TRANSPARENCY IN THE OPEN GOVERNMENT ERA

EDITED BY

IRÈNE BOUHADANA

WILLIAM GILLES

RUSSELL WEAVER

LES ÉDITIONS IMODEV

Légal deposit: Bibliothèque Nationale de France
February 2015
ISBN : 979-10-90809-05-5 (Paperback)

Printed in France

Les éditions Imodev ©
Institut du Monde et du Développement
pour la Bonne Gouvernance Publique (IMODEV)
49 rue Brancion 75015 Paris – France
www.imodev.org

CHAPTER 13
TRANSPARENCY, PRIVACY & THE SNOWDEN AFFAIR

Russell L. WEAVER

Professor of Law & Distinguished University Scholar, University of Louisville, Louis D. Brandeis School of Law

In many respects, the U.S. government is more open and transparent than it has ever been. Congress has enacted various statutes – the Freedom of Information Act (FOIA)[1], the Federal Advisory Committee Act (FACA)[2], and the Government in the Sunshine Act[3] – designed to give citizens more information regarding the inner workings of government. Congressional legislation has been supplemented by the "Open Government Initiative" (OGI) in which President Barack Obama promised to make his administration more open and transparent than any previous administration. Obama's Initiative included a pledge to develop better data release technology, facilitate the communication and release of governmental information, make more information available to the public through FOIA[4], and create an enabling policy framework for open government[5].

In addition to promoting openness and transparency, U.S. society has always emphasized individual privacy, especially privacy against governmental intrusions. This interest in privacy dates back to the founding of the nation, and abuses perpetrated by British officials during the American colonial period[6]. Concerned about the British use of general warrants and writs of assistance, which gave colonial officials broad authority to search the colonists and their homes, the new Americans demanded constitutional

1. 5 U.S.C. § 552 (1967).
2. 5 U.S.C. § App. (1972); 86 Stat. 770 (1972).
3. 5 U.S.C. § 552(b) (1976).
4. 5 U.S.C. § 552.
5. *See* Barack Obama, *Memorandum on Transparency and Open Government* (Jan. 21, 2009).
6. *See* Russell L. Weaver, *The James Otis Lecture: The Fourth Amendment, Privacy and Advancing Technology*, 80 Miss. L.J. 1131-1227 (2011).

protections against governmental intrusions.[7] These demands resulted in adoption of the Fourth Amendment to the United States Constitution which prohibited government from engaging in "unreasonable searches and seizures"[8] Privacy protections accelerated in the nineteenth century following publication of a seminal article by Samuel Warren and Justice Louis D. Brandeis on autonomy and privacy.[9] In that article, they forcefully articulated the need to protect "privacy," characterizing "the right to be let alone" as "the right most valued by civilized men."[10] The Warren and Brandeis article led to the creation of the modern tort of invasion of privacy which includes protection against both the government and private individuals, and creates four separate and distinct tort causes of action: 1) intrusion upon the plaintiff's seclusion or solitude, or into private affairs; 2) public disclosure of embarrassing private facts about the plaintiff; 3) publicity that places the plaintiff in a false light in the public eye; and 4) appropriation of the plaintiff's name or likeness for the defendant's advantage.[11]

Despite these significant movements toward openness and transparency, and enhanced privacy protections, recent revelations regarding the National Security Agency's (NSA) surveillance program[12] suggest that the U.S. government is not overly open and transparent or very protective of privacy. The NSA revelations highlight the contradictory pressures that government faces today. Although governments may talk about transparency and openness, and give lip service to the need to protect individual privacy, governments always maintain a level of secrecy,[13] and routinely engage in spying and surveillance. Although governments have a legitimate interest in shielding certain types of information (*e.g.*, state secrets or information vital that is potentially damaging to national security or foreign relations),[14] the question is one of balance.

This article discusses the NSA surveillance operations, as well as concerns regarding how those operations impact governmental transparency and

7. *Id.*

8. U.S. CONST., AMDT. IV.

9. *See* Samuel B. Warren & Louis B. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

10. *Id.*

11. *See* William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383 (1960); *see also* UNDERSTANDING THE FIRST AMENDMENT, *supra* note 23, at 48-52.

