Information & Communications Technology Law, 2014
Vol. 23, No. 3, 192–219, http://dx.doi.org/10.1080/13600834.2014.970375

Routledge
Taylor & Francis Group

The pendulum effect: comparisons between the Snowden revelations and the Church Committee. What are the potential implications for Europe?

Maria Helen Murphy*

Law Department, National University of Ireland, Maynooth, Ireland

This article considers how the pendulum metaphor can be applied to shifts in popular opinion concerning the right to privacy. At times, the media portrays privacy as an individualistic right, serving at the behest of criminals and terrorists. Every so often, however, an event occurs that starkly reminds the public of the value of privacy. Public opinion drives debate and this debate often leads to legal reform. The Church Committee, formed in response to the Watergate scandal, is a classic example of the effect the exposure of abuse can have on the regulation of privacy. Over time, however, legislative gains in privacy protection have a tendency to erode. In addition, extreme events, such as the terrorist attacks of 9/11, can cause the pendulum to swing back to the opposite position. Following the exposure of mass surveillance practices by Edward Snowden, the world has, once again, been questioning government surveillance activities. This article seeks to consider the transatlantic impact of the National Security Agency revelations. Transparency is highlighted as a crucial regulating force on excessive government interference with privacy rights.

Keywords: Snowden; surveillance; privacy; data retention; European Union

Introduction

The concept of a swinging pendulum frequently serves as a political metaphor, illustrating oscillations from one policy position to another over time.[1] The metaphor borrows from the scientific principle that the restoring force of gravity, combined with the mass of a pendulum, will cause it to swing back and forth indefinitely. In addition to being used to portray electoral swings,[2] trends in criminal justice,[3] and education

*Email: maria.murphy@nuim.ie

[1]See, for example, M Lebo and H Norpoth, 'The PM and the Pendulum: Dynamic Forecasting of British Elections' (2007) 37 BJ Pol S 71; S Ranchod-Nilsson, 'Gender Politics and the Pendulum of Political and Social Transformation in Zimbabwe' (2006) 32 JSAS 49; B Jackson, *The Challenge of Domestic Intelligence in a Free Society: A Multidisciplinary Look at the Creation of a US Domestic Counterterrorism Intelligence Agency* (Rand Corporation, 2009) 90, 112.

[2]M Harrop, 'The Pendulum Swings: The British Election of 1997' (1997) 32 Gov't & Oppos 305; S Severinghaus, 'Mongolia in 2000: The Pendulum Swings Again' (2001) 41 Asian Surv 61; D Collier, 'The Ideal Pendulum Swing: From Rhetoric to Reality' (2008) 13 BJCL 175.

[3]G Miller, 'Watching the Correctional Pendulum Swing' (1993) 62 FBI Law Enforcement Bulletin 24; D Spader, 'Megatrends in Criminal Justice Theory' (1985–1986) 13 AJCL 157; D Collier, 'The Ideal Pendulum Swing: From Rhetoric to Reality' (2008) 13 BJCL 175; K Parker, 'Coddling Not Allowed'

reforms,[4] the metaphor of the pendulum has been utilised by many to demonstrate how public opinion regarding the balance between security and surveillance has tended to see–saw at various points in history.[5] The logic underlying this theory is that in times of crisis, the government may curtail civil liberties in order to protect national security. Etzioni has commented that once the threat has passed, the intrusive measures 'can gradually be rolled back.'[6] While this understanding of the balance between the powers of the State and the protection of civil liberties may place undue faith in the ability of societal forces to correct the excesses of its government systems over time, it can be useful to illustrate observable shifts in public opinion and subsequent developments in government policy. Due to the secrecy of surveillance systems, the public often only learns of the true nature of government activity following the actions of a whistle-blower, like Edward Snowden. Due to this information deficit, the pendulum is only prone to swing back in favour of greater protection of privacy rights once the relevant information enters the public domain.

Often, the importance of privacy is weighed against the importance of national security. This balancing can place an undue burden on the right to privacy, as a threat to privacy appears remote in comparison to a threat to personal safety. Privacy, as a fundamental right, has faced criticisms of varying degrees of severity. At the more moderate end of the scale, Hixon has described privacy as being a right worth protecting, but not worth protecting 'on the grand scale that claims for privacy are pressed today.'[7] More negatively, privacy has been described as a 'cult' that 'rests on an individualist conception of society.'[8] In popular discourse, privacy is often wholly identified as a benefit to the individual, weighing against general social goods, such as security.[9] Despite the vigorous protestations of civil liberties organisations a frequently made argument is that privacy is a moribund right that people no longer need and is, in fact, an anachronistic value in modern life.[10] Predictably, the argument goes, in the war on terror and organised crime, privacy is even less important. Popular culture is infected with an 'us v. them' mentality

Chicago Tribune (Chicago, 24 November 1999) <articles.chicagotribune.com/1999–11-24/news/9911240048_1_discipline-psychotropic-greater-communication-and-education> accessed 10 October 2014.

[4]P Wolfe and L Poynor, 'Politics and the Pendulum: An Alternative Understanding of the Case of Whole Language as Educational Innovation' (2001) 30 Educational Researcher 15–20; C Mellon, 'Technology and the Great Pendulum of Education' (1999) 32 JRCE 28; D Coulby, R Cowen and C Jone, *Education in Times of Transition* (Psychology Press, 2000).

[5]D Clarke and E Neveleff, 'Secrecy, Foreign Intelligence, and Civil Liberties: Has the Pendulum Swung Too Far?' (1984) 99 PSQ 493; P Pillar, 'The Pendulum of Opinion on Security and Privacy' *The National Interest* (11 June 2013) <www.brookings.edu/research/opinions/2013/06/09-security-privacy-surveillance-phone-internet-terrorism-pillar> accessed 10 October 2014; O Kerr, 'Technology, Privacy, and the Courts: A Reply to Colb and Swire' 102 Mich L Rev 933; R Matthew and G Shambaugh, 'The Pendulum Effect: Explaining Shifts in the Democratic Response to Terrorism' (2005) 5 Analyses of Social Issues and Public Policy 223; D Solove, 'Data Mining and the Security-Liberty Debate' (2008) 75 U Chi L Rev 343.

[6]A Etzioni, *The Limits of Privacy 25* (Basic Books, 1999) 25; See D Solove, *Nothing to Hide: The False Trade-off between Privacy and Security* (Yale University Press, 2011) 55–56.

[7]G Laurie, *Genetic Privacy: A Challenge to Medico-legal Norms* (CUP, 2002) 47. R Hixson, *Privacy in a Public Society* (OUP, 1987) 4.

[8]H Arndt, 'The Cult of Privacy' (1949) 21 AQ 68, 70–71; S Benn, 'Privacy, Freedom, and Respect for Persons' in F Schoeman (ed), *Philosophical Dimensions of Privacy* (CUP, 1984) 303.

[9]See D Solove, *Understanding Privacy* (Harvard University Press, 2008) 10.

[10]J Rule, *Privacy in Peril* (OUP, 2007) xi.

where the idea of protecting privacy rights is viewed by many as abhorrent pandering to terrorists and criminals.[11]

Such complacency is occasionally checked, however. Often this task is performed by the press, such as when the News of the World phone hacking scandal was exposed.[12] When reports emerged exposing the phone hacking of celebrities, politicians, and members of the Royal Family, there was mild public interest.[13] When the recognisable and relatable figure of Millie Dowler and her family became part of the story, however, the increased level of outrage was palpable.[14] Revelations like this make people stop and think, turn the intangible into the material and remind people that privacy is a right worth protecting. This article considers how non-voluntary transparency has influenced surveillance policy in the past by examining the aftermath of the Watergate scandal and the Bush administration warrantless wiretapping scandal. The Edward Snowden revelations have, once again, brought the question of privacy to the fore of public consciousness. By refusing to view this latest scandal in isolation, this article gains insight from previous experiences. This article considers the effect of the Snowden revelations on public opinion and assesses the implications of the disclosures from the European perspective. Transparency is highlighted as a crucial regulating force on excessive government interference with privacy rights.

Watergate and the Church Committee

During the Cold War, public anxiety was high and the threat posed by the Soviet Union was keenly felt. With the Cold War being waged through technological and political competition, the importance of espionage and the fear of foreign spies rose.[15] This environment enabled the rapid expansion of the powers and capabilities of government investigative agencies.[16] In spite of the fact that public perception tends to associate the abuses exposed following the Watergate scandal solely with the Nixon administration, such a

[11]C Gearty, 'Reflections on Civil Liberties in an Age of Counterterrorism' (2003) 41 OHLJ 185, 187.
[12]The Guardian, *Phone Hacking: How the Guardian Broke the Story* (Guardian Books, 2011).
[13]N Davies, 'Phone Hacking Was Rife at News of the World, Claims New Witness' *The Guardian* (London 8 September 2010) <www.theguardian.com/media/2010/sep/08/phone-hacking-news-of-the-world-witness> accessed 10 October 2014; S Lanville and H Mulholland, 'Met Police Refuse to Reopen Phone-hacking Inquiry' *The Guardian* (London 9 July 2009) <www.theguardian.com/politics/2009/jul/09/police-refuse-reopen-tapping-inquiry> accessed 10 October 2014; N Davies, 'Phone Hacking Approved by Top News of the World Executive – New Files' *The Guardian* (London 15 December 2010) <www.theguardian.com/media/2010/dec/15/phone-hacking-sienna-miller-evidence> accessed 10 October 2014.
[14]N Davies and A Hill, 'Missing Milly Dowler's Voicemail Was Hacked by News of the World' *The Guardian* (London 5 July 2011) <www.theguardian.com/uk/2011/jul/04/milly-dowler-voicemail-hacked-news-of-world> accessed 10 October 2014; P Wilkinson, 'Milly Dowler: Murdered Schoolgirl at Heart of Hacking Scandal' *CNN* (Atlanta, USA 29 November 2012) <edition.cnn.com/2012/11/28/world/europe/milly-dowler-profile/> accessed 10 October 2014.
[15]F Schwarz and A Huq, *Unchecked and Unbalanced: Presidential Power in a Time of Terror* (New Press, 2007) 14–24. For discussion of the exaggerated domestic Communist threat, see H Johnson, *The Age of Anxiety: McCarthyism to Terrorism* (Harcourt, 2005) and R Rovere, *Senator Joe McCarthy* (Harcourt, 1959).
[16]A Cinquegrana, 'The Walls (and Wires) have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978' (1989) 137 U Pa L Rev 793, 797–798; W Diffie and S Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption* (MIT Press, 1998) 155–165; D Solove, 'Reconstructing Electronic Surveillance Law' (2003–2004) 72 Geo Wash L Rev 1264.

perception is misleading. While Nixon and Hoover certainly abused their powers, administrations from Roosevelt's through to Nixon's all sanctioned overly broad investigations and lawless conduct.[17]

In spite of this, Watergate was a crucial moment in American history.[18] Following the exposure of President Nixon's commandeering of the US intelligence agencies in order to investigate his political opponents, there was an unprecedented backlash against the expansion of Executive power.[19] In addition to the resignation of President Nixon, the year of 1974 saw the introduction of the Privacy Act to govern the collection, maintenance, and use of personally identifiable information about individuals by federal agencies.[20] In the following year, the US Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities set to work under the chairmanship of Senator Frank Church (Church Committee).[21]

Among the many examples of abuses perpetrated by the US intelligence agencies – and exposed by the Church Committee – were a panoply of intrusive and covert measures directed against Martin Luther King.[22] Martin Luther King was just one victim among many who were targeted under the government Counter Intelligence Program (COUNTELPRO) that was set up in order to investigate political dissent.[23] Other targets included members of the American Communist Party and opponents of the war in Vietnam.[24] In addition, the Church Committee reported that surveillance had been directed at figures as diverse as Albert Einstein, Muhammad Ali, certain members of Congress, and the Supreme Court.[25] The Church Committee was severely critical of the intelligence agencies, pointing out that certain techniques used by the agencies were contrary to the 'the ideals which have given the people of this country and of the world hope for a better, fuller,

[17]Hearings Before the Select Committee to Study Governmental Operations with Respect to Intelligence Activities of the US Senate (1976) 94th Congress Volume 2, 10. When Roosevelt began his term as President in 1933, the FBI was comprised of 353 agents. On his death in 1945, the number of agents had increased to 4380. R Kessler, *The Bureau: The Secret History of the FBI* (St Martin's, 2002) 57; D Solove, 'Reconstructing Electronic Surveillance Law' (2003–2004) 72 Geo Wash L Rev 1264, 1272. F Schwarz and A Huq, *Unchecked and Unbalanced: Presidential Power in a Time of Terror* (New Press, 2007) 24.

