997) *Intelligence and National Security* 178.

Johnson L.K, 'Congressional Supervision of American's Secret Agencies: The Experience and Legacy of the Church Committee' 64(1) (2004) *Public Administration Review* 3.

Johnson L.K, 'The Church Committee Investigation of 1975 and the Evolution of Modern Intelligence Accountability' 23(2) (2008) *Intelligence and National Security* 198.

Johnson L.K, 'Ostriches, Cheerleaders, Skeptics and Guardians: Role Selection by Congressional Intelligence Overseers' 28(1) (2008) *SAIS Review* 2893.

Kadidal S, 'NSA Surveillance: The Implications for Civil Liberties' 10(1) (2014) *Journal of Law and Policy for the Information Society* 433.

Kay R.S, 'The European Convention on Human Rights and the Authority of Law' 8(2) (1993) *Connecticut Journal of International Law* 217.

Kaiser A.B, 'Case Comment: German data retention provisions unconstitutional in their present form; decision of 2 March 2010, NJW, p. 833' 6(3) (2010) *European Constitutional Law Review* 503.

Kelley K, 'The Foreign Intelligence Surveillance Act of 1978' 13 (1980) *Vanderbilt Journal of Transnational Law* 719.

Kerr O.S. 'A Reader's Guide to the Stored Communication Act and a Legislator's guide to Amending It.' 72(6) (2004) *The George Washington Law Review* 1701.

Kerr O.S, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution'* 102 (2004) *Michigan Law Review* 801.

Kerr O.S., 'Do We Need A New Fourth Amendment' 107(6) (2009) *Michigan Law Review* 951.

Kerr O.S, 'Applying The Fourth Amendment to the Internet: A General Approach' 62(4) (2009-2010) *Stanford Law Review* 1005.

Kerr OS, 'An Equilibrium-Adjustment Theory of the Fourth Amendment' 125 (2011) *Harvard Law Review* 476.

Kerr OS, 'The Fourth Amendment and the Global Internet' 67(2) (2015) *Stanford Law Review* 285.

Kesan JP, Hayes CM, and Bashir M, 'A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy' 91 (2016) *Indiana Law Journal* 267.

Kierkegaarda S, Watersb N, Greenleafc G, Bygraved LA., Lloyd I and Saxby S, 30 years on – The review of the Council of Europe Data Protection Convention 108' 27 (2011) *Computer Law and Security Review* 223.

Kokott J, and Sobotta C, 'The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR' 3(4) (2013) *International Data Privacy Law* 222.

Korbin S.J, 'Safe harbours are hard to find: the trans-Atlantic data privacy dispute, territorial jurisdiction and global governance' 30 (2004) *Review of International Studies* 111.

Krotoszynski R.J, 'The Polysemy of Privacy' 88(3) (2013) *Indiana Law Journal* 881.

Krotoszynski R.J, "Reconciling Privacy And Speech In The Era of Big Data: A Comparative Legal Analysis' 56 (2015) *William And Mary Law Review* 1279.

Kosta E, and Valcke P, 'Retaining the data retention directive' 22(5) (2006) *Computer Law & Security Report* 380.

Kosta E, 'The Way to Luxembourg: National Court Decisions on the Compatibility of the Data Retention Directive with the Rights to Privacy and Data Protection' 10(3) (2010) *scripted* 339.

Kratochvíl J, 'The Inflation of the Margin of Appreciation by the European Court of Human Rights,' 29(3) (2001) *Netherlands Quarterly of Human Rights* 324.

Kris D, 'Trends and Predictions in Foreign Intelligence Surveillance: The FAA and Beyond' 8 (2016) *Journal of National Security Law and Policy* 377.

Krotoszynski Jr J, 'The Polysemy of Privacy' 88(3) (2013) *Indiana Law Journal* 881.

Kühling J, and Heitzer S, 'Returning through the National Back Door? The future of data retention after the ECJ Judgment on Directive 2006/24 in the UK and Elsewhere' 40(2) (2015) *European Law* 263.

Ku S.R, 'The Founder's Privacy: The Fourth Amendment and the Power of Technological Surveillance' 86 (2002) *Minnesota Law Review* 1325.

Kuleza J, 'USA Cyber Surveillance and EU Personal Data Reform: PRISM's Silver Lining?' 2(2) (2014) *Groningen Journal of International Law* 72.

Kumm M, 'Constitutional Rights as Principles. On the Structure and domain of Constitutional Justice. A review essay on A Theory of Constitutional Rights' 2(3) (2004) *International Journal of Constitutional Law* 574.

Kuner C, 'The European Union and the Search for an International Data Protection Framework' 2(2) (2014) *Groningen Journal of International Law* 55.

Kurek J, 'How To Achieve An Active Balance Between Effective Preventing Crime And Protecting Privacy Of Citizens' Online Search As A New Challenge For Justice' 3(3) (2009) *Masaryk University Journal of Law and Technology* 377.

LaFave W.R, 'Fourth Amendment Vagaries of Probable Cause, Imperceptible Plain View, Notorious Privacy and Balancing Askew' 74 (1983) *Journal of Criminal Law and Criminology* 1171.

Lam, C, 'Unsafe Harbor: The European Union's Demand For Heightened Data Privacy Standards In Schrems v Irish Data Protection Commissioner' 40(3) (2017) *Boston College International and Comparative Law Review* 1.

Langston M.B., 'Rediscovering Congressional Intelligence Oversight: Is Another Church Committee Possible Without Frank Church?' 2 (2015) *Texas A & M Law Review* 433.

Lanois P, 'Time To Forget: EU Privacy Rules And the Right To request The Deletion of data On The Internet' 18(4) (2014) *Journal Of Internet Law* 20.

Lazowski A, and Wessel R.A, 'When Caveats Turn into Locks: *Opinion* 2/13 on Accession of the European Union to the ECHR' 16(1) (2015) *German Law Journal* 179.

Lenaertes K, 'Fundamental Rights in the European Union' 25(6) (2000) *European Law Review* 575.

Letsas G, 'The Truth in Autonomous Concepts: How To Interpret the ECHR' 15 (2004) *European Journal of International Law* 279.

Letsas G, 'Two Concepts of the Margin of Appreciation' 26(4) (2006) *Oxford Journal of Legal Studies* 705.

Lightle R, 'Balancing National Security Policy: Why Congress Must Assert Its Constitutional Check On Executive Power' 42 (2014) *Florida State University Review* 255.

Lindsay J.M, 'Deference and Defiance: The Shifting Rhythms of Executive Legislative Relations in Foreign Policy' 33(3) (2003) *Presidential Studies Quarterly* 530.

Lobel J, 'The Commander in Chief and the Courts' 37(1) (2007) *Presidential Studies Quarterly* 49.

Logan C, 'The FISA Wall and Federal Investigations' 4 (2009) *New York University Journal of Law and Liberty* 209.

Lundy J.R, 'Police Undercover Agents: New Threat to First Amendment Freedoms' 37(2) (1969) *The George Washington Law Review* 634.

Lupton R, 'Communications (Retention of Data) Act 2011' 16(4) (2011) *Bar Review* 85.

Maclin M.T, 'Constructing Fourth Amendment principles from the Government Perspective: Whose Amendment Is It Anyway?' 25(4) (1988) *American Criminal Law Review* 669.

Maier B, 'How Has the Law Attempted to Tackle the Borderless Nature of the Internet?' 18(2) (2010) *International Journal of Law and Information Technology* 142.

Manget F.F, 'Intelligence and the Rise of Judicial Intervention' 15(2) (1995) *The Journal of Conflict Studies* 43.

Mantelero A, 'The EU Proposal for a General Data Protection Regulation and the roots of the 'right to be forgotten' 29 (2013) *Computer Law and Security Review* 230.

Markou C, 'The Cyprus and other EU Court rulings on data retention: The Directive as a privacy bomb' 28 (2012) *Computer Law and Security Review* 468.

Maras M.H, 'While the European Union was Sleeping, the Data Retention Directive was passed: The Political Consequences of Mandatory Retention' 6(2) (2011) *Hamburg Review of Social Sciences* 1.

Maras M.H, 'The Social consequences of a mass surveillance measure: What happens when we become the 'others' ?' 40 (2012) *International Journal of Law, Culture and Justice* 65.

Maras MH, 'The economic costs and consequences of mass communications data retention: is the data Retention Directive a proportionate response?' 33(2) (2012) *European Journal of Law and Economics* 447.

Marshall G, 'The Right to Privacy: A Sceptical View' 21(2) (1975) *McGill Law Journal* 242.

Martinico G, 'Is the European Convention going to be "supreme"? A comparative - constitutional overview of ECHR and EU law before national courts' 23 (2012) *European Journal of International* 401.

(----- -----) *Mass surveillance. Who is watching the watchers?* (Council of Europe, 2016).

Mayer J, 'The Secret Sharer,' (2011, 23 May) *The New Yorker.*

McAdams R.H, Privacy in *Knotts*. Beeper Privacy and Collective Fourth Amendment "Tying Rights" 71 (1985) *Virginia Law Review* 297.

McCarthy M.T, 'Recent Developments: US patriot Act' 39 (2002) *Harvard Journal on Legislation* 435.

McGarvey S, 'The 2006 EC Data Retention Directive: A Systemic Failure' 10 (2011) *Hibernian Law Journal* 119.

McGolderick D, 'Developments in the Right to be Forgotten' 13(4) (2013) *Human Rights Law Review* 761.

McIntyre, T.J., 'Data retention in Ireland: Privacy, Policy and proportionality' *Computer Law and Security Report* 24 (2008) 326.

Milanovic M 'Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age' 56(1) (2015) *Harvard International Law Journal* 81.

Mitsilegas V, 'Surveillance and Digital Privacy in the Transatlantic "War On Terror": The Case For a Global Privacy Regime' *Columbia Human Rights Law Review* 47 3(1) (2015-16) 1.

Mondale W.F, Stein R.A, and Fahnhorst M.C, 'National Security and the Constitution: A Conversation Between Wallter F. Mondale and Robert A. Stein 98 (2014) *Minnesota Law Review* 2011.