12. *E.g.*, Doug Stanglin; *Snowden Says NSA Can Tap Email Chats, The Courier-Journal*, A3 (Aug. 1, 2013); Shane Scott, *Disclosures on NSA, Surveillance Put Awkward Light on Previous Denials, N.Y. Times*, Jun. 12, 2013, at A. 18.

13. *See* William E. Funk, Sidney Shapiro & Russell L. Weaver, ADMINISTRATIVE LAW 623 (West, 4th ed., 2010) (hereafter Funk, Shapiro & Weaver).

14. *Id. See, e.g., United States v. Nixon*, 418 U.S. 683 (1974) (ordering President Nixon to release information, but noting that confidentiality regarding the President's conversations and correspondence is generally privileged, and going on to note that this privilege is "fundamental to the operation of Government and inextricably rooted in the separation of powers under the Constitution.").

individual privacy, and the tradeoffs that society has made in order to combat terrorism.

§ 1 – The Snowden Revelations

In June, 2013, Edward Snowden, an employee for an NSA contractor (Booz Allen Hamilton), revealed to the world that the United States government was involved in a massive secret surveillance and data collection operation.[15] Snowden, who was stationed in Hawaii,[16] stole thousands of documents from the NSA involving the years 2007 to 2012,[17] and fled to Hong Kong.[18] There, Snowden made contact with a well-known journalist, who had written about Julian Assange of WikiLeaks,[19] and provided the journalist with an extensive interview and copies of thousands of classified documents disclosing the scope of the NSA surveillance program.[20] Eventually, Snowden fled to Russia where he was granted temporary asylum.[21]

Before the Snowden disclosures, some may have suspected that the U.S. government was spying on ordinary citizens. However, Snowden revealed a surveillance operation that was so grand that one commentator described it as "breathtaking."[22] The NSA employs 35,000 people,[23] and operates with a budget of $10.8 billion per year.[24] With such a large staff, and a huge budget, the NSA was able to engage in worldwide surveillance.[25] One commentator suggested that the staggering breadth of the program as motivated by the NSA's desire "not to miss anything," enhanced by a staggeringly large budget and a "near-invisibility" of the program from governmental scrutiny.[26]

Snowden's revelations led to disclosure of the fact that the NSA was collecting a staggering array of information about people all over the world. The NSA was prying into all types of electronic communications, including information that could be gleaned from phone calls and

15. *E.g.*, Scott, *supra* note 12, at A18.
16. *See* Mark Mazzetti & Michael S. Schmidt, *Ex-CIA Worker Says He Disclosed U.S. Surveillance*, The New York Times, A1 (June 10, 2013).
17. *See See* Scott Shane, *No Morsel Too Minuscule for All-Consuming NSA: From Spying on Leader of U.N. to tracking Drug Deals, on Ethos of 'Why Not?'*, The New York Times, A10 (Nov. 13, 2013); Stanglin, *supra* note 12, at A3.
18. *See* Charlie Savage & Mark Mazzetti, *Cryptic Overtures and a Clandestine Meeting Gave Birth to a Blockbuster Story*, The New York Times, Jun. 10, 2013, at A. 13.
19. *See* Peter Maass, *How Laura Poitras Helped Snowden Spill His Secrets*, The New York Times, § MM (Aug. 13, 2013).
20. *Id.*
21. *See* Steven Lee Myers & Andrew E. Kramer, *Defiant Russia Grants Snowden Year' Asylum*, The New York Times, A1 (Aug. 1, 2013).
22. *See* Shane, *supra* note 17, at A10.
23. *See id.*, at A1.
24. *See* Shane, *supra* note 17, at A1.
25. *See How Laura Poitras Helped Sowden*, *supra* note 19.
26. *See* Shane, *supra* note 17, at A10.