[18]F Emery, *Watergate* (Simon and Schuster, 1995); L Liebovich, *Richard Nixon, Watergate, and the Press: A Historical Retrospective* (Greenwood Publishing Group, 2003).

[19]K Olson, *Watergate: The Presidential Scandal that Shook America* (University Press of Kansas, 2003).

[20]Privacy Act 1974 <http://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf> accessed 10 October 2014.

[21]R Miller (ed), *US National Security, Intelligence and Democracy: From the Church Committee to the War on Terror* (Routledge, 2008) 1.

[22]For example, the FBI intercepted King's telecommunications and installed surveillance devices in his hotel room. F Schwarz and A Huq, *Unchecked and Unbalanced: Presidential Power in a Time of Terror* (New Press, 2007) 21–24. See also C Gentry, *J Edgar Hoover: The Man and the Secrets* (WW Norton, 1991) 140–142.

[23]R Powers, *Secrecy and Power: The Life of J Edgar Hoover* (Free Press, 1987), 339; D Solove, 'Reconstructing Electronic Surveillance Law' (2003–2004) 72 Geo Wash L Rev 1264, 1274.

[24]D Solove, 'Reconstructing Electronic Surveillance Law' (2003–2004) 72 Geo Wash L Rev 1264, 1274.

[25]D Solove, 'Reconstructing Electronic Surveillance Law' (2003–2004) 72 Geo Wash L Rev 1264, 1274; C Gentry, *J Edgar Hoover: The Man and the Secrets* (WW Norton, 1991) 140–142; F Jerome, *The Einstein File: J Edgar Hoover's Secret War Against the World's Most Famous Scientist* (St Martin's Press, 2002).

fairer life.'[26] Senator Frank Church highlighted the ever-present risk of excessive executive power when he pointed out that extensive surveillance capabilities could at any time, 'be turned around on the American people and no American would have any privacy left, such is the capability to monitor everything: telephone conversations, telegrams, it doesn't matter. There would be no place to hide.' In a striking statement, Church warned America of the potential end result of excessive executive power and opacity:

> I don't want to see this country ever cross the bridge. I know the capacity that is there to make tyranny total in America, and we must see to it that this agency and all agencies that possess this technology operate within the law and under proper supervision, so that we never cross over that abyss. That is the abyss from which there is no return.[27]

The Church Committee identified several significant flaws in the operation of the US intelligence services. Among the most significant flaws highlighted were the presence of ambiguous laws which granted wide discretion to the members of the executive branch, the expectation of permanent secrecy among inside parties, and weak congressional oversight resulting in a lack of accountability.[28] Each of these weaknesses reinforced each other by providing a hospitable environment for overreach where ambiguity and opacity were the norm. When individuals never expect their actions to be reviewed, they are unlikely to expend much time assessing the legal implications of their chosen course of action. Each of these lessons remains relevant today.

Out of the Watergate scandal, the findings of the Church Committee, and public dissatisfaction with executive abuse grew an inter-branch compromise in the shape of the Foreign Intelligence Surveillance Act 1978 (FISA).[29] FISA was created in order to regulate the collection of intelligence on foreign powers within the USA.[30] The Act was designed under the reasoning that a more permissive regime is justifiable when collecting foreign intelligence.[31] This approach was supported by the traditional view that enemies of the

[26]Select Committee to Study Governmental Operations, 'Intelligence Activities and the Rights of Americans' Bk II v, Senate Resolution 21 (27 January 1975) 285 <http://www.aarclibrary.org/publib/church/reports/ir/pdf/ChurchIR_6_Addenda.pdf> accessed 10 October 2014. F Schwarz and A Huq, *Unchecked and Unbalanced: Presidential Power in a Time of Terror* (New Press, 2007) 23.
[27]J Bamford, 'The Agency That Could Be Big Brother' *New York Times* (New York 25 December 2005) <www.nytimes.com/2005/12/25/weekinreview/25bamford.html?pagewanted=print> accessed 10 October 2014; ——, 'High-Level US Government Officials Have Warned for 40 Years that Mass Surveillance Would Lead to Tyranny in America' (3 July 2013) *Washington's Blog* <www.washingtonsblog.com/2013/07/top-experts-have-warned-for-50-years-that-mass-surveillance-would-lead-to-tyranny-in-america.html> accessed 10 October 2014.
[28]F Schwarz and A Huq, *Unchecked and Unbalanced: Presidential Power in a Time of Terror* (New Press, 2007) 5, 23–24, 45–47.
[29]According to a Senate Report, 'This legislation is in large measure a response to the revelations that warrantless electronic surveillance in the name of national security has been seriously abused.' Senate Report Number 95–604 (1977), 7. R Dawson, 'Shifting the Balance: The DC Circuit and the Foreign Intelligence Surveillance Act of 1978' (1993) 61 Geo Wash L Rev 1380, 1386; D Solove, 'Reconstructing Electronic Surveillance Law' (2003–2004) 72 Geo Wash L Rev 1264, 1277. F Schwarz and A Huq, *Unchecked and Unbalanced: Presidential Power in a Time of Terror* (New Press, 2007) 50, 53. Foreign Intelligence Surveillance Act of 1978, Pub L No 95–511, 92 Stat 1783.
[30]D Solove, 'Reconstructing Electronic Surveillance Law' (2003–2004) 72 Geo Wash L Rev 1264, 1289. P Swire, 'The System of Foreign Intelligence Surveillance' (2003–2004) 72 Geo Wash L Rev 1306.
[31]A different regime was to operate in the domestic context, for example the Federal Wiretap Act of 1968 applied to the interception of domestic conversations using telephone lines. This Act was later

state are more likely to be foreigners and that in any case foreigners are not entitled to the same protection as American citizens. FISA created a special court of federal district court judges and this court was assigned the authority to grant foreign intelligence surveillance orders.[32] Hearings in the FISA Court are held *ex parte* and in secret.[33] According to the original understanding, FISA was to serve as the 'exclusive means' to conduct electronic foreign intelligence surveillance.[34]

While the FISA procedure was never a glowing example of transparent procedure, having been evocatively described as being held in a 'cipher-locked windowless, secure room on the top floor of the Department of Justice,' its original incarnation was a significant achievement in the light of how jealously executive authorities guard their control over surveillance operations.[35] Prior to the report of the Church Committee, excessive secrecy had facilitated the continual expansion of the executive branch by inhibiting the corrective force of public opinion. The exposure of the extent of the executive abuse led to significant reform that brought the balance between security and civil liberties closer to equilibrium.

While the public reaction and legislative change that arose following the Church Committee report supports the pendulum theory, the pendulum metaphor is, of course, inadequate to fully illustrate the ebb and flow of surveillance policy. History has shown us that when new safeguards and procedures are set in place, there is quite often a trickle effect where the executive begins to find methods to work around any new restrictions.[36] Schwarz points out that while the findings of the Church Committee led to significant reform, 'many of the same flaws began to reappear' by the mid-1980s.[37] In line with the pendulum metaphor, however, a national crisis can have a significant precipitating effect and can catalyse a forceful swing of the pendulum back in favour of security and surveillance at the expense of the right to privacy. In recent times, the response to the attacks of 9/11 is the epitome of this phenomenon.

9/11 and the aftermath

The effects of the attacks of 9/11 were not exclusively felt in New York, Washington, or the USA; there was global aftershock. In spite of this, however, the USA was the direct target and it is, perhaps, not surprising that since the attacks of 9/11, the US Government has become obsessed with 'ferreting out national security threats' with modern surveillance techniques.[38] While the 9/11 Commission reported numerous failures of coordination between intelligence agencies in the build up to the attacks, the most significant failure

updated by the Electronic Communications Privacy Act (ECPA) of 1986. The ECPA has been amended several times since its introduction. FISA has also been amended many times since the original enactment. See B Hund, 'Disappearing Safeguards: FISA Nonresident alien "loophole" is unconstitutional' (2007) 15 Cardozo J Int'l & Comp L 269.

[32]50 USC §1803(a). A review court (The Foreign Intelligence Surveillance Court of Review) was also established to hear government appeals 50 USC §1803(b).

[33]50 USC § 1093(a).

[34]Foreign Intelligence Surveillance Act (FISA) of 1978, 50 USC § 1809 (2000 & Supp II 2002). W Banks, 'The Death of FISA' (2007) 91 Minn L Rev 1209, 1215.

[35]R Turkington and A Allen, *Privacy Law: Cases and Materials* (West Group, 2002) 213.

[36]F Schwarz and A Huq, *Unchecked and Unbalanced: Presidential Power in a Time of Terror* (New Press, 2007) 56.

[37]Ibid 6.

[38]C Slobogin, *Privacy at Risk* (University of Chicago Press, 2007) 3.

highlighted was the 'day-to-day gaps in information sharing.'[39] In spite of this, the executive seized the opportunity to engage in a large-scale expansion of their surveillance powers.

FISA, as originally designed, struck an arguable balance between the need of the executive branch to conduct foreign intelligence surveillance for the purposes of security with its duty to respect the Constitutional requirements under the Fourth Amendment.[40] The post-9/11 climate of fear and patriotism provided the executive branch with the perfect opportunity to push through legislative reform, most notably through the introduction of the PATRIOT Act.[41] The PATRIOT Act amended FISA in several substantial ways. Amendments included broadening the scope of email search warrants, intercepting telephone conversations through the use of roving wiretaps, and increasing the flow of foreign intelligence information between agencies.[42] An amendment of particular concern was the departure from the 'primary purpose' requirement. Section 218 of the PATRIOT Act expanded FISA authorisation for surveillance that had foreign intelligence collection as its primary purpose to include FISA authorisation of surveillance which had the collection of foreign intelligence as a 'significant purpose.'[43] This is problematic as one of the original defences made of the relaxed FISA regime was that it had limited applicability.[44] Following the introduction of the PATRIOT Act, the government could take advantage of the looser framework provided by FISA even when foreign intelligence gathering was 'only one of the goals.'[45]

Even though the PATRIOT Act was not designed in response to the attacks of 9/11, the Act was rushed through Congress in a climate of public fear and political pressure that

[39]The 9/11 Commission Report (WW Norton, 2004) 266–267, 271, 339–352. F Schwarz and A Huq, *Unchecked and Unbalanced: Presidential Power in a Time of Terror* (New Press, 2007) 59.

[40]The Fourth Amendment of the US Bill of Rights protects

> [t]he 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.

[41]Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub L No 107056, 115 Stat 272.

[42]See N Henderson, 'The Patriot Act's Impact on the Government's Ability to Conduct Electronic Surveillance of Ongoing Domestic Communications' (2002) 52 Duke L J 179; J Whitehead and S Aden, 'Forfeiting "Enduring Freedom" For "Homeland Security": A Constitutional Analysis of the USA PATRIOT Act and the Justice Department's Anti-Terrorism Initiatives' (2001–2002) 51 Am U L Rev 1081–1133, 1083; D Solove, 'Reconstructing Electronic Surveillance Law' (2003–2004) 72 Geo Wash L Rev 1264, 1278; D Solove and M Rotenberg, *Information Privacy Law* (Aspen Publishers, 2003) 341–344.

[43]§218 (amending 50 USC. §1804 (a)(7)(B)). A consistent defense of the relaxed FISA procedures has been the externality of the threat. The Executive reminds the public that any restriction on rights is solely in the context of the war on terrorism, drawing comfortable allusions of wartime enemies in a manner that would not affect the life and rights of the average American citizen. It is clear however that the boundaries have been blurred, and Executive expansion under the guise of emergency protection has serious privacy infringing consequences for the average citizen. An important aspect of FISA is the dichotomy created between non-resident aliens and citizens. It was determined that non-resident aliens were more likely than citizens to be officers of a foreign power and therefore more likely to be sources of foreign intelligence information and more likely to be visiting the United States for a limited time. See B Hund, 'Disappearing Safeguards: FISA Nonresident alien "loophole" is unconstitutional' (2007) 15 Cardozo J Int'l & Comp L 269.

[44]D Solove, 'Reconstructing Electronic Surveillance Law' (2003–2004) 72 Geo Wash L Rev 1264, 1290.