Mondale, W.F, Stein RA, and Fisher C, 'No Longer a Neutral Magistrate: The Foreign Intelligence Surveillance Court in the Wake of the War on Terror' 106 (6) (2016) *Minnesota Law Review* 2251.

Moreham, N.A, 'The right to respect for private life in the European Convention on Human Rights: a re-examination' 1 (2008) *European Human Rights Law Review* 44.

Mornin J.D, 'NSA Metadata Collection and the Fourth Amendment' 29(4) (2014) *Berkeley Technology Law Journal* 985.

Morrisson C.C, 'Margin of Appreciation in European Human Rights Law' 6 (1973) *Human Rights Law Journal* 263.

Movius L.B, Krup N, 'U.S. and E.U. Privacy Policy: Comparison of Regulatory Approaches' 3 (2009) *International Journal of Communication* 169.

Mowbray A, 'The Creativity of the European Court of Human Rights' 5(1) (2005) *Human Rights Law* 57.

Mowbray A, 'A Study of the Principle of Fair Balance in the Jurisprudence of the European Court of Human Rights' 10(2) (2010) *Human Rights Law Review* 289.

Mowbray A, 'The Interlaken Declaration - The Beginning of a New Era for the European Court of Human Rights?' 10(3) (2010) *Human Rights Law Review* 519.

Murray P.J, 'The Adequacy Standard Under 95/46/EC: Does U.S. Data Protection Meet This Standard? 21(3) (1997) *Fordham International Law Journal* 932.

Murphy C.C, "Note on Romanian Constitutional Court, Decision No. 1258 of 8 October 2009 regarding the unconstitutionality exception of the provisions of Law No. 298/2008 regarding the retention of the data generated or processed by the public electronic communications service providers or public network providers, as well as for the modification of Law No. 506/2004 regarding the personal data processing and protection of private life in the field of electronic communication area" 47 (2010) *Common Market Law Review* 933.

Murphy E, 'The Politics of Privacy, in the Criminal Justice System: Information Disclosure, The Fourth Amendment and Statutory Law Enforcement Exemptions' 111(4) (2013) *Michigan Law Review* 485.

Murphy M.H, 'A shift in the approach of the European Court of Human Rights in surveillance cases: a rejuvenation of necessity?' 5 (2014) *European Human Rights Law Review* 507.

Murphy M.H, 'Data retention in the aftermath of Digital Rights Ireland and Seitlinger' 24(4) (2014) *Irish Criminal Law Journal* 105.

Neocleous M, 'Security, Liberty and the Myth of Balance: Towards a Critique of Security Politics' 6 (2007) *Contemporary Political Theory* 131.

Ní Loideáin N, 'EU Law and Mass Internet Surveillance in the post-Snowden Era' 3(2) (2015) *Media and Communication Data* 53.

Nissenbaum H, 'Privacy as Contextual Integrity' 9(1) (2004) *Washington Law Review* 101.

Novack G.A, 'Electronic Surveillance: The New Standards' 35 (1968) *Brooklyn Law Review* 49

Ojanen T, 'Privacy is more than just a seven-letter word: the Court of Justice of the European Union sets constitutional limits on mass surveillance' 10(3) (2014) *European Constitutional Law Review* 528.

O'Beirne B, 'The European Court of Human Rights' recent expansion of the right to privacy: a positive development?' 14(2) (2009) *Coventry Law Journal* 14.

O'Connor M.P, and Rumann C, 'Going, Going, Gone: Sealing the fate of the Fourth Amendment.' (26) 4 (2003) *Fordham International Law Journal* 1234.

O'Donnell, T.A, 'The Margin of Appreciation Doctrine: Standards in the jurisprudence of the European Court of Human Rights' 4(4) (1982) *Human Rights Quarterly* 474.

Ohm P, 'The Argument Against Technology-Neutral Surveillance Laws' 88 (2010) *Texas Law Review* 1685.

O'Reilly J.T., 'Access to Records Versus Access to Evil: Should Disclosure Laws Consider Motives as a Barrier to Records Release' 12 (2002) *The Kansas Journal of Law and Public Policy* 559.

Owens J.E, *Presidential Power and Congressional Acquiescence in the "War" on Terrorism*: A New Constitutional Equilibrium' 34(2) (2006) *Politics and Policy* 258.

Paine C et al, 'Internet users' perceptions of "privacy concerns" and "privacy actions.' 65 (2007) *International Journal of Human-Computer Studies* 526.

Papakonstantinou V, and de Hert P, 'The Amended EU Law On ePrivacy and Electronic Communications after its 2011 implementation: New rules on Data Protection, Spam, Data Breaches and Protection of Intellectual Property Rights' 29(1) (2011) *Journal of Computer and Information Law* 29.

Paris M.L, 'Paving The Way: Adjustments of Systems And Mutual Influences Between The European Court Of Human Rights And European Union Law Before Accession' 51(1) (2014) *The Irish Jurist* 59.

Pell S.K, and Soghoian C, 'A Lot More than A Pen Register and Less than a Wiretap: What the StingRay Teaches Us About How Congress Should Approach the reform of Law Enforcement Surveillance Authorities' 16 (2013) *Yale Journal of Law and Technology* 134.

Peltz-Steele R.J., 'The Pond Betwixt: Differences In The US-EU Data Protection/Safe Harbour Negotiation' *Journal of Internet Law* 19(1) (2015) 14.

Peppet S.R, 'Unravelling Privacy: The Personal Prospectus And The Threat of A Full-Disclosure Future.' 105(3) (2011) *Northwest University Law Review* 1153.

Pfiffner JP, 'The Contemporary Presidency. Constraining Executive Power: George W. Bush and the Constitution ' 38(1) (2008) *Presidential Studies Quarterly* 123.

Phillips M, 'A New Legal Theory For The Age of Mass Surveillance.' (2013, 17 December) *The New Yorker*

Poorbaugh K, 'Security Protocol: A Procedural Analysis Of The Foreign intelligence Surveillance Courts' 3 (2013) *University of Illinois Law Review* 1363.

Rascoff S.J, 'Presidential Intelligence' 129(3) (2016) *Harvard Law Review* 633.

Rauhofer J 'Just because you're paranoid, doesn't mean they're not after you: Legislative developments in relation to the mandatory retention of communications data in the European Union' 3(4) (2006) *SCRIPT-ed* 322.

Rauhofer J, and Mac Síthigh D, 'The data Retention Directive Never Existed' 11(1) (2014) *scripted* 119.

(----------) 'Reforming the Foreign Intelligence Surveillance Court to Curb Executive Branch Abuse of Surveillance Techniques' (2015) 37 *Campbell Law Review* 519.

Reidenberg J.R, 'The Data Surveillance State in the United States and Europe' 49 (2014) *Wake Forest Law Review* 583.

Richards N.M, 'The Dangers of Surveillance' 126 (2013) *Harvard Law Review* 1934.

Rivkin Jr, D.B, 'Answering The Critics Of The Legal Case For The War On Terror' 32(2) (2009) *Harvard Journal of Law and Public Policy* 485.

Robinson G.H, 'We're Listening! Electronic Eavesdropping, FISA and the Secret Court' 36 (2000) *Williamette Law Review* 51.

Rosen J, 'The Naked Crowd: Balancing Privacy In An Age of Terror' Isaac Marks Memorial Lecture. 46(4) (2004) *Arizona Law Review* 607.

Rubenfeld J, 'The End of Privacy' 61 (2008) *Stanford Law Review* 101.

Ryssdall R, 'The Coming of Age of the European Convention of Human Rights' 1 (1996) *European Human Rights Law Review* 18.

Saltzburg A, 'Another Victim of Illegal Narcotics: The Fourth Amendment (As Illustrated by the Open Fields Doctrine)' 48 (1986) *University of Pittsburgh Law Review* 1.

Sanchez P, 'A (My) Space of One's Own: On Privacy and Online Social Networks' 1 (2007) *Northwestern Journal of Technology and Intellectual Property* 73.

Şandru S, 'About Data Protection And Data Retention In Romania' 7(2) (2013) *Masaryk University Journal of Law and Technology* 379.

Schauer F, 'A Comment on the Structure of Rights,' 27 (1993) *Georgia Law Review* 415.

Schlanger M, 'Intelligence Legalism and the National Security Agency's Civil Liberties Gap' 6(1) (2015) *Harvard National Security Journal* 112.

Schoenfeld G, *Necessary Secrets* (2010), cited in Mayer, J, 'The Secret Sharer: Is Thomas Drake an Enemy of the State?,' *New Yorker*, May 23, 2011.

Schwartz M, 'The Whole Haystack. The NSA claims it needs access to all our phone records. But is that the best way to catch a terrorist?' *New Yorker* 26 January, 2015.

Schwartz P, 'Data Processing and Government Administration: The Failure of the American Legal Response to the Computer' 43 (1992) *Hastings Law Journal* 1321.

Schwartz P, 'German and U.S. Telecommunications Privacy Law: Legal Regulations of Domestic Law Enforcement Surveillance' 54 (2002) *Hastings Law Journal* 751.

Schwartz P.M, and Peifer K.N, 'Posner's Privacy and the German Right of Personality: Are Four Privacy Torts better than one Unitary Concept?' 98 (2010) *California Law Review* 1915.

Schwartz P.M, 'Systematic government access to private-sector data in Germany' *International Data Privacy Law* (2)4 (2012) 289.

Sellars S, 'Online privacy: do we have it and do we want it?' A review of the risks and UK case law' 33(1) (2011) *European Intellectual Property Review* 9.

Seymore D, 'The Extension of the European Convention on Human Rights to Central and Eastern Europe: Prospects and Risks' 8 (1993) *Connecticut Journal of International Law* 243.

Shany Y, 'Towards s General Margin of Appreciation Doctrine in International Law?' 16(5) (2006) *European Journal of International Law* 907.

Sievert, R.J 'Time To Rewrite The Ill-Conceived And Dangerous Foreign Intelligence Surveillance Act of 1978' 31 (2014) *National Security Law Journal* 47, 82.