e-mails, text messages, records of credit card purchases and information from social media networks. [27] In addition, the NSA hacked into foreign computers and installed software that allowed it to monitor actions on those computers,[28] and issued a secret order to Verizon Wireless requiring that company to turn over its phone records.[29] The NSA also developed a tool nicknamed "muscular" that it used to hack into Yahoo and Google data communication centers, thereby accessing hundreds millions of individual accounts belonging to both Americans and non-Americans.[30] As a result, the size of the NSA surveillance program grew by leaps and bounds, involving every e-mail sent through either the Google or Yahoo systems or posted on the Google.doc system,[31] and implicating some 1.8 million customer accounts[32] and 182 million communication records over a thirty-day period,[33] including "to" and "from" e-mail information, as well as text, audio and video information.[34] In addition, there was evidence suggesting that the U.S. Central Intelligence Agency (CIA) paid AT&T some $10 million per year for access to AT&T data files,[35] allowing the CIA to ask AT&T to search its database for information related to designated individuals.[36] However, because the CIA is prohibited from engaging in domestic spying on Americans, restrictions were imposed on the AT&T data collection process to protect the identity of Americans.[37] In theory, the NSA surveillance program was focused on obtaining access to communications of "foreign intelligence value,"[38] and on electronic communications that carried information pertaining to foreign intelligence targets.[39] Whether this was actually true is unclear. In any event, the NSA was storing collected information for up to five years.

The NSA was even spying on foreign leaders, including the heads of allied nations such as Germany, France, Brazil, Israel and Japan,[40] and had even

27. *See id.* at A10.
28. *See id.*, at A11.
29. *See How Laura Poitras Helped Sowden, supra* note 19.
30. *See* Barton Gellman &Ashkan Soltani, *NSA Hacks Yahoo, Google: Global Data Links Expose Untold Millions of Accounts,* THE COURIER-JOURNAL, A-1 (Oct. 31, 2013).
31. *See* Martha Mendoza, *Reagan's Order Led to NSA's Broader Spying,* THE COURIER-JOURNAL, A10, c. 1-6 (Nov. 24, 2013).
32. *Id.*
33. *Id.*
34. *Id.*
35. *See* Charlie Savage, *C.I.A. Ties to AT&T's Add Another Side to Spy Debate,* INTERNATIONAL HERALD TRIBUNE, A5 (Nov. 8, 2013).
36. *Id.*
37. *Id.* ("... when the company produces records of international calls with one end in the United States, it does not disclose the identity of the Americans and 'masks' several digits of their numbers...").
38. *See* Mendoza, *supra* note 31, at A10.
39. *Id.*
40. *Id.* at A1 & A10.

monitored German Chancellor Angel Merkel's cellphone.[41] In addition, the NSA spied on United Nations Secretary General Ban Ki-moon, in advance of a visit to the White House, in order to gain access to his talking points for the meeting.[42] This spying on allies produced anger and outrage with the Germans characterizing the spying as "completely unacceptable.[43] French President Francois Hollande responded similarly, denouncing the NSA spying as "totally unacceptable."[44]

The NSA may have collected so much information that it was simply unable to analyze or make effective use of that information.[45] Indeed, some of the data involved languages that NSA analysts were not capable of reading or analyzing.[46] The NSA defended its possession of this mega-data on the basis that it gave the NSA the ability to quickly search and uncover data as needed.[47] One estimate suggests that as much as fifty percent of the surveillance delivered to President Obama each morning was based on NSA surveillance.[48]

The U.S. government's surveillance program was hardly limited to electronic surveillance. The evidence reveals that the government was surveilling individuals, including U.S. citizens, in other ways. For example, the government has asserted the right to search all electronic devices that cross the U.S. border, including laptops, smart phones, etc., as well as the right to copy the information contained on those devices.[49] For those that run afoul of the NSA, these border searches could be frequent, rigorous and oppressive. For example, Laura Poitras, the journalist who worked with Snowden, assisting him in his disclosures, was continually harassed.[50] She was placed on a "terrorist watch list" that made it difficult to board flights,[51] and she was detained and cross-examined more than 40 times at airports.[52] In addition, she assumed that the government was surveilling her e-mails, phone calls and web browsing.[53]

---

41. *See* Alison Smale, *Anger Growing Among Allies on U.S. Spying: Merkel Calls Obama in Fallout Over NSA*, The New York Times, A1 (Nov. 21, 2013).
42. *Id.*
43. *See* Smale, *supra* note 41.
44. *See* Alissa J. Rubin, *French Condemn Surveillance by NSA: Anger After Report of Data Collection*, The New York Times, A1 (Oct. 21, 2013).
45. *See* Shane, *supra* note 17, at A10.
46. *Id.* at A11 (suggesting that some uncovered material was essentially worthless because of a shortage of trained linguists).
47. *Id.*
48. *Id.*
49. *See* Russell L. Weaver, *Administrative Searches, Technology & Personal Privacy*, 22 Wm. & Mary Bill Rt. J. 571 (2013).
50. *See How Laura Poitras Helped Sowden, supra* note 19.
51. *Id.*
52. *Id.*
53. *Id.*