[45]Ibid 1291.

facilitated its speedy adoption.[46] Prior to the tragic events that took place on 9/11, the Department of Justice had drafted a comprehensive proposal for 'updating' the surveillance laws, elements of which had been rejected in Congress a number of times previously.[47] The introduction of the PATRIOT Act could be seen as the executive capitalising on the public mood in a time of severe national stress in order to push through a 'wish list.'[48] Taking advantage of a sense of emergency, the executive managed to expand its power as Congress relinquished its role in legislation and leadership. At the time of its enactment, the PATRIOT Act was subjected to criticism on the grounds that it represented an excessive power grab on behalf of the executive. While there were divergent opinions on the issue,[49] Hund went so far as to describe the remaining safeguards designed to prevent the abusive wiretapping of non-resident aliens as a mere 'filing requirement.'[50]

In spite of the concessions Congress made in enacting the PATRIOT Act and amending FISA, and the satisfaction expressed by the Bush administration with the new rules,[51] additional and covert executive expansion was to be uncovered in 2005. In the New York Times, James Risen and Eric Lichtblau exposed how the NSA had been circumventing the updated FISA procedures under a classified presidential order.[52] It was revealed

[46]B Howell, 'Seven Weeks: The Making of the USA PATRIOT Act' (2003–2004) 72 Geo Wash L Rev 1145; R Ericson and K Haggerty, *The New Politics of Surveillance and Visibility* (University of Toronto Press, 2006) 148.

[47]See D Solove, 'Reconstructing Electronic Surveillance Law' (2003–2004) 72 Geo Wash L Rev 1264, 1277 and O Kerr, 'Internet Surveillance Law After the USA Patriot Act: The Big Brother that Isn't' (2003) 97 North Western University Law Review 607, 637.

[48]D Solove, 'Reconstructing Electronic Surveillance Law' (2003–2004) 72 Geo Wash L Rev 1264, 1277.

[49]Orin Kerr has suggested that the criticism of the PATRIOT Act has been overblown. O Kerr, 'Internet Surveillance Law After the USA Patriot Act: The Big Brother that Isn't' (2003) 97 North Western University Law Review 607, 637. For a contrasting opinion see J Whitehead and S Aden, 'Forfeiting "Enduring Freedom" For "Homeland Security": A Constitutional Analysis of the USA PATRIOT Act and the Justice Department's Anti-Terrorism Initiatives' (2001–2002) 51 Am U L Rev 1081–1133. A Washington Post editorial described the public debate over the fate of the law as having 'fallen victim to election-year demagoguery. Critics talk about it as though it were a comprehensive menace, while President Bush and Attorney General John D. Ashcroft often treat skepticism of it as softness in the war on terror.' Editorial, 'More Patriot Act Games' *Washington Post* (Washington July 18 2004) <www.washingtonpost.com/wp-dyn/articles/A58330-2004Jul17.html> accessed 10 October 2014; A Etzioni, *How Patriotic is the Patriot Act?: Freedom Versus Security in the Age of Terrorism* (Routledge, 2004).

[50]B Hund, 'Disappearing Safeguards: FISA Nonresident Alien "Loophole" is Unconstitutional' (2007) 15 CJICL 169, 174.

[51]As pointed out by Greenwald, 'Bush expressly asked for changes to the law in the aftermath of 9/11, thereafter praised the law, and misled Congress and the American people into believing that they were complying with the law.' G Greenwald, 'NSA legal arguments' *Unclaimed Territory* (19 February 2006) <glenngreenwald.blogspot.ie/2006/02/nsa-legal-arguments.html> accessed 10 October 2014.

[52]While the programme was defended by the Bush administration, the administration also attempted to reassure the public that the NSA only had the power to intercept international calls and emails of people in very limited circumstances. In spite of this, it was later uncovered that large telecommunications companies had been providing the NSA with the call records of millions of Americans. L Cauley, 'NSA Has Massive Database of American Phone Calls' *USA Today* (McClean, USA 11 May 2006 <http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm> accessed 10 October 2014; J Bamford, 'The Agency That Could Be Big Brother' *New York Times* (New York 25 December 2005) <http://www.nytimes.com/2005/12/25/weekinreview/25bamford.html?adxnnl=1&pagewanted=all&adxnnlx=1405868637-YQJ01BZqxvR76MAwGpHX1Q> accessed 10 October 2014.

that the NSA had been conducting surveillance without warrants or other judicial approval.[53] While certain aspects of the updated FISA regime were cause for concern following the PATRIOT Act, 'at least the procedures were prescribed by law.'[54]

Instead of assuming responsibility for the warrantless wiretapping programme, the executive branch defended its decision to circumvent even the heavily amended version of FISA.[55] The administration defended the programme as a necessary 'early warning system' justified by statute under the Authorization for Use of Military Force (AUMF)[56] and the US Constitution through the Commander in Chief clause in Article II.[57] The warrantless wiretapping programme was described as an 'unprecedented expansion in presidential power'[58] and was widely criticised for lacking the Fourth Amendment safeguards of individualised suspicion and judicial oversight.[59] The secret programme undermined the existing legal structure as information gathered through the warrantless programme was often subsequently used to obtain FISA Court approval.[60] When used this way, the FISA regime served as mere white-wash for the warrantless programme. Notwithstanding the criticism, however, the scandal failed to penetrate the public consciousness to the degree that might be expected and there was scant evidence of a swing of the pendulum in favour of greater protection of civil liberties.

Instead of engaging in a discussion of privacy-enhancing reform, such as that engaged upon following the report of the Church Committee, Congress enacted the Protect America Act 2007 in what has been described as 'a few days of feverish activity immediately before its summer recess.'[61] The Protect America Act 2007 was designed to provide a legal basis for the activities that the executive had, up until that time, been conducting in secret.[62] The Protect America Act of 2007 removed the warrant requirement for government surveillance

[53] J Risen and E Lichtblau, 'Bush Lets US Spy on Callers Without Courts' *New York Times* (New York 16 December 2005) http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all&_r=0 accessed 10 October 2014; D Eggen and C Lane, 'On Hill, Anger and Calls for Hearings Greet News of Stateside Surveillance' *Washington Post* (Washington 17 December 2005) http://www.washingtonpost.com/wp-dyn/content/article/2005/12/16/AR2005121601825.html> accessed 10 October 2014.

[54] The regime had been criticised for operating under excessive secrecy, for conducting ex parte proceedings, and for failing to provide notice of surveillance to targets. W Banks, 'The Death of FISA' (2007) 91 Minn L Rev 1209, 1233.

[55] Letter from William Moschella to Pat Roberts and others (22 December 2005) 3 <http://www/usdoj.gov/ag/readingroom/surveillance6.pdf> accessed 10 October 2014. The Executive argued that the surveillance only covered situations where one end of the communication is a known or reasonably suspected affiliate of al Qaeda. In the light of the deceptive way the Administration had expanded its powers, these assurances were unconvincing in the absence of any independent verification outside the executive branch.

[56] Pub L No 107-40, 115 Stat 224 (2001).

[57] The claimed inherent power comes from a 'perceived historical responsibility for overseeing collection of foreign intelligence in times of conflict and peace.' Even if one was to accept the legitimacy of this broad authority, however, the 'vague criteria used to select targets' and the minimal internal review provided were difficult to justify. See K Wong, 'The NSA Terrorist Surveillance Program' 43 HJL 517, 522, 527.

[58] K Wong, 'The NSA Terrorist Surveillance Program' 43 HJL 517, 518.

[59] B Nolan and others, 'On NSA Spying: A Letter to Congress' *New York Review of Books* (New York 9 February 2006) <http://www.nybooks.com/articles/18650> accessed 10 October 2014.

[60] J Risen, *State of War* (Free Press, 2006) 54.

[61] P Schwartz, 'Reviving Telecommunications Surveillance Law' (2008) 75 U Chi L Rev 287, 306.

[62] S Bellovin and others, 'Risking Communications Security: Potential Hazards of the Protect America Act' (2008) 6 Security and Privacy Magazine 24, 33.

of foreign intelligence targets 'reasonably believed' to be outside of the USA.[63] Schwartz opines that the exceptions introduced by the Protect America Act swallowed the general rule requiring FISA Court approval.[64]

In addition to legislating for the warrantless surveillance programme, Congress further capitulated to the demands of the executive branch by legislating to inhibit oversight by the court system. Following the 2005 revelations, legal proceedings were initiated across the country in an attempt to make the telecommunications companies liable for their involvement in the warrantless surveillance programme.[65] The lawsuits were an avenue for the public to investigate the details of the programme, but the Bush administration sought retroactive immunity for the telecommunications companies.[66] With the granting of immunity to the telecommunications companies, the public was again prevented from discovering what its own government was doing with their information.[67]

It is clear that the 2005 disclosures did not result in an abrupt swing in surveillance law and policy, and the balance between surveillance programmes and the protection of privacy did not experience the 'correction' that might be expected. One explanation for the lack of popular outrage may simply be that the terror of the 11 September attacks was still too fresh and the public remained happy to accept greater restriction of their liberties in exchange for a perception of greater security. A related explanation may be the lack of personalisation of the issue in the national conversation. Not only did the whistle-blowers remain in the background of the story,[68] the surveillance was largely perceived as something that affected the 'other' in society.[69] Whether that 'other' was represented by

[63]Later, the FISA Amendments Acts of 2008 and 2012 reauthorised many provisions of the Protect America Act.

[64]P Schwartz , 'Reviving Telecommunications Surveillance Law' (2008) 75 U Chi L Rev 287, 308. By giving the Attorney General and the Director of National Intelligence the power to authorise telecommunications companies to acquire intelligence 'reasonably believed to be outside the United States' the Protect America Act 'stripped' the FISA Court of jurisdiction. Recent Developments, 'Protect America Act of 2007' (2008) 45 HJL 581, 581.

[65]Previously a court order would have been sought by a telecommunication company before disclosing customer calling data to the Government. See J Klosek, *The War on Privacy* (Praeger, 2007) 39–40; See for example, *Hepting v AT&T* 439 F Supp 2d. 974, 984 (ND Cal 2006).

[66]FISA Amendments Act 2008; Z Keller, 'Big Brother's Little Helpers: Telecommunication Immunity and the FISA Amendment Act of 2008' (2009) 70 Ohio St L J 1215, 1230; Recent Developments, 'Protect America Act of 2007' (2008) 45 HJL 581, 593; M Wagner, 'Warrantless Wiretapping, Retroactive Immunity, and the Fifth Amendment' (2009–2010) 78 Geo Wash L Rev 204, 205.

[67]D Eggen, 'Immunity for Telecoms May Set Bad Precedent, Legal Scholars Say' *Washington Post* (Washington 22 October 2007) <www.washingtonpost.com/wp-dyn/content/article/2007/10/21/AR2007102101041.html> accessed 10 October 2014; D Solove, 'The New Foreign Intelligence Surveillance Act' *Concurring Opinions* (11 July 2008) <http://www.concurringopinions.com/archives/2008/07/the_new_foreign.html> accessed 10 October 2014; G Greenwald, 'US Supreme Court Finalizes Gift of Immunity to the Telecom Giants' *Washington Post* (Washington 10 October 2012) <www.theguardian.com/commentisfree/2012/oct/10/supreme-court-telecoms-win-immunity> accessed 10 October 2014.

[68]M Isikoff, 'The Whistleblower Who Exposed Warrantless Wiretaps' *Newsweek* (New York 13 December 2008) <www.newsweek.com/whistleblower-who-exposed-warrantless-wiretaps-82805> accessed 10 October 2014.

[69]A poll conducted by CBS News found that the majority of Americans disapprove of the NSA's surveillance programmes when directed at 'ordinary' Americans, but not when directed at terrorist suspects. S Dutton and others, 'Most Disapprove of Gov't Phone Snooping of Ordinary Americans' CBS News (New York 12 June 2013) <www.cbsnews.com/news/most-disapprove-of-govt-phone-snooping-of-ordinary-americans/> accessed 10 October 2014; E Brown, 'Most Americans Object

suspected terrorists or simply by foreigners and aliens living in the USA, the general public remained comfortable with the concept of 'if you have nothing to hide, you have nothing to fear.'[70] Of course, several key facts distinguish the circumstances of the 2005 revelations from those that emerged in 2013 through the disclosures by Edward Snowden.