Sievert R, 'The Foreign Intelligence Surveillance Act of 1978 Compared with the Law of Electronic Surveillance in Europe' 43(2) (2016) *American Journal of Criminal Law* 125.

Simbro E.M., 'Disclosing Stored Communication Data to Fight Crime: The U.S. and E.U. Approaches to Balancing Competing Privacy and Security Interests' 43(3) (2010) *Cornell University Law Journal* 585.

Simitis S, 'Reviewing Privacy in an Information Society' 135(9) (1987) *University of Pennsylvania Law 7*07.

Sinha A.G, 'NSA Surveillance Since 9/11 and the Human Right to Privacy' 59 (2013) *Loyola Law Review* 861.

Sklansky D.A, 'Two More Ways Not to Think about Privacy and the Fourth Amendment' 82 (2015) *The University of Chicago Law Review* 223.

Sloan L.D, 'Echelon And The Legal Restraints On Signals Intelligence: A Need For Reevaluation' 50 (2001) *Duke Law Journal* 1467.

Slobogin C, 'Government Data Mining and the Fourth Amendment' 75(1) (2008) *Chicago Law Review* 317.

Smismans S, 'The European Union's Fundamental Rights Myth' 48(1) (2010) *Journal of Common Market Studies* 45.

Smith R, 'The Margin of Appreciation and Human Rights Protection in "The War on Terror": Have the Rules Changed before the European Court of Human Rights?' 8(1) (2011) *Essex Human Rights Review* 124.

Solis, G.D., 'Cyber Warfare' 219 (2014) *Military Law Review* 1.

Solove D.J, 'Digital Dossiers and the Dissipation of Fourth Amendment Privacy' 75(5) (2002) *Southern California Law Review* 1083.

Solove D.J, 'The Virtues of Knowing Less. Judging Privacy Protections Against Discourse' 53 (2003) *Duke Law Journal* 967

Solove D.J, 'I've Got Nothing to Hide and other Misunderstandings of Privacy' 44 (2007) *San Diego Law Review* 745.

Solove D.J, 'Data Mining and the Security-Liberty Debate' 75 (2008) *University of Chicago Law Review* 343.

Sottiaux S, and Van Der Schyff G, 'Methods of International Adjudication: Towards a More Structured Decision-Making Process for the European Court of Human Rights' 31(1) (2008) *Hastings International and Comparative Law Review* 115.

Steiker C.S, 'Brandeis in *Olmstead*: Our Government Is the Potent, the Omnipresent Teacher' 79 (2009) *Mississippi Law Journal* 149.

Steinhardt B, 'Does Privacy have a Future After 9/11? 11(1) (2003)*Journal of Contingencies and Crisis Management* 32.

Stute, D.J., 'Privacy Almighty? The CJEU's Judgment on *Google Spain Sl v. AEPD*' 36(4) (2015) *Michigan Journal of International Law* 649.

Sulmasy G, and Yoo J, 'Katz and the War on Terrorism' 41 (2007-08) *University of California, Davis* 1219.

Severson D, 'American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offers Only Cosmetic Change' 56(2) (2015) *Harvard International Law Journal* 465.

Swire P.P, 'The System of Foreign Intelligence Surveillance' 72 (2004) *George Washington Law Review* 1306.

Squitieri C, 'The Limits Of The Freedom Act's Amicus Curiae' 11(3) (2015) *Washington Journal Of Law, Technology and Arts* 197.

Swire P, and Kennedy-Mayo De Brae, 'How Both the EU and the U.S. are 'Stricter' than Each Other For the Privacy of Government Requests for Information' 66 (2017) *Emory Law Journal* 617.

(----------) 'The Foreign Intelligence Surveillance Act: Legislating a Judicial Role in National Security Surveillance' (1980) 78 *Michigan Law Review* 116.

Tréguer, F 'Intelligence Reform and the Snowden Paradox: The Case of France' *Media and Communication* 5(1) (2017) 17.

Tridimas T, 'Terrorism and the ECJ: empowerment and democracy in the EC legal order' 34(1) (2009) *European Law Review* 103.

Tsesis A 'The Rights To Erasure: Privacy, Data Brokers And The Indefinite Retention of Data' 49 (2014) *Wake Forrest Law Review* 442.

Tzanou M, 'The EU as an emerging 'Surveillance Society': The function creep case study and challenges to privacy and data protection' 4 (2010) *The Vienna Online Journal On International Constitutional Law* 407.

Tzanou M, 'Is Data Protection The Same As privacy? An Analysis Of Telecommunications' Metadata Retention Measures' 17(3) (2013) *Journal of Internet Law* 20.

Thierer A, 'In Pursuit of Privacy in a World Where Information Control is Failing' 36(2) (2013) *Harvard Journal of Law and Public Policy* 410.

Tien L. 'Privacy, Technology and Data Mining' 30 (2004) *Ohio Northern University Law Review* 389.

Tridimas T, 'Terrorism and the ECJ: empowerment and democracy in the EC legal order' 34(1) (2009) *European Law Review* 103.

Tracol X, 'Legislative genesis and judicial death of a directive: The European Court of Justice invalidated the data retention directive (2006/24/EC) thereby creating a sustained period of legal uncertainty about the validity of national laws which enacted it' 30 (2014) *Computer Law and Security Review* 736.

Tümay M, 'The "Margin of Appreciation Doctrine" Developed By The Case Law Of The European Court Of Human Rights' 5(2) (2008) *Ankara Law Review* 201.

Tzanou M, 'Is Data Protection the Same as Privacy? 17(3) (2013) *Journal of Internet Law* 20.

Van Alstyne W.W, 'A Critical Guide to Marbury v Madison' 1 (1969) *Duke Law Journal* 1.

Vainio N, and Miettinen S, 'Telecommunications data retention after *Digital Rights* Ireland: legislative and judicial reactions in the Member States' 23(3) (2015) *International Journal of Law and Information Technology* 290.

Vița V, 'The Romanian Constitutional Court and the Principle of Primacy: 1 To Refer or Not to Refer?' 16(6) (2015) *German Law Journal* 1623.

Vladeck S.J, 'The FISA Court and Article III' 72(3) (2015) *Washington and Lee Law Review* 1161, 1164.

Waldock H, 'The Effectiveness of the system set up by the European Convention on Human Rights' 1 (1980) *International Human Rights Law Journal* 1.

Waldron J, 'Security and liberty: The Image of balance' 11(2) (2003) *Journal of Political Philosophy* 191.

Walker K, 'The Costs of Privacy' 25(1) (2001) *Harvard Law and Public Policy* 87.

Warbrick C, 'The principles of the European Convention on Human Rights and the response of states to terrorism' 3 (2002) *European Human Rights Law Review* 287.

Warren S, and Brandeis L, 'The Right to Privacy' 4 (1890) *Harvard Law Review*193.

Warren A, and Dirsken A, 'Augmenting State Secrets: Obama's Information War' 9(1) (2014) *Yale Journal of International Affairs* 68.

Warren S.D, and Brandeis LD, 'The Right To Privacy' IV (5) (1890) *Harvard Law Review* 193.

Wasserstorm S.J, and Seidman L.M, 'The Fourth Amendment as Constitutional Theory' 77 (1988-89) *Georgetown Law Journal* 19.

Weiler J.H.H, 'The Transformation of Europe' 100 (1991) *The Yale Law Journal* 2403.

West, S.R, 'The Story of Us: Resolving the Face-Off Between Autobiographical Speech and Information Privacy' 67 (2010) *Washington and Lee Law Review* 589.

Whitman J.Q., 'The Two Western Cultures of Privacy: Dignity versus Liberty' 113 (2004) *The Yale Law Journal* 1153.

Whites B, 'The FISA Court Speaks' *Legal Times* (19 February 1996) 1.

Woodburn N, 'NSA Surveillance And Interference With Citizens' Property Rights' 7 (2016) *Faulkner Law Review* 287.

Yourow H.C, 'The Margin of Appreciation Doctrine in the Dynamics of European Human Rights Jurisprudence' 3 (1987) *Connecticut Journal of International Law*111.

Yoo J, 'The Terrorist Surveillance Program and The Constitution' 14(3) (2007) *George Mason Law Review* 565.

Zuiderveen B.F, and Arnbak A, 'New Data Security Requirements and the Proceduralization of Mass Surveillance Law After the European Data Retention Case' (2015) *Amsterdam Law School Legal Studies Research.*

Newspaper Articles

Ahmed M, and Robinson D, 'EU data protection rules shake-up set to rile US tech groups' *Financial Times* (March 12, 2015).

(------- --------) 'Angela Merkel rebukes US and Britain over NSA surveillance' *The Telegraph* 29 January, 2014.

Ball J, 'NSA stores metadata of millions of web users for up to a year, secret files show' *The Guardian* 30 September 2013.

Ball J, Border J, and Greenwald G, 'Revealed: how US and UK spy agencies defeat internet privacy and security.' *The Guardian* 6 September, 2013.

Black I, 'NSA Spying Scandal: What We Have Learned,' *The Guardian* June 10 2013.

Boycott O, 'UK-US surveillance régime was unlawful for seven years' *The Guardian* 6 February 2015.

Colmes J, 'Obama says surveillance helped Case in Germany' *The New York Times* 19 June, 2013.

(------- ---------) 'Data retention: Netherlands court strikes down law as breach of privacy.' *The Guardian* (12 March 2015).

DeBonis M, 'Congress turns away from post-9/11 law, retooling U.S. surveillance powers' *The Washington Post* (2 June, 2015).

Dworkin R, 'It is absurd to calculate human rights according to a cost-benefit analysis' (*The Guardian* 24 May 2006).

Entous A, and Gorman S, 'Europeans Shared Spy Data With U.S.' *The Wall Street Journal* 29 October, 2013.

Fontella-Khan J, and Spiegel P, 'Washington Pushed EU to dilute data protection' *Financial Times* June 12, 2013.