§ 2 – Governmental Transparency

The Snowden disclosures raise very troubling issues regarding transparency, openness and governmental oversight. Any surveillance and data collection program is subject to possible abuse, and such a massive program is of particular concern because it is subject to possible abuse. Following the Snowden revelations, evidence emerged suggesting that the NSA was involved in improprieties. Indeed, at point following revelations of improprieties, the NSA promised to halt various illegal practices, but there is evidence suggesting that the NSA nevertheless continued to act illegally.[54] Some contend that the improprieties were not committed in bad faith, but rather were attributable to "poor management, lack of involvement by compliance officials and lack of internal verification."[55] In one case, the NSA asserted that an improper collection was attributable to a "typographical error."[56] Regardless, a federal intelligence court judge concluded that "those responsible for conducting oversight at the NSA had failed to do so effectively."[57]

The U.S. government's spying program did not begin with President Obama. Indeed, the NSA was created in 1952,[58] and President Ronald Reagan signed an executive order providing for expanded surveillance of non-U.S. citizens.[59] However, the program began ramping up following the 9/11 attacks when President George W. Bush invoked the Terrorist Surveillance Act to justify expanded surveillance.[60] That act was eventually replaced by the Foreign Intelligence Surveillance Act (FISA) which created a secret court to oversee governmental surveillance and data collection operations.[61]

While few doubt the government's need to combat terrorism, or to engage in surveillance in aid of that effort, and those who have criticized Snowden often focus on harm to the nation from his revelations regarding the NSA program. The difficulty is that the breadth of the NSA program, coupled with the extent of secrecy, raise very troubling implications for governmental openness and transparency. There was a point in history when governments considered themselves above criticism. In 1606, England's Star Chamber created the crime of seditious libel in *de Libellis Famosis*.[62] That decision

54. *See* Eileen Sullivan, *NSA Vowed Repeatedly to Fix Spying Missteps,* THE NEW YORK TIMES, A17, c. 1-6 (Nov. 20, 2013).
55. *Id.*
56. *Id.*
57. *Id.*
58. *See* Shane, *supra* note 17, at A1.
59. *See* Mendoza, *supra* note 31, at A10.
60. *See* Kimberly Dozier, *Spy Program Origins Outlined: President George W. Bush OK'd Effort in October'01,* THE COURIER-JOURNAL, A3 (Dec. 22, 2013).
61. *Id.*
62. 77 Eng. Rep. 250 (Star Chamber 1606).

replaced, in part, the criminal offense of constructive treason,[63] and made it a crime to criticize the government or governmental officials (and, at one point, the clergy as well).[64] The crime was enforced by "threats of punishment, litigation costs, and stigma,"[65] and was justified by the notion that criticism of the government "inculcated a disrespect for public authority."[66] "Since maintaining a proper regard for government was the goal of the offense, it followed that truth was just as reprehensible as falsehood" and therefore was not a defense.[67] Indeed, truthful criticisms were punished more severely than false criticisms because truthful criticisms were regarded as potentially more damaging to the government.[68] Today, the concept of seditious libel has disappeared, as have concepts of absolute monarchy and divine right, and been replaced by democratic principles. In a modern democratic system, a level of governmental transparency is an essential element [69] If the

63. *See* William T. Mayton, *Toward a Theory of First Amendment Process: Injunctions of Speech, Subsequent Punishment, and the Costs of the Prior Restraint Doctrine*, 67 CORNELL L. REV. 245, 248 (1982).

64. *Id.* Indeed, in *de Libellis Famosis,* the defendants had ridiculed high clergy.

65. *Id.*

66. *Id.*; *see also* Matt J. O'Laughlin, *Exigent Circumstances: Circumscribing the Exclusionary Rule in Response to 9/11*, UMKC L. REV. 707,720-21 (2002).