The Snowden revelations

It is notable in itself that the NSA revelations of 2013 are commonly referred to as the 'Snowden revelations.' Edward Snowden, the former NSA intelligence contractor and CIA employee, has firmly entered the public consciousness.[71] Snowden made a deliberate choice to not only disclose thousands of documents to selected members of the press, but also chose to expose his identity as the whistle-blower. According to Snowden, he felt he had 'an obligation to explain why I'm doing this and what I hope to achieve.'[72] Snowden has also been considered in his actions; as pointed out by Greenwald, it would be difficult for the government to characterise Snowden as either 'unstable' or 'naive.'[73]

It is also important to highlight that the Snowden revelations exposed the vastness of NSA surveillance operations. Snowden was reported as stating that '[t]he NSA specifically targets the communications of everyone. It ingests them by default. It collects them in its system and it filters them and analyzes them and it measures them and it stores them.'[74] The 'collect it all' mentality of the intelligence agency personalised the issue for many individuals.[75] This perception was fuelled with headlines such as 'NSA collecting phone records of millions of Verizon customers daily' and 'NSA Uses Angry Birds, Candy Crush to Spy on Americans.'[76] The PRISM programme was one of the first stories that

To NSA Surveillance Against "Ordinary" Citizens, But Not Terrorism Suspects: Poll' *International Business Times* (New York 11 June 2013) <www.ibtimes.com/most-americans-object-nsa-surveillance-against-ordinary-citizens-not-terrorism-suspects-poll-1302793> accessed 10 October 2014.

[70]See J Monaghan, 'Terror Carceralism: Surveillance, Security Governance and De/civilization' (2013) 15 P&S 3–22; D Solove, '"I've Got Nothing to Hide" and Other Misunderstandings of Privacy' (2007) 44 San DLR 745.

[71]A Peterson, 'Edward Snowden, Celebrity?' *The Washington Post* (Washington 7 March 2014) <www.washingtonpost.com/blogs/the-switch/wp/2014/03/07/edward-snowden-celebrity/> accessed 10 October 2014.

[72]G Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State* (Metropolitan Books, 2014) 18.

[73]Ibid 31.

[74]A Davidson, 'Edward Snowden, The NSA Leaker, Comes Forward' *New Yorker* (New York 9 June 2013) <www.newyorker.com/online/blogs/closeread/2013/06/edward-snowden-the-nsa-leaker-comes-forward.html> accessed 10 October 2014.

[75]O Garcia, 'NSA Leaks About Spying Are Scaring Some Americans Away From The Internet' *Huffington Post* (New York 22 July 2013) <www.huffingtonpost.com/2013/07/22/nsa-leaks-spying-internet_n_3633510.html> accessed 10 October 2014.

[76]R Levinson-Waldman, 'The Double Danger of the NSA's "Collect It All" Policy on Surveillance' *The Guardian* (London 10 October 2013) <www.theguardian.com/commentisfree/2013/oct/10/double-danger-nsa-surveillance> accessed 10 October 2014; E Nakashima and J Warrick, 'For NSA Chief, Terrorist Threat Drives Passion to "Collect It All"' *Washington Post* (Washington 14 July 2013) <www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html> accessed 10 October 2014; J Mick, 'NSA Uses Angry Birds, Candy Crush to Spy on Americans' *Daily*

emerged from the Snowden leaks and the press coverage of the programme revealed how PRISM enabled the NSA to compel the provision of personal information from popular and pervasive US companies, including Facebook, Microsoft, Apple, Yahoo! and Google.[77] Later reports further documented how personally intrusive surveillance could be.[78] For example, it was discovered that the NSA cooperated with Britain's GCHQ in order to intercept webcam images of millions of individuals not suspected of any wrongdoing.[79]

The Snowden revelations led to popular protest and rallies across the USA.[80] The general sense that NSA surveillance has the potential to affect all citizens, and not just terrorists or criminals, is illustrated by the following statement made at an anti-surveillance rally, 'I am 10. And I don't believe I should worry about every word that I write in my emails to my friends.'[81] While polls have shown that a majority of individuals remain generally supportive of surveillance programmes, a notable shift in public perception has been detected following the Snowden disclosures.[82] Significantly, in a Pew Research Center poll

Tech (New York 28 January 2014) <www.dailytech.com/NSA+Uses+Angry+Birds+Candy+Crush+to+Spy+on+Americans/article34211.htm> accessed 10 October 2014; G Greenwald, 'NSA Collecting Phone Records of Millions of Verizon Customers Daily' *The Guardian* (London 6 June 2013) <www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order> accessed 10 October 2014.

[77]The NSA had gained access to private user content, such as private messages, photos, and videos. G Greenwald and E MacAskill, 'NSA Prism Program Taps in to User Data of Apple, Google and Others' *The Guardian* (London 7 June 2013) <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> accessed 10 October 2014; I Brown and D Korff, 'Foreign Surveillance: Law and Practice in a Global Digital Environment' (2014) 3 EHRLR 243, 243. Initial reporting on the PRISM programme overstated the reach of the programme. In spite of this, the PRISM programme appeared to strike a chord with the public. M Masnick, 'Privacy and Civil Liberties Board Mostly Unconcerned About PRISM Or Backbone Tapping By NSA' *Tech Dirt* (2 July 2014) <https://www.techdirt.com/articles/20140702/06315727755/privacy-civil-liberties-board-mostly-unconcerned-about-prism-backbone-tapping-nsa.shtml> accessed 10 October 2014.

[78]G Greenwald and E MacAskill, 'NSA Prism Program Taps in to User Data of Apple, Google and Others' *The Guardian* (London 7 June 2013) <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data> accessed 10 October 2014; R Lempert, 'PRISM and Boundless Informant: Is NSA Surveillance a Threat?' *Brookings* (13 June 2013) <http://www.brookings.edu/blogs/up-front/posts/2013/06/13-prism-boundless-informant-nsa-surveillance-lempert> accessed 10 October 2014; O Garcia, 'NSA Leaks About Spying Are Scaring Some Americans Away From The Internet' *Huffington Post* (New York 22 July 2013) <www.huffingtonpost.com/2013/07/22/nsa-leaks-spying-internet_n_3633510.html> accessed 10 October 2014.

[79]S Ackerman and J Ball, 'Optic Nerve: Millions of Yahoo Webcam Images Intercepted by GCHQ' *The Guardian* (London 28 February 2014) <www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo> accessed 10 October 2014.

[80]A Fitzpatrick, 'Thousands to Join "Restore the Fourth" Anti-NSA Rallies' *Mashable* (2 July 2013) <mashable.com/2013/07/02/restore-the-fourth/> accessed 10 October 2014; In addition, the disclosures spurred the creation of a movement – comprising technology companies and civil liberties groups – that has united in an attempt to improve encryption standards. K Zetter, 'Anti-surveillance Movement Wants to "Reset the Net"' *Wired* (San Francisco 7 May 2014) <www.wired.co.uk/news/archive/2014-05/07/reset-the-net> accessed 10 October 2014.

[81]D Kuriakose, '1984 Day Sees "Restore the Fourth" Protests Across the Country' *Mashable* (New York 5 August 2013) <mashable.com/2013/08/04/1984-day> accessed 10 October 2014.

[82]A Pew Research Center poll conducted in June 2013 found that 56% of Americans believe that the NSA's collection and tracking of telephone records is an acceptable way for the government to investigate terrorism. In the same poll, however, 41% of those polled were found to believe the tactics to be unacceptable. See ——, 'Majority Views NSA Phone Tracking as Acceptable Anti-terror Tactic' *Pew Research Center* (10 June 2013) <www.people-press.org/2013/06/10/majority-views-nsa-phone-tracking-as-acceptable-anti-terror-tactic/> accessed 10 October 2014.

conducted following the first Snowden leaks,[83] 47% of individuals stated that they were concerned that anti-terrorism policies were excessively restricting civil liberties and 35% stated that they were more concerned that more restrictions would be necessary to adequately protect national security.[84] This is a notable reversal of opinion from previous polls conducted by the Pew Research Center.[85] One possible explanation for the shift in opinion may be the reportage detailing the generalised nature of the surveillance programmes. Privacy has the tendency to be viewed as an intangible right until it affects the individual personally and the Snowden revelations served as a stark reminder that the average citizen is not immune from government surveillance.

This logic may also explain the heightened outrage of international leaders when they discovered that their communications had also been subjected to surveillance.[86] Senator Dianne Feinstein provides another interesting example of how personal exposure to surveillance can alter our understanding of privacy. Following the Snowden revelations, Feinstein – a staunch defender of the intelligence agencies – contended that information was only collected on 'bad guys.'[87] Her opinion changed somewhat when she discovered that the computers of Senate staffers had been under scrutiny.[88] Accordingly, in addition to drawing

[83]Telephone interviews were conducted on 1480 adults living across all 50 US states and the District of Columbia in the summer of 2013. ——, 'Majority Views NSA Phone Tracking as Acceptable Anti-terror Tactic' *Pew Research Center* (10 June 2013) <www.people-press.org/2013/06/10/majority-views-nsa-phone-tracking-as-acceptable-anti-terror-tactic/> accessed 10 October 2014; G Greenwald, 'Major Opinion Shifts, in the US and Congress, on NSA Surveillance and Privacy' *The Guardian* (London 29 July 2013) <www.theguardian.com/commentisfree/2013/jul/29/poll-nsa-surveillance-privacy-pew> accessed 10 October 2014.

[84]——, 'Few See Adequate Limits on NSA Surveillance Program' *Pew Research Center* (26 July 2013) <http://www.people-press.org/2013/07/26/few-see-adequate-limits-on-nsa-surveillance-program/> accessed 10 October 2014; See G Greenwald, 'Major Opinion Shifts, in the US and Congress, on NSA Surveillance and Privacy' *The Guardian* (London 29 July 2013) <www.theguardian.com/commentisfree/2013/jul/29/poll-nsa-surveillance-privacy-pew> accessed 10 October 2014.

[85]As recently as 2010, 47% of those polled said that they were more concerned that government policies 'have not gone far enough to adequately protect the country,' while 32% said that they were more concerned that 'they have gone too far in restricting the average person's civil liberties.' C Doherty, 'Balancing Act: National Security and Civil Liberties in Post-9/11 Era' *Pew Research Center* (7 June 2013) <www.pewresearch.org/fact-tank/2013/06/07/balancing-act-national-security-and-civil-liberties-in-post-911-era/> accessed 10 October 2014; ——, 'Few See Adequate Limits on NSA Surveillance Program' *Pew Research Center* (26 July 2013) <http://www.people-press.org/2013/07/26/few-see-adequate-limits-on-nsa-surveillance-program/> accessed 10 October 2014.

[86]I Traynor and P Lewis, 'Merkel compared NSA to Stasi in heated encounter with Obama' *The Guardian* (London 17 December 2013) <www.theguardian.com/world/2013/dec/17/merkel-compares-nsa-stasi-obama> accessed 10 October 2014; J Borger, 'Brazilian President: US Surveillance a "Breach of International Law"' *The Guardian* (London 24 September 2013) <www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance> accessed 10 October 2014; J Wolverton, 'World Leaders React to NSA Surveillance of Their Phone Calls' *The New American* (25 October 2013) <www.thenewamerican.com/usnews/foreign-policy/item/16808-world-leaders-react-to-nsa-surveillance-of-their-phone-calls> accessed 10 October 2014; M Pengelly, 'NSA Listed Merkel Among Leaders Subject to Surveillance – Report' *The Guardian* (London 29 March 2014) <www.theguardian.com/world/2014/mar/29/nsa-merkel-leaders-surveillance-documents-snowden> accessed 10 October 2014.

[87]T Mak and B Everett, 'Dianne Feinstein on NSA: "It's Called Protecting America"' *Politico* (Washington, 6 June 2013) <www.politico.com/story/2013/06/dianne-feinstein-on-nsa-its-called-protecting-america-92340.html> accessed 10 October 2014.

[88]Feinstein is the Chairman of the US Senate Select Committee on Intelligence; M Masnick, 'Senator Feinstein Finally Finds Surveillance To Get Angry About: When It Happened To Her Staffers' *Tech Dirt* (San Francisco 11 March 2014) <https://www.techdirt.com/articles/20140311/07212926527/

attention to current surveillance practices, the Snowden revelations increased public awareness of privacy issues. Just as there had been calls for investigation and open evaluation following the Watergate leaks, there were calls for reform in the wake of the Snowden revelations. By shining light on the covert practices of the NSA, Snowden empowered the public to express whether or not they were satisfied with the – previously secret – status quo.

Legal responses to the Snowden revelations

Following the Watergate scandal, the Church Committee was formed to investigate the surveillance activities of intelligence agencies. Several reforms were introduced following the Church Report, with FISA being the most significant legislative change. The first Snowden leak was published in the summer of 2013 and documents continue to be reviewed and reported on by journalists, such as Glenn Greenwald, who have been entrusted with copies of the NSA files.[89] While President Obama may claim that he had called for a review of US surveillance operations prior to the Snowden revelations, it is undeniable that the Snowden leaks have given significant momentum to surveillance reform.[90] Despite much discussion of reform in the USA, the tangible results have been underwhelming thus far.