Gellman B, and Poitras L, 'U.S., British intelligence mining data from nine U.S. internet companies in broad secret programme' *Washington Post* June 6, 2013.

Gellman B, and Mille G, 'Black budget summary details U.S. spy network's successes, failures and objectives' *The Washington Post* 29 August, 2013.

Gibbs S, 'Data Regulators Reject EU-US Privacy Shield safe harbour deal,' *The Guardian* 14 April 2016.

Goldenberg S, 'US law chief defends domestic wiretapping' (*The Guardian* 7 February, 2006).

Gorman S, 'NSA's Domestic Spying Grows as Agency Sweeps Up Data,' (Wall Street Journal, March 10, 2008).

Greenwald G, 'NSA collecting phone records of millions of Verizon customers daily' *The Guardian* 6 June 2013.

Greenwald G, and MacAskill E, 'Boundless Informant: the NSA's secret tool to track global surveillance data' *The Guardian* June 8 2013.

Greenwald G, and Ackerman S, 'How the NSA is still harvesting your online data' *The Guardian* June 27, 2013.

Greenwald G, and Ackerman S, 'NSA Collected US email records in bulk for more than two years under Obama,' *The Guardian* June 27, 2013.

Greenwald G, 'NSA tool collects 'nearly everything a user does on the internet' *The Guardian* 30 July 2013.

Greenwald G, 'XKeyscore: NSA tool collects nearly everything a user does on the internet.' *The Guardian* 31 July 2013.

Gruson L, 'Explosion Displaces Hundreds of Businesses' (*New York Times*. 28 February 1993).

Harding L, 'Footage released of Guardian editors destroying Snowden hard drives' *The Guardian* 31 January 2014.

Harris P, 'U.S. data whistleblower: 'It's a violation of everybody's rights,' *The Guardian* 15 September, 2012.

Henderson B, (ed), 'Angela Merkel rebukes US and Britain over NSA surveillance' *The Telegraph* 29 January, 2014.

Hersh S.M., 'Underground for the C.I.A. in New York: An Ex-Agent Tells of Spying on Students' (*New York Times* December 29, 1974)

Johnson B, 'Privacy no longer a social norm, says Facebook founder.' *The Guardian* (11 January, 2010).

Kristoff N, 'Liberal Reality Check' *The New York Times* 31 May 2002.

Leonnig C.D, 'Court: Ability to Police U.S. Spying programme Limited' *Washington Post* (15 August, 2013).

Lichtblau E, 'Bush Defends Spy Program and Denies Misleading Public' (*New York Times*, January 2, 2006).

Lichtbaum E, 'Senate Panel Rebuffed on Documents on U.S. Spying' (The *New York Times*, February 2, 2006.

Lynch S, 'Pan-European data protection agreed despite Irish concerns' *The Irish Times* (Saturday, March 14, 2015).

Meyer J, 'The Secret Sharer,' *The New Yorker* 23 May, 2011.

MacAskill E, 'Obama defends "system of checks and balances" around NSA surveillance' *The Guardian* 17 June 2013.

MacAskill E, et al, 'GCHQ taps fibre-optic cables for secret access to world's communications' *The Guardian* 21 June, 2013.

MacAskill E, et al, 'We are starting to mater the internet. And our Capability is impressive' *The Guardian* 22 June, 2013.

MacAskill E, Borger J, Davies N, Hopkins N, and Ball J, 'How GCHQ watches your every move' *The Guardian* 22 June 2013.

MacAskill E, 'NSA paid millions to cover PRISM compliance costs for tech companies.' *The Guardian* August 23, 2013.

MacAskill E, "Extreme surveillance" becomes UK law with barely a whimper' *The Guardian* 19 November 2016.

McCarthy T, 'Obama defends secret NSA surveillance programs,' *The Guardian* (7 June 2013).

(----------) 'NSA slides explain the PRISM data-collection program' *The Washington Post* 6 June 2013).

Muir H, and Cowan R, 'Four bombs in 50 minutes - Britain suffers its worst ever terror attack,' (*The Guardian* 8 July 2005).

Peterson A, 'Patriot Act Author: 'There has been a failure of oversight' *The Washington Post* October 11, 2013.

Nakashima E, and Gellman B, 'Court Gave NSA broad leeway in surveillance, documents show' *The Washington Post* June 30 June 2014.

Nakashima E, 'NSA gathered thousands of Americans' emails before Court ordered it to revise its tactics.' *The Washington Post* August 21, 2013.

Perlroth N, Larson, J, and Scott S, 'NSA Able to Foil Basic Safeguards of Privacy on Web' *The New York Times* 5 September 2013.

Poitras L, 'The Program,' *New York Times* August 22, 2012.

Priest D, 'Help from France In Covert Operations' *The Washington Post* 3 July, 2005.

(---------- ---------) 'President Obama's Dragnet' *New York Times* 6 June 2013.

Risen J, and Lichtblau E, 'Bush Lets U.S. Spy on Callers Without Courts.' *New York Times* (14 December, 2005).

Risen J, and Lichtblau E, 'Bush Lets U.S. Spy on Callers Without Courts *The New York Times* 16 December 2005.

Risen J, and Poitras L, 'NSA Examines Social Networks of US Citizens' (*New York Times* September 29, 2013).

Roberts D, and Ackerman S, 'Obama defiant over NSA revelations ahead of summit with Chinese Premier,' *The Guardian* June 7, 2013.

Safire W, 'You are a suspect,' *New York Times* 14 November, 2002).

Sanger D.E, 'Bush Says He Ordered Domestic Spying.' (*The New York Times*, December 18, 2005).

Savage C, 'Obama says NSA Curbs would Address Worries' *The New York Times* 25 March 2014.

Scally D, 'NSA Whistleblowers' testimony electrifies Bundestag committee' *Irish Times* 5 July, 2014

Schwartz M, 'The Whole Haystack. The NSA claims it needs access to all our phone records. But is that the best way to catch a terrorist?' *New Yorker* 26 January, 2015.

(----------) 'Secret Documents Reveal NSA Campaign Against Encryption' *New York Times* 5 September, 2013.'

Shapiro W, Usual Adversaries Unite Over Threat to Liberties, *USA Today* 26 (September 2001).

Singer N, 'Data Protection Laws, an Ocean Apart' *The New York Times (*February 2, 2013).

Smale A, 'Anger Growing Among Allies on U.S. Spying,' *The New York Times* October 23, 2013.

Steinhauer J, and Weisman J, 'U.S. Surveillance in Place Since 9/11 Is Sharply Limited' *The New York Times* 2 June, 2015.

Stolberg S, 'On First Day, Obama Quickly Sets a New Tone,' *The New York Times* January 21, 2009.

Stothard P, and Dejevsky M, 'Malta summit declares: Cold War is over' *The Times* December 4, 1989.

Taylor M, and Hopkins N, 'World's leading authors: state surveillance of personal data is theft.' *The Guardian* (10 December 2013).

Tempest M, 'Clarke tells MEPs to back EU anti-terror measures' *The Guardian*, 7 September 2005.

(----------) Transcript. 'President Bush's Address.' (*The New York Times*, December 17, 2005).

Traynor I, 'New EU rules to curb transfer of data to US after Edward Snowden revelations' *The Guardian* (17 October 2013).

Travis A, Home Affairs, *The Guardian* 17 October 2016.

Valentino-DeVries J, and Gorman S, 'Secret Court's Redefinition of 'Relevant' Empowered Vast NSA Data-Gathering' *The Wall Street Journal* 8 July 2013.

(----------) 'Verizon forced to hand over telephone data - fall Court Ruling' *The Guardian* June 5, 2013.

Wagenseil P, 'NSA Mass Surveillance Useless, Former Bush Official Says,' *Tom's Guide* (24 February 26, 2014).

Waterfield B, Hope C, and Foster P, 'EU leaders warn US spying could harm fight against terror' *Daily Telegraph* 25 October 2013.

Cases

European Court of Justice

Cases C-539/10 P and C-550/10 P *Al-Aqsa v Council* Judgment of 12 January 2013.

Joined Cases C-584/10 P, C-593/10 P and C-595/10 P *Commission, Council, United Kingdom v Yassin Abdullah Kadi* Judgment of 18 July 2013.

Case C-614/10 *Commission v Austria* Judgment of 16 October 2010.

Case C-518/07 *Commission v Germany* Case C-518/07 Judgment of 9 March, 2010.

Case C-270/11 *Commission v Sweden* Judgment of 30 May 2013.

Joined Cases C-293/12 and 594/12 *Digital Rights Ireland and Seitlinger and Others* Judgment of 8 April 2014.

Case C-473/12 *Institut professionnel des agents immobiliers (IPI) v Geoffrey Englebert and Others* Judgment of 7 November 2013.

Cases C-402/05 and C-415/05 *Kafi and Al Barakaat International Foundation v Council and Commission* Judgment 3 September 2008.

Case C-127/08 *Metock and Ors v Minister for Justice, Equality and Law Reform* Judgment of 25 July 2008.

Case C-305/05 *Ordre des barreaux francophones and germanophone & Others v Conseildes Ministres* (ECJ, Grand Chamber) Judgment of 26 June 2007.

Joined Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others* Judgment of 20 May 2003.

Case C-275/06 Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU Unreported January 29, 2008.
Case C-203/15 *Tele 2 Severige and Watson* (Grand Chamber) 21 December, 2016.
Case C-145/09 *Tsakouridis* EU:C:2010 Judgment 23 November 2010.
Volker and Markus Schecke GbR v. Land Hessen C-92/09 and C-93/09 *Eifert v. Land Hessen and Bundesanstalt für Landwirtschaft und Ernährung*, Judgment 9 November 2010.
Joined Cases C-402/05 P and C-415/05 *Yassin Abdullah Kadi and Al Barakaat International Foundation v Council of the European Union and Commission of the European Communities* Grand Chamber Judgment 3 September 2008.