In August 2013, President Obama appointed a Review Group on Intelligence and Communications Technologies to assess the surveillance regime in advance of reform proposals.[91] The review group published a report in December 2013 and recommended several reforms of the current system.[92] In January 2014, President Obama addressed some of

senator-feinstein-finally-finds-surveillance-to-get-angry-about-when-it-happened-to-her-staffers.shtml> accessed 10 October 2014; A Napolitano, 'Freedom for me, but not for thee – Dianne Feinstein, the CIA and you' *Fox News* (New York 20 March 2014) <www.foxnews.com/opinion/2014/03/20/freedom-for-me-but-not-for-thee-dianne-feinstein-cia-and/> accessed 10 October 2014. On learning that the CIA had Searched the Computers of Senate offices without authorisation, Feinstein expressed 'grave concerns.' G Miller, E O'Keefe and A Goldman, 'Feinstein: CIA Searched Intelligence Committee Computers' *Washington Post* (Washington 11 March 2014) <www.washingtonpost.com/world/national-security/feinstein-cia-searched-intelligence-committee-computers/2014/03/11/982cbc2c-a923-11e3-8599-ce7295b6851c_story.html> accessed 10 October 2014; H Abdullah, 'Feinstein says CIA Spied on Senate Computers' *CNN* (Atlanta, USA 12 March 2014) <edition.cnn.com/2014/03/11/politics/senate-cia/index.html?iref=allsearch> accessed 10 October 2014.

[89]The first article covered the NSA collection of Verizon phone records. G Greenwald, 'NSA Collecting Phone Records of Millions of Verizon Customers Daily' *The Guardian* (London 6 June 2013) <www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order> accessed 10 October 2014; T Kludt, 'Greenwald Says "There's A Lot More Coming", Argues NSA Revelations Don't Harm Security' *Talking Points Memo* (Washington 15 July 2014) <talkingpointsmemo.com/livewire/mccain-boston-bombings-prove-sen-rand-paul-wrong-on-terror> accessed 10 October 2014.

[90]Office of the Press Secretary, 'Remarks by the President in a Press Conference' *White House* (9 August 2013) <www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference> accessed 10 October 2014.

[91]A Peterson, 'Obama's "Outside Experts" for NSA Review Are Former Intel and White House Staffers' *Washington Post* (Washington 22 August 2013) <www.washingtonpost.com/blogs/the-switch/wp/2013/08/22/obamas-outside-experts-for-nsa-review-are-former-intel-and-white-house-staffers/> accessed 10 October 2014.

[92]Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, 'Liberty and Security in a Changing World' 12 December 2013 <apps.washingtonpost.com/g/page/world/nsa-review-boards-report/674/> accessed 10 October 2014. Additional – more critical – review was carried out by the Privacy and Civil Liberties Oversight Board (PCLOB). In January 2014 the PCLOB reported that the s.215 bulk collection of telephone records program 'lacks a viable legal foundation under s.215, implicates constitutional concerns

the concerns raised in the report and stated that he would work with Congress to pursue appropriate reforms to the bulk metadata collection programme under s.215 of the PATRIOT Act.[93] In February, changes were made by the Foreign Intelligence Surveillance Court on the request of the administration.[94] Since the Snowden revelations, legislative reform efforts have been numerous, but the USA Freedom Act has emerged as the most viable proposal.[95] While the USA Freedom Act has been 'watered down' from its original incarnation introduced in October 2013,[96] it was passed by the US House of Representatives in May 2014.[97] In order to become law, the USA Freedom Act must be approved by the Senate and must be signed by the President.[98]

While US reform efforts remain in flux it is interesting to note the global repercussions of the Snowden revelations. Initially, the global impact was dominated by the privacy of

---

under the First and Fourth Amendments, raises serious threats to privacy and civil liberties as a policy matter, and has shown only limited value.' Privacy and Civil Liberties Oversight Board, 'Report on the Telephone Records Program Conducted under s.215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court' 23 January 2014, 16 <www.pclob.gov/All Documents/Report on the Telephone Records Program/PCLOB-Report-on-the-Telephone-Records-Program.pdf> accessed 10 October 2014. The PCLOB recommended that the government end the bulk collection of telephone records programme. This recommendation was rejected by the Obama administration. According to the White House Press Secretary administration officials 'simply disagree with the board's analysis on the legality of the program.' J Hattem, 'Holder dismisses NSA Report' *The Hill* (21 January 2014) <thehill.com/policy/technology/196313-holder-dismisses-nsa-report> accessed 10 October 2014. In July 2014, the PCLOB released a second report which found that the s.702 programme – concerned with the collection of foreign digital information – was 'legal and effective' in protecting national security. Privacy and Civil Liberties Oversight Board, 'Report on the Surveillance Program Operated Pursuant to s.702 of the Foreign Intelligence Surveillance Act' 2 July 2014, 161 <www.pclob.gov/All Documents/Report on the Section 702 Program/PCLOB-Section-702-Report-PRE-RELEASE.pdf> accessed 10 October 2014.

[93]Office of the Press Secretary, 'Remarks by the President on Review of Signals Intelligence' *The White House* (17 January 2014) <www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence> accessed 10 October 2014.

[94]——, 'FISC Approves Government's Request to Modify Telephony Metadata Program' *Office of the Director of National Intelligence* (6 February 2014) <www.dni.gov/index.php/newsroom/press-releases/198-press-releases-2014/1013-foreign-intelligence-surveillance-court-approves-government-s-request-to-modify-telephony-metadata-program> accessed 10 October 2014.

[95]S Davies, 'A Crisis of Accountability' *The Privacy Surgeon* (June 2014) 72 <https://cippic.ca/uploads/Snowden_at_one_year-global_survey.pdf> accessed 10 October 2014.

[96]——, 'Leahy & Sensenbrenner Join To Introduce USA FREEDOM Act' *Jim Sensenbrenner* (Press Release 29 October 2013) <sensenbrenner.house.gov/news/documentsingle.aspx?DocumentID=356911> accessed 10 October 2014; D Kravets, 'NSA reform falters as House passes gutted USA Freedom Act' *Ars Technica* (22 May 2014) <atarstechnica.com/tech-policy/2014/05/nsa-reform-falters-as-house-passes-gutted-usa-freedom-act/> accessed 10 October 2014; E Swarztrauber, 'Privacy Advocates tell Congress: Fix Watered-down USA Freedom Act!' *Tech Freedom* (19 June 2014) <techfreedom.org/post/89310684884/privacy-advocates-tell-congress-fix-watered-down-usa> accessed 10 October 2014; T Eddlem, 'USA Freedom Act Gutted Before House Passage; Heads to Senate' *New American* (26 May 2014) <www.thenewamerican.com/usnews/constitution/item/18340-usa-freedom-act-gutted-before-house-passage-heads-to-senate> accessed 10 October 2014.

[97]D Roberts and K McVeigh, 'NSA Surveillance Reform Bill Passes House by 303 Votes to 121' *The Guardian* (London 22 May 2014) <www.theguardian.com/world/2014/may/22/nsa-reform-bill-usa-freedom-act-passes-house> accessed 10 October 2014.

[98]J Eggerton, 'USA Freedom Act Gets Tough Reception in Senate' *Broadcasting & Cable* (Washington 6 June 2014) <www.broadcastingcable.com/news/washington/usa-freedom-act-gets-tough-reception-senate/131607> accessed 10 October 2014; A Byers, 'Hill Surveillance Reform: Time Is Not Its Side' *Politico* (Washington 17 July 2014) <www.politico.com/story/2014/07/hill-surveillance-reform-time-109015.html> accessed 10 October 2014.

Heads of States[99] and the sanctity of trade talks.[100] As the revelations continued, it became clear that the NSA – and by extensions its Five Eyes partners – had far greater access to the world's communications than previously surmised.[101] While the initial outrage and debate in many European states has not been followed by successful legislative reform,[102] the Snowden revelations continue to cause ripples at the European Union level. In the wake of the revelations, the EU Commissioner for Home Affairs, Cecilia Malmstrom, threatened to suspend USA access to European financial and travel data if the USA failed to show that the USA respected EU data protection rules.[103] In addition to launching an inquiry into the Snowden revelations,[104] the Parliament of the EU has had Snowden address the Parliament through video conference technology.[105] Other developments at the EU level – discussed below – cannot be so unambiguously traced to the Snowden revelations. In spite of a more indirect relationship between these recent developments and the disclosures, it seems clear that the privacy-conscious environment that Snowden helped to create is hospitable to the strengthening of privacy and data protection in the EU.

[99]S Romero and R Archibold, 'Brazil Angered Over Report N.S.A. Spied on President' *New York Times* (New York 2 September 2013) <www.nytimes.com/2013/09/03/world/americas/brazil-angered-over-report-nsa-spied-on-president.html?_r=0> accessed 10 October 2014; J Borger and others, 'G20 Summits: Russia and Turkey React with Fury to Spying Revelations' *The Guardian* (London 17 June 2013) <www.theguardian.com/world/2013/jun/17/turkey-russia-g20-spying-gchq> accessed 10 October 2014; ——, '"No Longer in the Cold War": Merkel Infuriated by US Spying' *Der Spiegel* (Hamburg 1 July 2013) <www.spiegel.de/international/world/merkel-furious-at-us-spying-and-eu-to-check-offices-for-bugs-a-908859.html> accessed 10 October 2014.

[100]I Traynor, L Osborne and J Doward, 'Key US-EU Trade Pact under Threat after More NSA Spying Allegations' *The Guardian* (London 30 June 2013) <www.theguardian.com/world/2013/jun/30/nsa-spying-europe-claims-us-eu-trade> accessed 10 October 2014.

[101]P Hamilos, 'Spain Summons US Ambassador over Claim NSA Tracked 60 m Calls a Month' *The Guardian* (London 28 October 2013) <www.theguardian.com/world/2013/oct/28/spain-summons-us-ambassador-nsa-calls> accessed 10 October 2014; G Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State* (Metropolitan Books, 2014) 118–119; G Corera, 'Spying Scandal: Will the "Five Eyes" Club Open up?' *BBC* (London 29 October 2013) <www.bbc.com/news/world-europe-24715168> accessed 10 October 2014; N Hopkins and J Borger 'Exclusive: NSA Pays £100 m in Secret Funding for GCHQ' *The Guardian* (London 1 August 2013) <www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden> accessed 10 October 2014.

[102]C Kerry, 'Missed Connections: Talking With Europe About Data, Privacy, And Surveillance' *Center for Technology Innovation at Brookings* (May 2014) <www.brookings.edu/~/media/research/files/papers/2014/05/20%20europe%20privacy%20surveillance%20kerry/kerry_europefreetradeprivacy.pdf> accessed 10 October 2014; M Holland, 'Europe's Reaction to the Snowden Revelations: Indifference, Resignation and Complete Bewilderment' *C't* (26 February 2014) <www.heise.de/ct/artikel/Europe-s-reaction-to-the-Snowden-revelations-Indifference-resignation-and-complete-bewilderment-2118252.html> accessed 10 October 2014.

[103]A Croft, 'EU Threatens to Suspend Data-sharing with US over Spying Reports' *Reuters* (5 July 2013) <www.reuters.com/article/2013/07/05/usa-security-eu-idUSL5N0FB1YY20130705> accessed 10 October 2014.

[104]Committee on Civil Liberties, Justice and Home Affairs, 'Report on the US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs(2013/2188(INI))' (21 February 2014) <www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A7-2014-0139&language=EN> accessed 10 October 2014.

[105]G Schmitz, 'European Parliament: Snowden Will Make Video Appearance' *Der Spiegel* (Hamburg 12 December 2013) <www.spiegel.de/international/world/edward-snowden-to-make-video-appearance-to-european-parliament-a-938725.html> accessed 10 October 2014.

One area of the law that has received increased attention in the aftermath of the Snowden revelations is data protection. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention No. 108) was initially developed by the Council of Europe in 1981 in response to significant developments in information and communications technology.[106] In an effort to bring about harmonisation of data protection regulation within the internal market, the European Community adopted Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data in 1995.[107] The status of the right to data protection as a fundamental right in Europe has been significantly enhanced with the entry into force of the Lisbon Treaty and the now binding nature of Article 8 of the EU Charter of Fundamental Rights (EU Charter).[108]

With the exponential growth in online communications, the manner in which the associated user data is protected has become increasingly important. A vast amount of both traffic and content communications data is stored by private companies, such as Microsoft and Google, and the ability to access this data is clearly valued by the investigative arm of government. Due to the belief that current data protection law is out of date, reforms of the law have been proposed for several years.[109] While the reform process had appeared stalled, fresh impetus for reform was created following the Snowden revelations.[110] The former EU Commissioner for Justice and Fundamental rights, Vivien Reding has frequently

[106]Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108) (Strasbourg, 28.I.1981); Council of Europe, Explanatory Report to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108). <http://conventions.coe.int/Treaty/EN/Reports/Html/108.htm> accessed 10 October 2014; P Hustinx, 'Data Protection in the European Union' [2005] *Privacy & Informatie* 62; N Purtova, 'Private law solutions in European data protection: Relationship to privacy, and waiver of data protection rights' (2010) 28 NQHR 179.