European Court of Human Rights

A and Others v United Kingdom No. 3455/05, Grand Chamber 2009.
Ahmed v Austria (Application No 25964 (1986).
Aksoy v Turkey Application No. 21987/93 18 December 1996 (1997) 23 E.H.R.R. 553.
Amann v Switzerland (2000) 30 E.H.R.R. 843.
Barford v Denmark, 149, ECtHR (Series A) (1989).
Brannigan and McBride v United Kingdom, Series A, No. 258-B Application Nos. 14553-14554/89 26 May 1993 (1994) 17 E.H.R.R. 539.
G. and J.H. v The United Kingdom, 44787/98 Judgment 25 September 2001.
C.G v Bulgaria 2008) 47 E.H.R.R. 51.
Copland v the United Kingdom 45 E.H.R.R. 37.
Cubature v Moldova, No. 27138/04, (2010).
Esbester v the United Kingdom (1994), 18. E.H.R.R. CD72.
El Haski v Belgium 2013) 56 E.H.R.R 31.
Florida Star v B.J.F (1989) 491 U.S. 530.
Gaskin v United Kingdom 12 ECtHR 26 (1989).
Goodwin v The United Kingdom [Grand Chamber], Application Number 28957/95, 2002.
Greece v United Kingdom (Application No 176/56 (1958-9), 174.
Handyside v U.K. 1979-80 E.H.R.R. 737.
Hatton v United Kingdom (2003) 37 E.H.R.R. 28.
Huvig v France, 24 April 1990, § 26, Series A no. 176-B.

Iordachi and Others v Moldova Application no. 25198/02 Fourth Section 10 February 2009.

Khan v United Kingdom (2001) 31 E.H.R.R. 45.

Klass and Others v Federal Republic of Germany (1979-80) 2 E.H.R.R. 214.

Kroon v Netherlands (1995) 19 E.H.R.R. 263.

Kruslin v France (1990) 12 E.H.R.R. 547.

Laizdou v Turkey, Judgment 23 March 1995, 71. E.C.t.H.R.

Lawless v Ireland (Appeal No 5319/57 (1960-61).

Leander v Sweden (1987) 9 E.H.R.R. 433.

Lewis v United Kingdom (2004) 39 E.H.R.R. 9.

Lewiston v United Kingdom (2003), 37 E.H.R.R. 31.

Liberty v United Kingdom (2009) 48 E.H.R.R. 1.

Liu v Russia, no. 42086/05, 6 December 2007.

Loizidou v Turkey, 310, ECtHR, Series A, (1995).

Lüdi v Switzerland, Application no. 12433/86 (1992).

M. v Netherlands (2004) 39 E.H.R.R., 414.

Malone v United Kingdom (1985) 7 E.H.R.R. 14.

Marker v The United Kingdom [Grand Chamber] nos. 30562/04 and 30566/04 (2008).

McGinley and Egan v United Kingdom (1998) 27 E.H.R.R. 1.

M.K. v France no. 19522/09, Judgment 18 April 2013.

Mubilanzila Maycka and Kaniki Mitunga v Belgium (Application no. 13178/03) Judgment 12 October 2006.

Nada v Switzerland (Application no. 10593/08) Judgment 12 September 2012.

Powell v United Kingdom (1990) 12 E.H.R.R. 355.

Rotaru v Romania, Grand Chamber, No. 28341/95 ECtHR.

Rotaru v Romania [2000] ECHR 192.

Sanoma Uitgevers B.V. v *The Netherlands* 31 March 2009, Application No. 38224/03.

*Saravia v Germany (*1987) 9 EHRR 433.

Sakharov v Russia Application No. 47143/06, 4 December 2015.

Szabó and Vissy v Hungary Application No. 37138/14. 12 January 2016. (2016) 63 E.H.R.R. 3.

S and Marper v the United Kingdom 48 EHRR 50. 1169.

Segerstedt-Wiberg v Sweden (2007) 44 E.H.R.R. 2.

Soering V United Kingdom (1989), Series A, No. 161.

Sunday Times v United Kingdom (1979) 2 EHRR 245.

The Republic of Ireland v The United Kingdom Series A, No. 25 18 January 1978 (1979-80) 2 E.H.R.R. 25.

Tyrer v The United Kingdom, Judgment 25 April 1978, 31, E.C.t.H.R.

Uzun v Germany (2011) 53 E.H.R.R. 24.

Van Kück v Germany (2003) 37, E.H.R.R. 51.

Von Hannover v Germany Application No. 59320/00 (2005), 40 E.H.R.R.

Van Vondel v Netherlands (2007) EHRR 12. 237.

Wises v France (1994) 17 EHRR 462.

Z v Finland (Application No. 22009/93) (1998) 25 E.H.R.R. 371.

Zolotukhin v Russia Application No.14939/0310 February 2009 (2012) 54 E.H.R.R. 16.

United States

ACLU v Clapper No. 13 Civ. 3994 (WHP) (S.D.N.Y. Dec. 27, 2013).

Bartnicki v Vopper 523 U.S., 514, 523-5 (2001).

Berger v New York 388 U.S. 41 (1967).

Bonome v Kaysen No 032767, 2004 WL 1194731.

Broadcasting Corp. v Cohn 420 U.S. 469, 491 (1975).

Brown v Allen 344 U.S. 443, 540 (1953).

California v Greenwood 486 U.S. 35 (1988).

Cox Broadcasting Corporation v Cohn 420 U.S. 469 at 496. 1975.

Eisenstaedt v Baird 405 U.S. 438 (1972).

Ex Parte Jackson 96 U.S. 727 (1877).

Florida Star v BJR 491 U.S. 524 (1989).

Goldman v United States 316 U.S. 129 (1942).

Griswold v Connecticut 331, U.S., 479 (1965).

Hamdan v Rumsfeld, 548 U.S. 557 (2006).

Hamdi v Rumsfeld, 542 U.S. 507, 582-583 (2004).

Hoffa v United States 385 U.S., 293, 302 (1966).

Hustler Magazine Inc. v Falwell 485 U.S. 46 (1988).

In re: Application of the United States of America for historical cell site data. Court of Appeals for the fifth circuit. Case: 11-20884. July 30, 2013.

In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted] No. BR 13-158 (FISA Ct. Oct. 11, 2013.

Katz v United States 389 U.S. 347 (1967).

Klayman v Obama 2013 WL 6571596 (D.D.C. 2013).

Kyllo v U.S. 593 U.S. 27, 31 (2001).

Lawrence v Texas 539 U.S. 558 (2003).

Lee v Florida 392 U.S. 378 (1968).

Lopez v United States 373 U.S. 427 (1963).

New York Times Co. v Sullivan 376 U.S. 264, 270 (1964).

Olmstead v United States 277 U.S. 438 (1928).

On Lee v United States 343 U.S. 747 (1952).

Raskas v Illinois 439, U.S. 128 (1978).

Rawlings v Kentucky 448. U.S. 98, (1980).

Roe v Wade 410 U.S. 113, 93 S. Ct. 705, 35 L. Ed. 2d 147 (1973).

Schwartz v Texas, 344 U.S. 199, (1952).

Shulman v Group Productions Inc 955 p.2d 469 478. (Cal 1998).

Silverman v United States 365 U.S. 505 (1961).

Smith v Maryland 442 U.S. 735 (1979).

Smith v Daily Mail Publishing Co.443 U.S. 97 (1979).

Snyder v Phelps 131 S. Ct 1207 (2011).

Steinbuch v Cutler No. 1-05-cv-00970 (D.D.C. May 16, 2005).

United States v Gines-Perez, 214 F. Supp. 2d 205 (D.P.R. 2002).

United States v Hambrick, 55F. Supp. 2d, 504, 508-09 (WD. Va. 1999).

United States v Jacobsen 466 U.S. 109, 113 (1984).

United States v Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan 2000).

United States v Miller, 425 U.S. 435, 443 (1976).

United States v Robinson 414 U.S. 218 (1973).

United States v Ross 458 U.S., 798, 825 (1982).

United States v Salvucci 448 U.S., 83 (1980).

United States v United States District Court, 407 U.S. 297, 308 (1972).

United States v Verdugo Urquidez 494 U.S. 259, 271 (1990).

United States v Warshak 6th Cir. Dec. 14, 2000.

United States v Warshak 631F. 3rd, 266/6th Cir. (2010).

United States v White 405 f 2d. 838 7th Cir. (1969).

Yahoo!, Inc v La Ligue Contre Le Racisme et L'Antisemitism.' (2010) 130 S. Ct 2705, 2730.
Youngstown Sheet & Tube Co v Sawyer, 343 US 579, 637 (1952).

Ireland

Digital Rights Ireland Limited v Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of An Garda Síochána, Ireland and the Attorney General and the Human Rights Commission (notice party) [2011] 1 I.L.R.M. 258.
Gray v Minister for Justice [2007] IEHC 52.
Maximilian Schrems v Data Protection Commissioner [2014] IEHC 310.
McD v L (2010) 2 I.R. 199.
Sunny Idah v DPP [2014] IECCA 3.
White v Morris [2007] IEHC 107.

United Kingdom

Secretary of State for the Home Department v R (Davis) [2015] EWCA Civ 1185, [2015] All ER (D) 196 (Nov).

United States Statutes

CIA Inspector General Act 1989
Communications Assistance for Law Enforcement Act 1994
Electronic Communications Privacy Act 1986
Foreign Intelligence Surveillance Act 1978
Intelligence Identities Act 1982
Intelligence Oversight Act 1980
Intelligence Authorisation Act for the Fiscal Year 1999
Intercept and Obstruct Terrorism Act 2001
Judicial Redress Act 2016.
Omnibus Crime Control And Safe Streets Act 1968
Patriot Act 2001
Protect America Act 2007
Stored Communications Act 1986
The Foreign Intelligence Surveillance Act 1978 Amendments Act 2008

Use of Military Force Act AMFU) 2001

Agreements

Agreement on Mutual Legal Assistance between the European Union and the United States of America, OJ L 181/34, 19 July 2003.

Article 29 Working Party Opinions

Opinion 9/2004 on a draft Framework Decision on the storage of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism. Proposal presented by France, Ireland, Sweden and Great Britain (Document of the Council 8958/04 of 28 April 2004)], Article 29 Data Protection Working Party, 11885/04/EN WP 99, Adopted on 9th November 2004 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion recommendation/files/2004/wp99_en.pdf> accessed 23 September 2016.

'Thirteenth Annual Report of the Article 29 Working Party on Data Protection.' European Justice Commission, 109. 14 July 2010 <ec.europa.eu/.../article-29/.../annual-report/.../13th_annual_report_en…> accessed 26 November 2014.

Article 29 Data Protection Working Party, 'Opinion 3/2006 on the Directive 2006/24/EC of the European Parliament and of the Council on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC,' 654/06/EN WP 119, 1.

These issues were raised by the Article 29 Working Party: Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, Brussels, Secretariat of the European Commission 919/14/EN <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf> accessed 23 August 2015.

Opinion SJ-0890/14 LIBE - Questions relating to the judgment of the Court of Justice of 8 April 2014 in Joined Cases C-293/12 and C-594/12, *Digital Rights Ireland* and *Seitlinger and others* - Directive 2006/24/EC on data retention - Consequences of the judgment. at 19, para 84 <http://www.statewatch.org/news/2015/apr/ep-ls-opinion-digital-rights-judgment.pdf> accessed 21 September 2016.

Article 29 Working Party. Opinion 01/2016 on the EU-US Privacy Shield draft adequacy decision. 16/EN WP 238. Adopted 13 April 2016, at 2 <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf> accessed 29 October 2016.

Council of the European Union Press Releases

Council of the European Union, (13 July 2005) Justice and Home Affairs Press Release 11116/05, (Presse 187), 1 <https://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/85703.pdf> accessed 23 October 2016.

Council of Europe Treaties

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg Council of Europe 28.I.1981European Treaty Series 108 <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680078b37> accessed 13 August 2016.

'Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows' Strasbourg, 8.XI.2001 European Treaty Series -Series 181 Council of Europe, European Treaty Series. No. 181, Strasbourg, 8.XI,2001 <https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680080626> accessed 26 July 2016.

European Commission Press Releases

'European Commission acts to bolster the EU's system of protecting fundamental rights' European Commission Press Release IP /10/291 of March 2010 <http://europa.eu/rapid/press-release_IP-10-291_en.htm?locale=en> accessed 28 October 2016.

European Commission Reports

European Commission, (2011) Report from the Commission to the Council and the European Parliament. Evaluation Report on the Data Retention Directive (Directive 2006/24/EC) COM 225 final.

European Commission Opinions

'Consultation on reform of Data Retention Directive: emerging themes and next steps,' <http://quintessenz.org/doqs/000100011699/2011_12_15,Eu_Commission_data_retention_reform.pdf> accessed 20 May 2013. (Leaked Report).

European Communities Joint Declarations

Joint Declaration by the European Parliament, Council and the Commission concerning the protection of fundamental rights and the ECHR (Luxembourg, 5 April 1977) Official Journal of the European Communities (OJEC). 27.04.1977, No C 103

European Convention on Human Rights Advisory Reports

Advisory Report on the Application of Protocol No. 14 to the European Convention on Human Rights and Fundamental Freedoms,' cited in *Netherlands International Law Review* 2009 56(1) 71-92

European Convention on Human Rights Advisory Conferences

High Level Conference on the Future of the European Court of Human Rights. Interlaken Declaration 19 February 2010. <http://www.echr.coe.int/documents/2010_interlaken_finaldeclaration_eng.pdf > accessed 21 October 2016.

European Data Protection Supervisor Opinions

Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC), 7, para 35 <www.edps.europa.eu/.../Opinions/2011/11-05-30_Evaluation_Report…> accessed 25 September, 2015.

European Parliament Publications

Bowden C, 'The US surveillance programmes and their impact on EU citizens' fundamental rights.' (2013) *European Parliament* Directorate-General For Internal Policies, 26.

'Fighting Cyber Crime and Protecting Privacy in the Cloud' Directorate-General For Internal Policies. Centre for the Study of Conflicts, Liberty and Security (European Parliament, 2012). 1 34.<http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/study_cloud_/study_cloud_en.pdf> accessed 1 April 2015.

European Union Commission Decisions

Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML.> accessed 13 July 2016.

European Union Commission Communications

Communication from the Commission to the European Parliament and the Council entitled 'Rebuilding Trust in EU-US Data Flows') COM (2013) 846 final, 27 November 2013) and Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU (COM (2013) 647 final, 27 November 2013).

European Commission Press Releases

EU Commission and United States agree on a new framework for transatlantic data flows: EU-US <http://europa.eu/rapid/press-release_IP-16-216_en.htm> accessed 21 October 2016.

European Union Charters

Charter of Fundamental Rights of the European Union, December 7 2000, 2000 O.J. C 364.

European Union Opinions

Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005) 438 final of 21.09.2005), Article 29 Working Party, 1868/05/EN WP 113, Adopted on 21st October 2005, 1, 2. <http://ec.europa.eu/justice/dataprotection/article29/documentation/opinionrecommendation/files/2005/wp113_en.pdf> accessed 21 September 2016.

Opinion Pursuant to Article 218 (11) TFEU, C-2/13. December 18 2014 <http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d5498e825298f346e99568a78451b88b99.e34KaxiLc3eQc40LaxqMbN4Pa3mSe0?text=&docid=160882&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=432736> accessed 7 September 2016.

European Union Statements

Joint Statement by the Council and the Commission in relation to Article 12 (Evaluation) of the Draft Directive, 5777/06 ADDI February 10, 2006.

European Union Directives

European Parliament and Council Directive 95/46. On the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995, O.J. (L 281) EC.

Directive 97/66/EC of 15 December 1997 of the European Parliament and of the Council Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector,

O.J. (L 24/1) 30.1.98.

Directive 2002/58/EC Of The European Parliament And Of The Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications) (OJ L 201, 31.7.2002, 37.

Directive 2006/24/EC Of The European Parliament And Of The Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC O.J. (L 105/54).

Directive 2016/680, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JIA, 2016 O.J. (L 119) 89.

European Union Regulations

Regulation (EU) 2016/679 Of THE European Parliament And Of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) .

Proposal for a Regulation Of The European Parliament And Of The Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) European Commission (Brussels, 10.1.2017) COM(2017) 10 final 2017/0003 (COD).

Irish Legislation

Irish Criminal Justice (Terrorist Offences) Act, 2005

UK Legislation

Regulation of Investigatory Powers Act, 2000 (RIPA)

Letters

Retention Directive by Letter C(2011) 4111 of 16 June 2011, in the case 2011/2089 whereby the European Commission initiated proceedings against Romania for failing to implement the Data Retention Directive and was given to months to do so.

Letter from Stefano Rodatà Chairman of the Article 29 Working Party to the European Parliament, Commission and Council of 7 June, 2001. Available at: <http://www.statewatch.org/news/2001/jun/07Rodota.pdf> accessed 3 September, 2016.

Reports

Church Committee Report 1976

Online Academic Publications

Cahall B, Bergen P, Sterman D, and Schneider E, 'International Security Policy Papers: Do NSA's Bulk Surveillance Programs Stop Terrorists? *International Security* (January 13, 2014) <https://www.newamerica.org/international-security/policy-papers/do-nsas-bulk-surveillance-programs-stop-terrorists/> accessed 10 November 2016.

De Londras F, 'Using The ECHR In Irish Courts: More Whisper Than Bang?' *Using the ECHR: Where are we Now?* (PILA Seminar, 13 May, 2013). available at: <https://www.ucd.ie/t4cms/pilaechrseminar130511fdelondras.pdf>. accessed 24 July, 2017.

Heuman S, and Scott B, 'Law and Policy in Internet Surveillance Programs: United States, Great Britain and Germany' (2013 September) *Impulse* <https://netzpolitik.org/wp-upload/Nr.25_Law_and_Policy_in_Internet_Surveillance_Programs.pdf> accessed June 7, 2015.

Husovec M, 'First European Constitutional Court Suspends Data Retention After The Decision Of The Court Of Justice Of The EU,' *The Centre for Internet and Society* 28 April 2014 <http://cyberlaw.stanford.edu/blog/2014/04/first-european-constitutional-court-suspends-data-retention-after-decision-court> accessed 17 September 2016.

Lohman J, 'Hamdan v Rumsfeld, 548 U.S. 557 (2006)' *Lawfare Hard National Security Choices* (12 November, 2012) <http://www.lawfareblog.com/wiki/the-lawfare-wiki-document-library/post-911-era-materials/post-911-era-materials-court-cases/hamdan-v-rumsfeld-548-us-557 2006/> accessed 23 March 2015.

Online Publications

Bracy J, 'Model clauses in jeopardy with Irish DPA referral to CJEU' (25.5.2016) *The Privacy Advisor*, <https://iapp.org/news/a/model-clauses-in-jeopardy-with-irish-dpa-referral-to-cjeu/> accessed 23 July 2016.

Cohn C, and Jaycox M, 'USA Freedom Act Passes: What We Celebrate, What We Mourn, and Where We Go From Here' (June 2, 2015) *Electronic Frontier Foundation* <https://www.eff.org/deeplinks/2015/05/usa-freedom-act-passes-what-we-celebrate-what-we-mourn-and-where-we-go-here> accessed 5 June, 2015.

(------ ---------) Foreign Intelligence Surveillance Act Court Orders, 1979-2015.' *Electronic Privacy Information Centre* <https://www.epic.org/privacy/surveillance/fisa/stats/> accessed 3 December 2016.

Gallagher R, U.S. 'Spy Law Authorizes Mass Surveillance of European Citizens' (January 8, 2013) *future*tense The Citizen's Guide To The Future* <http://www.slate.com/blogs/future_tense/2013/01/08/fisa_renewal_report_suggests_spy_law_allows_mass_surveillance_of_european.html> accessed 29 March 2015.

Gormley K, 'Long Live the Constitution,' (November 17, 2002) *Pittsburgh Post-Gazette* <http://old.post-gazette.com/forum/comm/20021117edgorm1117p1.asp> accessed 7 January 2017.