[107]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 [1995] OJ L281.

[108]In addition to the Charter recognition of the right, an explicit legal basis for the right to the protection of personal data is now contained in Article 16 of the Treaty on the Functioning of the European Union. These developments place the right to data protection at the same level as the EU Treaties.

[109]Commission Proposal for a Comprehensive Approach on Personal Data protection in the European Union, COM (2010), 609/3 (11 November 2010) <http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf> accessed 10 October 2014; H Crowther, 'The Draft Data Protection Regulation: Can We Start Counting our Chickens?' (2014) 14 P & DP 7, 7; ——, 'Reding Rallies Troops to Power Forward with Reform' (2014) 14 Privacy & Data Protection 1, 1; J Leyden, 'Call for Reform as UK Data Protection Rules Turn 10' *The Register* (16 July 2008) <www.theregister.co.uk/2008/07/16/dpa_10/> accessed 10 October 2014; L Danagher, 'An Assessment of the Draft Data protection Regulation: Does it Effectively Protect Data?' (2012) 3 EJLT; ——, 'Privacy Reforms on the Horizon: A Primer on Pending EU and US Privacy Proposals' *O'Melveny and Myers LLP* (16 December 2010) <www.omm.com/a-primer-on-pending-eu-and-us-privacy-proposals-12-16-2010/> accessed 10 October 2014.

[110]S Shuster, 'EU Pushes for Stricter Data Protection After Snowden's NSA Revelations' *Time* (New York 21 October 2013) <world.time.com/2013/10/21/e-u-pushes-for-stricter-data-protection-after-snowden-nsa-revelations/> accessed 10 October 2014; Q Peel and J Fontanella-Khan, 'Angela Merkel Calls for EU-wide Agreement on Data Protection' *Financial Times* (London 14 July 2013) <www.ft.com/cms/s/0/7a4b26d8-eca6-11e2-a0a4-00144feabdc0.html'axzz36VlC7aS5> accessed 10 October 2014; ——, 'EU: Reding Says Reforms Vital to Counter PRISM Data Access' *Data Guidance* (13 June 2013) <www.dataguidance.com/dataguidance_privacy_this_week.asp?id=2046> accessed 10 October 2014.

referenced the Snowden revelations when endorsing data protection reform.[111] An example of this is found in her assertion that US companies, such as Facebook and Google, should also be subjected to European data protection law and her statement that European ministers must 'give a positive answer to Snowden's wake-up call.'[112] While the reform efforts have not been unhindered,[113] Vivien Reding has asserted that 'the data protection reform is on track – it is on the right track.'[114]

In spite of the importance the EU places on data privacy and data protection, the EU has also introduced legislative measures that have been criticised as detrimental to privacy.[115] The Data Retention Directive mandates that member states must retain all telecommunications traffic data for between six months and two years.[116] In April 2014, the Court of Justice of the European Union (CJEU) found the directive to be in breach of the EU

[111]——, 'EU: Reding Says Reforms Vital to Counter PRISM Data Access' *Data Guidance* (13 June 2013) <www.dataguidance.com/dataguidance_privacy_this_week.asp?id=2046> accessed 10 October 2014; ——, '"Thank You Mr Snowden", Says EU's Reding' *Luxemburger Wort* (Luxembourg 20 September 2013) <www.wort.lu/en/international/thank-you-mr-snowden-says-eu-s-reding-523bdfa4e4b0c159be9abbba> accessed 10 October 2014; A Napolitano, 'An Accidental Ally For the European Union: "Thank You, Mr. Snowden" Says European Commission VP Reding in Hangout Debate' *Tech President* (9 January 2014) <techpresident.com/news/wegov/24653/accidental-ally-european-union-'thank-you-mr-snowden'-says-european-commission-vp-reding> accessed 10 October 2014; K Fiveash, 'EU Ministers Respond Sleepily to Viv Reding's "Snowden Wake-up Call" on Data Protection' *The Register* (9 June 2014) <www.theregister.co.uk/2014/06/09/viv_reding_justice_council_of_ministers_data_protection/> accessed 10 October 2014.

[112]J Fioretti, 'EU Says Firms like Google and Facebook must Meet Privacy Rules' *Reuters* (6 June 2014) <uk.reuters.com/article/2014/06/06/us-eu-dataprotection-idUKKBN0EH1ER20140606> accessed 10 October 2014.

[113]J Burn-Murdoch, 'Europe Deadlocked over Data Protection Reform' *The Guardian* (London 12 August 2013) <www.theguardian.com/news/datablog/2013/aug/12/europe-data-protection-directive-eu> accessed 10 October 2014.

[114]In an important sign of progress in May, the Council agreed its position concerning the application of the new data protection rules to countries outside the EU. At this stage, the Council must still agree its position on the full text. Once the Council has adopted its position it can then negotiate with the European Parliament, which adopted its position on the full text in March. Council of the European Union, 'Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data protection Regulation)–Partial General Approach on Chapter V' (28 May 2014) <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2010349%202014%20INIT> accessed 10 October 2014; Council of Europe, 'Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data protection Regulation)-Outcome of the European Parliament's first reading' (27 March 2014) <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN&ring=A7-2013-0402> accessed 10 October 2014; M Cross, 'New European data protection law "on track"' Law Society Gazette (1 July 2014) <www.lawgazette.co.uk/law/new-european-data-protection-law-on-track/5041971.article> accessed 10 October 2014; S Peers, 'Reforming EU Data Protection Law: the Council Takes Its First Baby Steps' *EU Law Analysis* (13 June 2014) <eulawanalysis.blogspot.ie/2014/06/reforming-eu-data-protection-law.html> accessed 10 October 2014.

[115]V Shannon, 'Data Retention: Europe's Plan to Track Phone and Net Use' *Der Spiegel* (Hamburg 20 February 2007) <www.spiegel.de/international/data-retention-europe-s-plan-to-track-phone-and-net-use-a-467475.html> accessed 10 October 2014.

[116]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 [2006] OJ L-105/54.

Charter.[117] While the Advocate General had previously opined that the Directive was incompatible with the EU Charter,[118] the strength of the language in the decision reached by the Court of Justice was unexpected. The Court pointed out that the Directive had general application and required the collection of data on 'all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made.'[119] Accordingly, the Court found the directive to be disproportionate. This decision represents a clear statement of intent on behalf of the Court of Justice, particularly in the light of it being the first major European ruling on surveillance following the Snowden revelations.[120]

In what could be interpreted as a thinly veiled reference to the Snowden revelations, the Court stated that

> the directive does not require that the data be retained within the EU. Therefore, the directive does not fully ensure the control of compliance with the requirements of protection and security by an independent authority, as is, however, explicitly required by the Charter. 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.[121]

The implication of this statement appears to be that legal systems outside the EU cannot be trusted to provide adequate protection of personal data. This statement has significant implications for multinationals that move information between the EU and other states. The Snowden revelations revealed how the NSA has the capability to access user information held by US technology companies through programmes such as PRISM and it is likely that this fact influenced the strong position taken by the Court of Justice on the matter.[122]

The landmark ruling on data retention in April was followed by another important privacy decision by the Court of Justice in May in *Google Spain SL Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González*.[123] The

[117]Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] WLR (D) 164.
[118]AG Opinion in Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2013] EUECJ C-293/12.
[119]Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] WLR (D) 164 [57].
[120]T McIntyre, 'Surveillance Judgment Is a Victory for Democracy' *Irish Independent* (Dublin 10 April 2014) <www.independent.ie/opinion/analysis/surveillance-judgment-is-a-victory-for-democracy-30172786.html> accessed 10 October 2014.
[121]Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] WLR (D) 164 [68].
[122]Under the PRISM programme, the NSA compels electronic communications service providers to provide the communications connected to certain 'selectors' related to non-US persons, such as email addresses. Privacy and Civil Liberties Oversight Board, 'Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act' 2 July 2014, 7 <http://www.wired.com/wp-content/uploads/2014/07/PCLOB-Section-702-Report-PRE-RELEASE.pdf> accessed 10 October 2014.
[123]The facts of the case involved a Spanish national who had previously sold his house to pay off social security debts. When his name was searched on Google, the search results included links to two newspaper articles from 1998 discussing these issues. The Spanish national believed that his name should no longer be associated with these prejudicial articles as he had since cleared his debts. Case C-131/12 *Google Spain SL Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] EUECJ C-131/12.

Court of Justice found that a Spanish national was entitled to have 'irrelevant' Google search results associated with his name removed. The Court of Justice relied on the 1995 Data Protection Directive in addition to the rights to privacy and protection of personal data as guaranteed by the EU Charter.[124] Unsurprisingly, Google and other online businesses have expressed dismay at the decision.[125] In its ruling, the Court of Justice makes it clear that the individual right to privacy occupies a privileged position over the business interests of private companies.[126] While the Court also privileged the rights to privacy and data protection above the access to information interests of internet users, the Court clarified that the balance would depend on the nature of the information in question and on the interest of the public in having that information.[127]

The fact that this 'right to be forgotten' ruling was delivered in the context of a significant resurgence of public interest in privacy rights globally cannot be ignored. While the Snowden revelations would not appear to have a direct relationship with the 'right to be forgotten,' the leaks have led to the increased prominence of privacy issues in the public debate. The general public is becoming increasingly conscious of the risks associated with data collection generally and as a result conditions are favourable for enhancing the protection of privacy across all sectors of society. This view is shared by other commentators, including Paul Bernal who remarks that, '[p]rivacy is becoming bigger and bigger news – and I have a strong feeling that the Snowden revelations influenced the thinking of the ECJ in last week's ruling, subconsciously if nothing else.'[128] Henry Farrell opines that while the decision of the Court of Justice is not directly connected to the Snowden revelations, the controversy may have empowered the Court to push for a more direct EU role in privacy.[129]

The Snowden revelations and the subsequent developments in EU case law have not been unnoticed at the domestic level. In June, the Irish High Court candidly discussed the impact the Snowden revelations have had on global privacy in *Schrems v Data*

[124]Following this ruling, if a European Union citizen believes that the search results delivered on the basis of his or her name are inaccurate, irrelevant, excessive, or out of date, he or she can request that the search engine erase those results. The search engine must conduct a balancing analysis to determine whether the search results comply with the principles of Data protection. If the search engine refuses to erase the offending search results, the individual is entitled to approach the relevant national authority who – if Data protection law requires – could compel the search engine to remove the search results in question.

[125]D Hakim, 'Right to Be Forgotten? Not That Easy' *New York Times* (New York 29 May 2014) <www.nytimes.com/2014/05/30/business/international/on-the-internet-the-right-to-forget-vs-the-right-to-know.html?_r=0> accessed 10 October 2014; N Hirst, 'Outcry over Right to Be Forgotten' *European Voice* (15 May 2014) <www.europeanvoice.com/article/n-business3-nh/> accessed 10 October 2014; N Lomas, 'Jimmy Wales Blasts Europe's "Right To Be Forgotten" Ruling as a "Terrible Danger"' *Tech Crunch* (7 June 2014) <techcrunch.com/2014/06/07/wales-on-right-to-be-forgotten/> accessed 10 October 2014.

[126]Case C-131/12 *Google Spain SL Google Inc v Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014] EUECJ C-131/12 [81].

[127]Ibid.

[128]P Bernal, 'A Week Not to Be Forgotten … .' *Paul Bernal's Blog* (19 May 2014) <https://paulbernal.wordpress.com/category/right-to-be-forgotten/> accessed 10 October 2014. The Snowden revelations have increased attention on data privacy issues in Europe. J Fioretti, 'Google Removes First Search Results after EU Ruling' *Reuters* (26 June 2014) <reuters.com/article/2014/06/26/google-searches-eu-idUKL6N0P749T20140626> accessed 10 October 2014.

[129]H Farrell, 'Five Key Questions about the European Court of Justice's Google Decision' *Washington Post* (Washington 14 May 2014) <www.washingtonpost.com/blogs/monkey-cage/wp/2014/05/14/five-key-questions-about-the-european-court-of-justices-google-decision/> accessed 10 October 2014.