Goitein E, 'The FISC's Newest Opinion: Proof of the Need for an *Amicus*' (June 23, 2015) *Just Security* <https://www.justsecurity.org/24134/fiscs-newest-opinion-proof-amicus/> accessed 23 December 2016.

(------- --------) 'Google and the "Right to be Forgotten" - What the Court Said and Why it Matters' (15 May 2014). *Mason Hayes and Curran Technology Law Blog* <http://www.mhc.ie/latest/blog/google-and-the-right-to-be-forgotten-what-the-court-said-and-why-it-matters> accessed 11 September 2016

Hudec, J.G, 'Unlucky *Shamrock* - The View From the Other Side' (2000) 44(5) Central Intelligence Agency Library <https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol44no5/html/v44i5a12p.htm> accessed 21 November 2016.

Maxwell W, and Wolf W, 'A Global Reality: Government Access to Data in the Cloud: A Comparative analysis of ten international jurisdictions' (23 May, 2012) *A Hogan Lovells White Paper* 1 <http://www.hldataprotection.com/uploads/file/Revised%20Government%20Access%20to%20Cloud%20Data%20Paper%20(18%20July%2012).pdf> accessed 7 January 2017.

Lynskey O, 'Tele2 Sverige AB and Watson et al: Continuity and Radical Change' (January 12, 2017) *European Law Blog* <http://europeanlawblog.eu/2017/01/12/tele2-sverige-ab-and-watson-et-al-continuity-and-radical-change/> accessed 12 January 2017.

Maxwell W, and Wolf C, 'A Sober Look at National Security Access to Data in the Cloud. Extravagant Claims About U.S. Access That Ignore Access by Foreign Jurisdictions' (May 22, 2013) *A Hogan Lovells White Paper* 1 <http://www.hldataprotection.com/files/2013/05/A-Sober-Look-at-National-Security-Access-to-Data-in-the-Cloud.pdf> accessed 7 January 2017.

(--------- --------) 'NSA Spying on Americans' *Electronic Frontier Foundation* <https://www.eff.org/nsa-spying> accessed 9 January 2017.

Peers S, 'The data retention judgement: The CJEU prohibits mass surveillance,' *EU Law Analysis* (8 April 2014) <http://eulawanalysis.blogspot.ie/2014/04/the-data-retention-judgment-cjeu.htm> accessed 26 September 2016.

Posner, E.A., S*tatement to the Privacy & Civil Liberties Oversight Board*, 14 March 2014, available online at <pclob.gov/Library/20140319-Testimony-Posner.pdf> accessed 19 January, 2017).

Schneier on Security 29 December 2005. <https://www.schneier.com/blog/archives/2005/12/project_shamroc.html> accessed 22 November 2016.

(----- --------) 'The CJEU rules that Data Retention Directive is invalid' *European Data Protection Supervisor* (Press Statement, 8 April, 2014). <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2014/14-04-08_Press_statement_DRD_EN.pdf. accessed 8 April 2014.

Van Oversttaeten T, and Entraygues A, 'The European Court of Justice to rule on the validity of standard contractual clauses' (30 May, 2016) *Linklaters* 1. :<http://www.linklaters.com/pdfs/mkt/brussels/160530_Alert_The_European_Court_of_Justice_to_rule_on-the_validity_of_standard_contractual_clauses.pdf.> accessed 29 September 2016.

White M, 'A Threat to Human Rights? The new e-Privacy Regulation and some thoughts of Tele2 and Watson' (10 January, 2017) *EU Law Analysis* <http://eulawanalysis.blogspot.ie/2017/01/a-threat-to-human-rights-new-e-privacy.html> accessed 17 January 2017.

Woods L, 'Zacharov v Russia: Mass Surveillance and the European Court of Human Rights' (16 December, 2015) *EU Law Analysis* <http://eulawanalysis.blogspot.ie/2015/12/zakharov-v-russia-mass-surveillance-and.html> accessed 21 January 2016

Hearings

Campbell Iain, Venice Commission, Speaking Notes, European Parliament Hearing on Mass Surveillance, 7th November 2013. <http://www.europarl.europa.eu/document/activities/cont/201311/20131114ATT74429/20131114ATT74429EN.pdf> accessed 23 December 2016.

Hearing on Current and Projected National Security Threats to the United States Before the Senate Select Committee on Intelligence, 113th Cong., 1st Sess., at 66 (March 12, 2013). Available at: <http://www.intelligence.senate.gov/131113pdfs/11389.pdf> Accessed 29 March 2015.

Unpublished Ph.Ds

Lester G, 'External Accountability: Congress, Opposition, and Oversight Development,' unpublished Ph.D Dissertation, University of California, Berkley, 2012.

U.S. Senate Reports

Senate Report. No. 95-604 (1977)

U.S. Senate Resolutions

Senate Resolution 400, 94th Congress (1976).

Online Media

Bamford J, 'The NSA Is Building The Country's Biggest Spy Centre (Watch what you say)' *Wired Magazine* March 15, 2012 <http://www.wired.com/2012/03/ff_nsadatacenter/> accessed 28 April 2015.

Benkler Y, 'In secret, Fisa court contradicted US Supreme Court on constitutional rights' (22 September, 2013) *The Guardian* <https://www.theguardian.com/commentisfree/2013/sep/22/secret-fisa-court-constitutional-rights> accessed 1 January 2017.

Burgess, P.J, 'Security After Privacy: After The Transformation of Personal Data in the Age of Terror' (Oslo 5/2008) *International Peace Research Institute*, Policy Brief, <http://file.prio.no/Publication_files/Prio/Security%20after%20Privacy%20(PRIO%20Policy%20Brief%205-2008).pdf> accessed 21 November 2016.

Cauley L, 'NSA has massive database of Americans' phone calls' (10 May 2006) USATODAY <http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm> accessed 29 April 2015.

Cornish A, 'Patriot Act Architect Criticizes NSA's Data Collection' (20 August, 2013) *NPR* <http://www.npr.org/templates/story/story.php?storyId=213902177> accessed 30 April 2015.

Cuccinelli K, Fitzgibbons M, 'A Much-Needed Facelift for the fourth Amendment' *Washington Examiner* (20 January, 2015) <http://www.washingtonexaminer.com/a-much-needed-facelift-for-the-fourth-amendment/article/2558889. accessed 16 January 2017.

Dorf, M.C. 'A Brief History of Executive Privilege, from George Washington to Dick Cheney.' <http://writ.news.findlaw.com/dorf/20020206.html> accessed 20 March 2015.

(----------) 'Dwyer's challenge to use of phone records to be heard next year' *RTE.ie* (15 June, 2017) <https://www.rte.ie/news/2017/0615/883049-graham-dwyer/> accessed 18 June 2017.

(--------- --------) Europe v Facebook, Press Release of 26 May, 2016. Cited in: 'Europe vs. Facebook: Austrian activist wins another legal battle over data protection' *RT* (26 May, 2016) <https://www.rt.com/news/344519-europe-vs-facebook-austrian-activist/> accessed 28 August 2016.

(-------- ---------) 'EU Weakens Data Protection at U.S. Request' (13 June, 2013) *Spiegel Online* <http://www.spiegel.de/international/world/eu-weakened-data-protection-laws-ahead-of-prism-spy-program-a-905520.html> accessed 1 June 2015.

Follorou J, and Johannes F, 'Révélations sur le Big Brother francais, (4 July, 2013) *Le Monde*, <www.lemonde.fr> accessed 28 August 2015.

Gellman B, 'NSA Broke Privacy Rules Thousands of Times Per Year, Audit Finds' *The Washington Post* (August 15, 2013) <https://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html?utm_term=.65c406d3aadf> accessed 10 January 2017.

(------- ------) 'Germany Spied on Friends and Vatican' *Spiegel Online* (November 7, 2015) <http://www.spiegel.de/international/germany/german-bnd-intelligence-spied-on-friends-and-vatican-a-1061588.html> accessed 9 January 2017.

Goodman A, 'NSA Whistleblower Thomas Drake Prevails Against Charges in Unprecedented Obama Administration Crackdown.' (21 March, 2012) *Democracy Now* <http://www.democracynow.org/2012/3/21/in_unprecedented_obama_admin_crackdown_nsa> accessed 21 April 2015.

Gude H Poitras L, and Rosenbach M, 'Mass Data: Transfers from Germany Aid U.S. Surveillance' (5 August, 2013) *Spiegel Online* <http://www.spiegel.de/international/world/german-intelligence-sends-massive-amounts-of data-to-the-nsa-a-914821.html> accessed 5 June, 2015.

Harris A, 'Spy agency Sought U.S. Call Records Before 9/11, Lawyers Say.' (*Bloomberg* 30 June 2006) <http://www.bloomberg.com/apps/news?pid=newsarchive&sid=abIV0cO64zJE> accessed 29 March 2015.

Isikoff M, 'The Whistleblower Who Exposed Warrantless Wiretaps' (13 December, 2008) *Newsweek* <http://www.newsweek.com/whistleblower-who-exposed-warrantless-wiretaps-82805> accessed 28 April 2015.

Lable C, and Vincour N, 'French Prosecutor Investigates U.S. Prism spying scheme' (28 August, 2013) *Reuters* 28 <http://www.reuters.com/article/2013/08/28/us-usa-security-france-idUSBRE97R0WE20130828> accessed 6 June 2015.

Levin J, 'Total Preparedness,' *National Law Review* (13 February, 2005). <http://www.national review.com/comment/comment-levin02l303.asp.> accessed 20 December 2016

Kerr O, 'How much has Congress changed on surveillance?' (2 June 2015) *The Washington Post* <https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/06/02/how-much-has-congress-changed-on surveillance/?utm_term=.d75a549c11e0> Accessed 29 December 2016.

McLaughlin J, 'US Mass Surveillance Has No Record of Thwarting Large Terror Attacks Regardless of Snowden Leaks,' (7 November, 2015) *The Intercept* <https://theintercept.com/2015/11/17/u-s-mass-surveillance-has-no-record-of-thwarting-large-terror-attacks-regardless-of-snowden-leaks/> accessed 1 November 2016.