Protection Commissioner.[130] While considering a case against the Irish Data Protection Commissioner for refusing to investigate Facebook, the High Court referred an essential question of privacy law to the CJEU.[131] The judgment of the High Court discussed the Snowden revelations in detail and considered how the exposure of PRISM and the language used by the Court of Justice in the *Digital Rights Ireland v Minister for Communications* decision may have significantly altered the legal position.[132] The decision of the High Court cast doubt on the legality of the current 'Safe Harbour' rules that govern the transfer of information between the EU and the USA. While a European Commission Decision issued in 2000 recognises Safe Harbour as providing adequate protection for personal data, the Irish High Court pointed out that the recent Snowden revelations have raised serious questions about the effectiveness of the system.[133] In addition, the High Court drew attention to the fact that since the sanctioning of the Safe Harbour regime by the Commission in 2000, Europe has seen the entry into force of the Lisbon Treaty which made the EU Charter legally binding.[134] In reference to the findings of the Court of Justice in the *Digital Rights Ireland* decision,[135] the High Court stated that 'it is not immediately apparent how the present operation of the Safe Harbour regime can in practice satisfy the requirements of Article 8(1) and Article 8(3) of the Charter.'[136] While the High Court judgment explicitly recognised the abuses carried out by the US security authorities, it also acknowledged that the US Foreign Intelligence Surveillance Court provides some judicial oversight.[137] An underlying message of the *Digital Rights Ireland* decision[138] seems to be echoed in the assertion by the Irish High Court that considerable legal difficulties are posed by 'the very fact that this oversight is not carried out on European soil.'[139]

In the light of this judgment from the Irish Court, and the recent judgments emerging from the Court of Justice, this is clearly a crucial moment for data protection and privacy in Europe. In spite of the absence of tangible legislative reform, the influence of the Snowden revelations is difficult to deny and privacy advocates are emboldened. While problems with the safe harbour regime had previously been acknowledged, the heightened concern with the system illustrates how the Snowden revelations have increased momentum. The renewed focus on privacy issues at the EU level appears to have been

[130] *Schrems v Data Protection Commissioner* [2014] IEHC 310.The case concerns the ongoing attempt by Max Schrems to force the Data Protection Commissioner to investigate Facebook's involvement with the PRISM programme through Facebook's transferring of personal data from Facebook-Ireland to Facebook Headquarters in the US.

[131] Mr Justice Hogan referred a question to the CJEU, asking whether an office holder enforcing data protection legislation (such as a Data Protection Commissioner) is bound by the Commission Decision which found the Safe Harbour regime to be adequate, or whether the office holder may conduct his or her own investigation of the matter taking into account the factual developments that have occurred following the original publication of the Commission Decision in 2000. *Schrems v Data Protection Commissioner* [2014] IEHC 310 [71].

[132] *Schrems v Data Protection Commissioner* [2014] IEHC 310 [10]-[18], [62]. Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] WLR(D) 164 (discussed above).

[133] *Schrems v Data Protection Commissioner* [2014] IEHC 310 [69]-[71].

[134] The EU Charter explicitly recognises both the right to respect for private life and the right to protection of personal data. *Schrems v Data Protection Commissioner* [2014] IEHC 310 [63].

[135] Joined Cases C-293/12 & C-594/12 *Digital Rights Ireland and Seitlinger and Others* [2014] WLR (D) 164 [57] (discussed above).

[136] *Schrems v Data Protection Commissioner* [2014] IEHC 310 [62].

[137] *Schrems v Data Protection Commissioner* [2014] IEHC 310 [14].

[138] Discussed above.

[139] *Schrems v Data Protection Commissioner* [2014] IEHC 310 [62].

driven by the transparency Snowden forced on the intelligence agencies. As a result of this transparency, Europe is re-evaluating how it protects its data.

Transparency

Shortly after Snowden revealed himself as the source of the NSA documents, the concept of the 'Snowden effect' was being discussed.[140] This term captures how the transparency that Snowden imposed on the intelligence agencies has sparked a public debate. Secrecy has been described as 'the boon companion of arbitrariness' and transparency has been called the 'cornerstone' of good governance with an important role to play in reducing abuse and enhancing public confidence.[141] It remains the case, however, that some degree of secrecy is an essential feature of any surveillance system. Inevitably, such operational necessity can result in an information deficit. In a properly functioning democracy, the public should have general awareness of its government's surveillance practices. According to Beetham, the basic principle of democracy is that,

> the people have a right to a controlling influence over the public decisions and decision-makers, and that they should be treated with equal respect and as of equal worth in the context of such decisions. These could be called for short the principles of popular control and political equality, respectively. [142]

Transparency is essential if the public is to make an informed decision on whether they are satisfied with their government. In a representative democracy, the public needs information if they are to campaign or vote for change. Transparency provides the citizen with more opportunity to decide what degree of interference they perceive to be acceptable and thereby empowers the citizen to demand change.

The revelations of the Church Committee demonstrated how 'assumptions of everlasting secrecy facilitated the abuses by the executive branch.'[143] The lack of clear comment from either the NSA or the President on the nature or extent of the programme following the exposure of the warrantless wiretapping scandal in 2005 provides another example of the secrecy that inhibits effective protection of the privacy rights.[144] The change of heart experienced by the Chairman of the Senate Intelligence Committee, Senator Diane Feinstein, following her learning that Senate computers had been spied on is indicative of the utter failure of oversight in the US system. Subsequent to her initial staunch defence of the intelligence agencies, she admitted that it had become clear to her that 'certain surveillance activities have been in effect for more than a decade and that the Senate Intelligence

[140]R McShane, 'The Snowden Effect' *The Economist* (London 10 August 2013) <www.economist.com/blogs/democracyinamerica/2013/08/american-surveillance> accessed 10 October 2014; K Hill, 'As "X-Keyscore" Revealed, Senators Criticize NSA Hoovering Of Phone Records' *Forbes* (31 July 2013) <www.forbes.com/sites/kashmirhill/2013/07/31/senators-question-nsa-hoovering-of-phone-records/> accessed 10 October 2014.

[141]L Lustgarten and I Leigh, *In from the Cold: National Security and Parliamentary Democracy* (Clarendon Press, 1994) 22; V Mäntysalo, 'The Role of Transparency and Recent Developments in Finland' (EGPA Conference, Bucharest 7–10 September 2011).

[142]D Beetham, 'Democracy: Key Principles, Institutions and Problems' in *Democracy: Its Principles and Achievements* (Inter-Parliamentary Union, 1998) 21.

[143]F Schwarz and A Huq, *Unchecked and Unbalanced: Presidential Power in a Time of Terror* (New Press, 2007) 45.

[144]Jacqueline Klosek, *The War on Privacy* (Praeger, 2007) 39.

Committee was not satisfactorily informed.'[145] The flaws in the system of oversight are great when even the Chairman of the Senate Intelligence Committee – a specially privileged security insider – is in the dark as regards the actions of the intelligence agencies.

Typically, when rights are infringed by the government we seek protection in the courts. There are practical problems in the area of surveillance and privacy that place a heavy burden on the individual. Due to the secret nature of surveillance it is often difficult to identify a particular incident of infringement and an accompanying justiciable harm. As Donner points out,

> the clandestine character of intelligence operations, the difficulty of identifying the source of a claimed abuse, handicaps the pursuit of a judicial remedy. And the ambiguity of the injury suffered by the target, contrasted with the importance of the interest (the security of the nation itself) asserted in defense of the challenged conduct increases a complainant's burdens.[146]

In order to overcome these limitations, an alternative approach must be taken if the powers of the government are to remain in check. Full and informed debate of issues – both the threats and the benefits – is an essential value in a democratic society, as it encourages participation and proportionate decision-making. O' Brien points out that the 'importance of privacy rights in a democratic society demands that the privacy/security tension is fully debated in an open and rational way, devoid insofar as is possible of rhetoric and sensationalism, with an assessment of some of the difficulties.'[147] Scepticism is a vital element in a democratic society and a system of checks and balances can provide a measure of control against excessive exertion of power by the executive branch.[148] Publicity through an open media and transparency of government actions are essential tools of control over government in a democratic society.[149]

While there are legitimate limitations on the type of transparency that is possible in the surveillance context, the publication of surveillance statistics has the potential to offer valuable protection and transparency. Limited publication of statistics reporting the levels and types of surveillance carried out by government authorities occurs in several countries,[150] however, it is clear that the standards and methods by which statistics are compiled vary and much reporting of statistics contains significant gaps.[151] Regardless of this, if the limitations and the processes behind the collection, compilation, and publication of surveillance statistics are transparent, surveillance statistics can be a useful tool for interested parties to keep the actions of their governments under scrutiny year on year.[152] It is submitted that the publication of comprehensive surveillance statistics lessens the impression of impunity

[145]P Lewis and S Ackerman, 'NSA: Dianne Feinstein Breaks Ranks to Oppose US Spying on Allies' *The Guardian* (London 29 October 2013) <www.theguardian.com/world/2013/oct/28/nsa-surveillance-dianne-feinstein-opposed-allies> accessed 10 October 2014.
[146]See F Donner, *The Age of Surveillance* (Vintage Books, 1980) xii.
[147]M O' Brien, 'Law, Privacy and Information Technology: A Sleepwalk Through the Surveillance Society?' (2008) 17 ICTL 25, 35.
[148]G Marx, *Undercover: Police Surveillance in America* (University of California Press, 1989) 775. See discussion in B Barber, *The Logic and Limits of Trust* (Rutgers University Press, 1983).
[149]A Westin, *Privacy and Freedom* (Atheneum, 1967) 24.
[150]Examples include the report of the Parliamentary Control Commission in Germany, the US 'Wiretap Report,' and the Annual Report of the Interception of Communications Commissioner in the UK.
[151]P Schwartz, 'Evaluating Telecommunications Surveillance in Germany: The Lessons of the Max Planck Institute's Study' (2003–2004) 72 Geo Wash L Rev 1244, 1252.
[152]See ——, 'FBI reporting concerning pen register/trap and trace statistics' (2009) <http://epic.org/privacy/wiretap/ltr_pen_trap_leahy_final.pdf> accessed 10 October 2014.

among members of the executive branch and can act as a deterrent to abusive action. Most crucially, statistics keep the public informed and enable the public to participate in the debate and exert control on their government if necessary.

So while statistics have the potential to offer a vital public check, a statistic requirement can also have a fatiguing effect on both the press and the public. In the worst case, statistics can even serve as privacy theatre.[153] This concept, coined by Paul Schwartz, suggests that the existence of statistics can reassure individuals that 'someone' is keeping an eye on things and as a result statistics could deter genuine engagement or vigorous investigation.[154] According to Schwartz, the collection of statistics can create a 'myth of oversight.'[155] In order to ensure that statistics are not inuring the public to the issue of surveillance and are not being manipulated to give a false impression, another line of defence is necessary, and it is submitted that the conscientious insider – who feels free to act as a whistle-blower – can play this crucial role.

Whistle-blowers

Without the work and risks taken by whistle-blowers, the public may have never learned of the contents of the Pentagon Papers, the warrantless wiretapping programme engaged by the Bush administration, the use of waterboarding by the US government,[156] or the NSA programmes exposed by Snowden. While Snowden does not meet the current US legal standard of whistle-blower, he does meet the 'vernacular' standard.[157] In addition to engendering discussion on the appropriate use of surveillance in modern society, Snowden has also sparked a debate on the practice of whistle-blowing in the national security context. In the context of this debate, he has been both 'hailed as a whistle-blower and denounced as a traitor.'[158] Notably, a Quinnipac poll conducted in August 2013 found that the majority of Americans view Snowden as a whistle-blower and not a traitor.[159]

In June 2013, Edward Snowden was charged with espionage and theft of government property.[160] While former President Jimmy Carter has stated that he would consider pardoning Snowden if he was found guilty of these charges, President Obama has made his divergent opinion clear.[161] The reality is that Snowden was fully aware of the risk he took by both

[153]P Schwartz, 'Reviving Telecommunications Surveillance Law' (2008) 75 U Chi L Rev 287, 288.
[154]Ibid.
[155]Ibid.
[156]S Shane, 'Ex-Officer Is First From CIA to Face Prison for a Leak' *New York Times* (New York 5 January 2013), <www.nytimes.com/2013/01/06/us/former-cia-officer-is-the-first-to-face-prison-for-a-classified-leak.html?pagewanted=all&_r=0> accessed 10 October 2014.
[157]L Paquette, 'The Whistleblower as Underdog: What Protection can Human Rights offer in Massive Secret Surveillance?' (2013) 17 IJHR 796, 798; S Vladec, 'The Espionage Act and National Security Whistleblowing After *Garcetti*' (2008) 57 Am ULR 1531, 1533.
[158]J Stratford and T Johnston, 'The Snowden 'revelations': Is GCHQ Breaking the Law?' (2014) EHRLR 129, 129.
[159]____, 'Snowden Is Whistle-Blower, Not Traitor, U.S. Voters Tell Quinnipiac University National Poll' *Quinnipiac University* (1 August 2013) <www.quinnipiac.edu/news-and-events/quinnipiac-university-poll/national/release-detail?ReleaseID=1930> accessed 10 October 2014.
[160] ____, 'US Files Criminal Charges Against NSA Whistleblower Edward Snowden' *The Guardian* (London 22 June 2013) <www.theguardian.com/world/2013/jun/22/us-charging-edward-snowden-with-espionage> accessed 10 October 2014.
[161]S Sullivan, 'Jimmy Carter Says He Would Consider Pardoning Edward Snowden' *Washington Post* (Washington 26 March 2014) www.washingtonpost.com/blogs/post-politics/wp/2014/03/26/jimmy-carter-says-he-would-consider-pardoning-edward-snowden/ accessed 10 October 2014.

exposing the NSA and coming forward publicly in his role as whistle-blower. According to Snowden, he understood that he would be made to suffer for his actions, but he asserts that 'I will be satisfied if the federation of secret law, unequal pardon and irresistible executive powers that rule the world that I love are revealed even for an instant.'[162] Even though Snowden understood that by exposing the NSA his life would 'likely be over,' he asserted that he was 'at peace with that' as it was the 'right thing to do.'[163] This is a remarkable sacrifice to make voluntarily and it would seem imprudent to expect the average conscientious insider to make such damaging personal choices in an effort to protect the public interest.

The acceptance of such personal risk appears even less likely when considered in the context of the aggressive pursuit of whistle-blowers by the US Government in recent times.[164] The Obama administration has frequently used the Espionage Act – primarily designed to prosecute treasonous information sharing with foreign enemies – against several individuals acting as whistle-blowers.[165] 11 individuals in US history have been charged under the Espionage Act for leaking classified information; seven of those prosecutions have occurred under President Obama.[166]

President Obama has argued that Snowden should have taken a different – less public – approach,[167] and has called for him to return to the USA and go to court to 'make his case' that 'what he did is right.'[168] The flaw in this argument is that, under the Espionage Act, acting in the public interest is not a defence.[169] Indeed, the Espionage Act does not distinguish between an individual acting as a whistle-blower or as a spy. In addition, the law does not provide the opportunity to argue that the leaked information should never

[162]G Greenwald, E MacAskill, and L Poitras, 'Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations' *The Guardian* (London 10 June 2013) <http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance> accessed 10 October 2014.

[163]G Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State* (Metropolitan Books, 2014) 18.

[164]S Shane, 'US Pressing Its Crackdown Against Leaks' *New York Times* (New York 17 June 2011) <http://www.nytimes.com/2011/06/18/us/politics/18leak.html?pagewanted=all&_r=0> accessed 10 October 2014; J Kiriakou, 'Obama's Abuse of the Espionage Act Is Modern-day McCarthyism' *The Guardian* (London 6 August 2013) <www.theguardian.com/commentisfree/2013/aug/06/obama-abuse-espionage-act-mccarthyism> accessed 10 October 2014.

[165]R Moberly, 'Whistleblowers and the Obama Presidency: The National Security Dilemma' (2012) 16 EREPJ 51, 75–76.

[166]J Kiriakou, 'Obama's Abuse of the Espionage Act Is Modern-day McCarthyism' *The Guardian* (London 6 August 2013) <www.theguardian.com/commentisfree/2013/aug/06/obama-abuse-espionage-act-mccarthyism> accessed 10 October 2014.

[167]Office of the Press Secretary, 'Remarks by the President on Review of Signals Intelligence' *The White House* (17 January 2014) <www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence> accessed 10 October 2014.

[168]Office of the Press Secretary, 'Remarks by the President in a Press Conference' *White House* (9 August 2013) <www.whitehouse.gov/the-press-office/2013/08/09/remarks-president-press-conference> accessed 10 October 2014.

[169]This is in spite of the fact that the lack of a public interest defence may render the statute unconstitutional. H Edgar and B Schmidt, 'The Espionage Statutes and Publication of Defense Information' (1973) 73 Col LR 929. For a discussion of how recent developments may have narrowed the Constitutional protection see S Vladec, 'The Espionage Act and National Security Whistleblowing After *Garcetti*' (2008) 57 Am ULR 1531, 1531. Pentagon Papers whistle-blower, Daniel Ellsberg has criticised calls for Snowden to return and face trial as 'either disingenuous or simply ignorant that current prosecutions under the Espionage Act allow no distinction whatever between a patriotic whistleblower and a spy.' D Ellsberg, 'Daniel Ellsberg: Snowden Would Not Get a Fair Trial – and Kerry is Wrong' *The Guardian* (London 30 May 2014) <www.theguardian.com/commentisfree/2014/may/30/daniel-ellsberg-snowden-fair-trial-kerry-espionage-act> accessed 10 October 2014.

have been withheld from the public.[170] Accordingly, national security whistle-blowers are denied the opportunity to defend their actions as just. In addition, the aggressive approach of the Obama administration means that a national security whistle-blower is likely to be subjected to extremely harmful treatment once arrested. Potential whistle-blowers will be aware of the recent handling of leakers, such as Private Chelsea Manning, who was sentenced to 35 years in prison following treatment in pre-trial detention that has been described as excessive and unfair.[171]

In the light of the strong disincentives to conscientiously disclose information deemed confidential by government agencies, an appropriate legal framework providing adequate protection for whistle-blowers needs to be designed in order to ensure that the government remains in check. The legal framework must contain clear standards addressing when an individual can disclose confidential information.[172] While it might make sense to treat whistle-blowers differently when national security is implicated,[173] the grave implications of unchecked and opaque intelligence agencies mean that some whistle-blower protection is essential. It is contended that a three-step system strikes the appropriate balance between secrecy and transparency in the surveillance context.[174] A three-step system requires a whistle-blower to report the suspected wrongdoing using internal procedures initially. This is important as it favours the internal reporting and correcting of issues and avoids any risk of harming national security or hindering operational effectiveness. If the internal reporting is unsuccessful, the whistle-blower can approach an external party, such as a regulator or an ombudsman. This body must be fully independent of the executive branch of government. If the organisation fails to respond adequately at this stage, the whistle-blower must then have the option to approach the public, most usually through the press.

While internal reporting along a prescribed channel is of course preferable as the standard first step – particularly in the surveillance context – fully internal and closed reporting systems have inherent flaws. This is particularly true where the whistle-blower aims to disclose an 'unlawful secret' that has received approval from those in power.[175] When the illegal secret is endorsed by senior officials, it is highly unlikely that the act of whistle-blowing is likely to effect change. Vladec points out that these are the most important cases to expose.[176] Due to the heightened stakes in the security context, it is prudent to establish a robust second step channel for whistle-blowers. An independent and expert

[170]T McCarthy, 'Snowden Unlikely to "Man up" in Face of Espionage Act, Legal Adviser Says' *The Guardian* (London 28 May 2014) <www.theguardian.com/world/2014/may/28/snowden-return-us-kerry-face-charges-espionage> accessed 10 October 2014.

[171]Ibid; G Greenwald, 'Even a Military Judge Recognizes What Many Progressives Denied: Bradley Manning Was Mistreated' *The Guardian* (London 9 January 2013) <http://www.theguardian.com/commentisfree/2013/jan/09/bradley-manning-wikileaks-mistreated-progressives> accessed 10 October 2014.

[172]L Paquette, 'The Whistleblower as Underdog: What Protection can Human Rights Offer in Massive Secret Surveillance?' (2013) 17 IJHR 796, 802.

[173]R Moberly, 'Whistleblowers and the Obama Presidency: The National Security Dilemma' (2012) 16 EREPJ 51, 116.

[174]For a general discussion of three step whistle-blower protection see, W Vandekerckhove, 'European Whistleblower Protection: Tiers or Tears?' in D Lewis (ed), *A Global Approach to Public Interest Disclosure* (Edward Elgar, 2010) 15–35. Vandekerckhove discusses the three-tiered model of whistle-blower protection in the European context.

[175]S Vladec, 'The Espionage Act and National Security Whistleblowing After *Garcetti*' (2008) 57 Am ULR 1531, 1544.

[176]Ibid 1544.

regulator will be able to exert scrutiny over the complaints, while maintaining a high level of secrecy.

In spite of the importance of providing this second step option, it is contended that protection of whistle-blowers who are compelled to go to the press remains essential. History has demonstrated that the press can provide a vital outlet for the frustrated whistle-blower. Before Daniel Ellsberg went to the press with the Pentagon Papers, he approached legislators in an effort to ignite a debate. After initial enthusiasm from two Senators,[177] both Senators backed out citing the political risk.[178] Following this lack of success, Ellsberg approached the press even though he knew this action could result in his imprisonment for many years.[179] Without building in legal protection for situations where the whistle-blower is compelled to resort to the fourth estate, any legislation is likely to have only symbolic value.[180]

Conclusion

The Snowden disclosures have created an 'international furore and raised concerns from the population far afield from the US.'[181] It has been reported that in spite of a significant amount of global 'activity' – such as parliamentary inquiries, diplomatic representations and media coverage – following the Snowden revelations, an insignificant number of tangible reforms have been introduced.[182] In spite of the erratic response to the revelations across the world, it is clear that the institutions of the EU have been comparatively active in their responses.[183] This article has discussed how the right to privacy and the right to protection of personal data have received increased focus in the wake of the Snowden revelations. Most striking has been the case law of the Court of Justice. The Court of Justice has often played a crucial role in charting the course for the European Union, and cases such as *Digital Rights Ireland* and *Google Spain* indicate that data protection and privacy are to be key issues on the EU agenda in the coming years.

This article opened with the observation that the pendulum metaphor can provide a useful illustration of the manner in which public opinion tends to oscillate between favouring greater security and greater privacy. Triggering events – such as terrorist attacks – can heighten this effect and government policy tends to respond to these

[177]Ellsberg first approached Senator William Fulbright and then approached Senator George McGovern.
[178]A Greenberg, *This Machine Kills Secrets: Julian Assange, the Cypherpunks, and Their Fight to Empower Whistleblowers* (Penguin, 2012) 35.
[179]Ibid.
[180]In addition to requiring a comprehensive legal structure, appropriate technological supports will also be necessary in order to create a system where harmful covert behaviour can be safely and efficiently exposed by genuine insiders. Greenberg argues that 'WikiLeaks' key advancement in the science of spilling information has been in separating the leaker from the leaked information.' The logic behind this argument is that buffering the source of the leak from the confidential information encourages disclosure. A Greenberg, *This Machine Kills Secrets: Julian Assange, the Cypherpunks, and Their Fight to Empower Whistleblowers* (Penguin, 2012) 5–6.
[181]L Paquette, 'The whistleblower as underdog: what protection can human rights offer in massive secret surveillance?' (2013) 17 IJHR 796, 798.
[182]S Davies, 'A Crisis of Accountability' *The Privacy Surgeon* (June 2014) 5 <https://cippic.ca/uploads/Snowden_at_one_year-global_survey.pdf> accessed 10 October 2014.
[183]Ibid 7.

shifts in public opinion. There was an increase in intrusive surveillance measures during the Cold War era and a surge in support for privacy protections following the Watergate scandal and the Church Committee Report. The delayed response to the Cold War surveillance techniques is representative of surveillance reform in general. The clandestine nature of surveillance can postpone the counteracting shifts in opinion that support greater privacy until the cloak of secrecy is pierced. Accordingly, shifts in opinion in favour of greater privacy will often only occur after a scandal or leak. Moreover, the intermittent and often incomplete nature of unauthorised disclosures is likely to lessen the force of the corrective swing in public opinion due to inertia caused by public uncertainty.

Due to this difficulty, this article rejects Etzioni's claim that once the threat has passed, the intrusive measures 'can gradually be rolled back.'[184] Due to the norm of secrecy in the surveillance context, the public will rarely know if a threat has actually passed or even what measures need to be rolled back. Accordingly, this article suggests that mandating the regular reporting of transparent and comprehensive surveillance statistics provides the public with increased control over their governments without threatening security. By increasing transparency, civil society can track government activity and provide a more consistent check than that possible through reliance on unauthorised disclosures. In spite of this, however, this article acknowledges the importance of whistle-blowers as a crucial final line of defence against nefarious government activity.

[184]A Etzioni, *The Limits of Privacy* (Basic Books, 1999) 25.