(--------) 'NSA/Surveillance: Damning new revelations and still no judicial inquiry' *fidh Worldwide Movement For Human Rights* <https://www.fidh.org/en/region/europe-central-asia/france/nsa-surveillance-damning-new-revelations-and-still-no-judicial. accessed 16 June, 2017.

(------ ---------) 'Obama "knew and approved" NSA spying on Chancellor Merkel,' *Russia Today* October 27, 2013. < http://rt.com/news/obama-nsa-spying-merkel-808/> accessed 25 April 2015.

(-------- -------) 'Obama Administration drowning in lawsuits filed over NSA surveillance' (July 16, 2013) RT.COM <http://rt.com/usa/snowden-leaks-surveillance-suits-174/> accessed 24 May 2015.

(----- ------) 'Pentagon's Terror Information Awareness will end,' (September 25 2003) USA To Day.com <http://usatoday30.usatoday.com/news/washington/2003-09-25-pentagon-office_x.htm. accessed 4 January 2017.

Risen J, Lichtblau E, '*Bush Lets **U.S. Spy** on Callers Without Courts,'* (December 16, 2005) *New York Times* <http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all> accessed 3 December 2016.

Robertson A, and Ingraham N, 'USA Freedom Act for NSA reform is voted down in the Senate' (November 18, 2014) *The Verge* <http://www.theverge.com/2014/11/18/7241967/usa-freedom-act-for-nsa-reform-is-voted-down-in-the-senate> accessed 23 December 2016

(------ -------) 'Secret Surveillance Policy Gives U.K. Government Warrantless Access to Bulk NSA Data' *LIBERTIES.EU* <http://www.liberties.eu/en/news/gchq-access-bulk-data> accessed 1 May 2015

Springer P, 'Sun on Privacy. 'Get over It' (26 January 1999) *Wired* <http://archive.wired.com/politics/law/news/1999/01/17538.> accessed 24 November 2016.

Temple-Raston D, 'FISA Court Appears To Be Rubber Stamp For Government Requests' (June 13, 2013) *NPR* <http://www.npr.org/2013/06/13/191226106/fisa-court-appears-to-be-rubberstamp-for-government-requests> accessed 28 December 2016.

(------- --------) 'The German PRISM: Berlin Wants to Spy Too' (17 June, 2013) *Spiegel Online International* <http://www.spiegel.de/international/germany/berlin-profits-from-us-spying-program-and-is-planning-its-own-a-906129.html> accessed 6 June 2015

(------ ---------) 'Tube wi-fi internet plan progresses despite security fears,' BBC News (25 March, 2011) available at: <http://www.bbc.com/news/uk-england-london-12856289> accessed 16 July, 2016.

Tung L, 'Four of Sweden's telecos stop storing customer data after EU retention directive' (11 April, 2014) *ZDNet* <http://www.zdnet.com/article/four-of-swedens-telcos-stop-storing-customer-data-after-eu-retention-directive-overthrown/> accessed 25 November 2016.

Van Buren P, 'Fear the Silence, Not the Noise.' (February 9, 2012) *TomDispatch.com* <http://www.tomdispatch.com/blog/175500/tomgram%3A_peter_van_buren,_in_washington,_fear_the_silence,_not_the_noise/> accessed 23 April 2015.

Wagenseil P, 'NSA Mass Surveillance Useless, Former Bush Official Says,' (24 February, 2014) *Tom's Guide* <www.tomsguide.com/us/rsa-nsa-spy-program-useless,news-18384.html. accessed 21 December 2016.

Foreign Intelligence Surveillance Act Court Orders, 1979-2015.' *Electronic Privacy Information Centre* <https://www.epic.org/privacy/surveillance/fisa/stats/> accessed 3 December 2016.

Position Papers

Obama B, and Beiden J, 'Blueprint for Change: Obama and Beiden's Plan for America' *Obams'08* 1 75 <https://s3.amazonaws.com/s3.documentcloud.org/documents/550007/barack-obama-2008-blueprint-for-change.pdf> accessed 1 May 2015.

(----- -------) 'Human Rights and the Fight Against Terrorism' *Council of Europe Guidelines* (Council of Europe Publishing, March 2005).

(------ --------) "Legal Authorities Supporting the activities of the National Security Agency Described by the President' US Department of Justice, Washington D.C., 20530, (January 19, 2006) 1. 6. <https://epic.org/privacy/terrorism/fisa/doj11906wp.pdf> accessed March 22, 2015.

Rumold M, 'A New Year, A New FISA Amendments Reauthorisation, But the Same Old Secret Law,' (January 10, 2013) *Electronic Frontier Foundation* <https://www.eff.org/deeplinks/2013/01/new-year-new-fisa-amendments-act-reauthorization-same-old-secret-law> accessed 27 April 2015.

Press Briefings

Press Briefing from Alberto Gonzales, U.S. Att'y Gen., and General Michael Hayden, Principal Deputy Director for National Intelligence (Dec. 19, 2005) <http://www.whitehouse.gov/news/releases/2005/12/20051219-1.html> accessed 23 November 2016.

Speeches

Kerr D, Principal Deputy Director of National Intelligence, Remarks and Questions and Answers at the 2007 Geospatial Intelligence (GEOINT) Symposium held on 23 October 2007. Cited in Harper J, 'Reforming Fourth Amendment Privacy Doctrine' (2008) 57 *American University Law Review* 1381.

United States Presidential Statements

Obama B, 'A New Standard of Openness,' White House Video, January 21, 2009. <https://www.whitehouse.gov/photos-and-video/video/a-new-standard-openness> accessed 3 May, 2015.

Obama B, 'President's Memorandum on Transparency and Open Government' (February 24, 2009) - Interagency Collaboration. Memorandum For Heads Of Departments And agencies M-09-12. <https://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_fy2009/m09-12.pdf> accessed 2 May 2015.

Obama B, Remarks By The President On National Security. *The White House* Office of the Press Secretary (May 21, 2009). *National Archives*, Washington D.C. <https://www.whitehouse.gov/the_press_office/Remarks-by-the-President-On-National-Security-5-21-09/> accessed 20 April 2015.

United States Administration Statements

Prepared Statement of Hon. Alberto R. Gonzales, Attorney General of the United States. February 6, 2006 <https://www.justice.gov/archive/ag/speeches/2006/ag_speech_060206.html> accessed 28 October 2016.

Statement by the President, Fairmont Hotel San Jose, California (June 7, 2013) The White House Office of the Press Secretary <https://www.whitehouse.gov/the-press-office/2013/06/07/statement-president> accessed 1 November 2016.

Statement of Administration Policy: H.R. 3361 - USA FREEDOM Act May 21, 2014 <http://www.presidency.ucsb.edu/ws/?pid=105338> accessed 21 December 2016.

United States Administration White Papers

U.S. Department of Justice, White Paper. Legal Authorities Supporting the Activities of the National Security Agency Described By The President. (January 19, 2006) <https://www.justice.gov/sites/default/files/opa/legacy/2006/02/02/whitepaperonnsalegalauthorities.pd> accessed 23 November 2016.

Administration White Paper. Bulk Collection Of Telephony Metadata Under Section 215 Of The USA Patriot Act (August 9, 2013) 1.

United States Administration Press Briefings

Press Briefing by Attorney General Gonzalez and Michael Hayden, Principal Deputy Director for National Intelligence (December 19, 2005) <https://georgewbush-whitehouse.archives.gov/news/releases/2005/12/20051219-1.html> accessed 2 November 2016.

United States Administration Reports

Clarke R.A, Morell M.J, Stone G.R, Sunstein CR., and Swire P, 'Liberty And Security In A Changing World' *Report and Recommendations of The President's Review Group On Intelligence and Communications Technologies* (12 December, 2013) <https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf> accessed 28 December 2016.

Medine D, (Chairman), Brand R, Collins Cook E, Dempsey J, and Wald P, 'Report on the Telephone Records Program Conducted under Section 215 of the USA Patriot Act and on the Operations of the Foreign Intelligence Surveillance Court' (23 January, 2014) *Privacy and Civil Liberties Oversight Board* <https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf> Accessed 28 December, 2016.

Nolan A, Thompson II R.M, and Chu V.S, 'Reform of the Foreign Intelligence Surveillance Courts: Introducing a Public Advocate' *Congressional Research Service* 7-5700. <https://fas.org/sgp/crs/intel/R43260.pdf> accessed 27 December 2016.

Miscellaneous Publications

Bigo D, Carrera S, Hernanz N, Jeandesboz J, Parkin J, Radazzi F, and Scherrer A, 'Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law' (November 2013) 62 CEPS Paper, in *Liberty and Security in Europe.*

(------- --------) The Federalist No. 47: 'The particular Structure of the New Government and the Distribution of Power Among its Different Parts'. James Madison, (*New York Packet* January 30, 1788).

(------ --------) Decision of the Romanian Constitutional Court 1258, 08 October 2009. English translation by Manolea, B and Argesiu, A <http://www.legi-internet.ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf> accessed 19 September 2016.

United Nations Human Rights Committee Resolutions

U.N. Human Rights Committee, General Comment 16. The Right to Respect of Privacy, Family, Home and Correspondence and Protection of Honour and Reputation (Article 17). Section 3, U.N. Doc.HRI/GEN/I Rev. 6 (April 8, 1988).

United Nations Human Rights Office of the High Commissioner for Human Rights. 'Dangerous practice of digital mass surveillance must be subject to independent checks and balances.' (16 July, 2014). <http://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=14875> accessed 24 March, 2015.

United Nations Reports

'The right to privacy in the digital age.' Report of the Office of the United Nations High Commissioner for Human Rights. United Nations General Assembly (30 June 2014) Henceforth cited as A/HCR/27/37

'Report of the Special Rapporteur on the protection and protection of human rights and fundamental freedom' United Nations General Assembly (23 September 2014). Henceforth cited as A/69/397.