67. *Id; see also* William R. Glendon, *The Trial of John Peter Zenger*, 68 N.Y. ST. B.J. 48, 49 (1996).

68. *See* Stanton D. Krauss, *An Inquiry into the Right of Criminal Juries to Determine the Law in America*, 89 J. CRIM. L. & CRIMINOLOGY 111, 183 n.290 (1998); *see also* Glendon, *supra* note 67, at 48.

69. *See* C. Edwin Baker, *Scope of the First Amendment Freedom of Speech*, 25 U.C.L.A. L. REV. 964 (1978); Robert H. Bork, *Neutral Principles and Some First Amendment Problems*, 47 IND. L.J. 1 (1971); Thomas I. Emerson, *Toward a General Theory of the First Amendment*, 72 YALE L.J. 877 (1963); Alexander Meiklejohn, *The First Amendment as an Absolute*, 1961 S. CT. REV. 245; Russell L. Weaver & Donald E. Lively, UNDERSTANDING THE FIRST AMENDMENT (4th ed. 2013). In the U.S., democratic principles are frequently relied on by the United States Supreme Court in construing the First Amendment protections for freedom of speech and of the press. For example, in *Garrison v. Louisiana*, 379 U.S. 64, 74–75 (1964), the Court stated that "speech concerning public affairs is more than self-expression; it is the essence of self-government." In *McDonald v. City of Chicago*, 130 S. Ct. 3020, 3098 (2010), the Court stated that freedom of expression is "essential to free government" and "to the maintenance of democratic institutions." In *Federal Election Commission v. Massachusetts Citizens for Life, Inc.*, 479 U.S. 238, 264 (1986), the court recognized that freedom of speech "plays a fundamental role in a democracy; as this Court has said, freedom of thought and speech 'is the matrix, the indispensable condition, of nearly every other form of freedom.' " As one commentator noted: "Every government must have some process for feeding back to it information concerning the attitudes, needs and wishes of its citizens. [...] The crucial point [is] not that freedom of expression is politically useful, but that it is indispensable to the operation of a democratic form of government. Once one accepts the premise of the Declaration of Independence — that governments derive 'their just powers from the consent of the governed' — it follows that the governed must, in order to exercise their right of consent, have full freedom of expression both in forming individual judgments and in forming the common judgment. [...] [O]nce a society was committed to democratic procedures, or rather in the process of committing itself, it necessarily embraced the principle of open political discussion." Emerson, *supra* note 69, at 993-884.

people are going to vote on candidates, and express their preferences on the major issues of the day, then they need to have enough information about the workings of government to enable them to make informed decisions.[70] The difficulty with the NSA program is that it has operated in deep stealth with almost no openness or transparency. For example, when the NSA demanded information from communications companies, it required them to maintain confidentiality on pain of criminal penalties. In other words, not only were the companies required to turn over the information, but they were required to keep the government's demands secret, and not allowed to alert their customers.[71]

Secrecy was maintained in other ways as well. In *Clapper v. Amnesty International USA*,[72] attorneys and human rights, labor, legal, and media organizations whose work required them to engage in sensitive and sometimes privileged telephone and e-mail communications with colleagues, clients, sources, and other individuals located abroad sought to challenge the NSA program. They argued that some of the people that they exchanged information with were likely targets of surveillance by the NSA because they were "associated with terrorist organizations," or were "people located in geographic areas that are a special focus" of the Government's counter terrorism or diplomatic efforts, or activists who oppose governments that are supported by the United States Government. Plaintiffs asserted injury because the NSA surveillance program compromised their "ability to locate witnesses, cultivate sources, obtain information, and communicate confidential information to their clients."[73] As a result, plaintiffs claimed that they had "ceased engaging" in certain telephone and e-mail conversations, and that the threat of surveillance compelled them to travel abroad in order to have in-person conversations.[74] In other words, because of the possibility of governmental surveillance, plaintiffs were forced to undertake "costly and burdensome measures" to protect the confidentiality of sensitive communications.[75] The plaintiffs sought a declaration that the NSA surveillance was unconstitutional, and they also sought injunctive relief precluding the Government from engaging in surveillance against them.[76] The U.S. Supreme Court held that plaintiffs lacked "standing" to bring the case because they could not show a "concrete, particularized, and actual or imminent" injury, that is fairly traceable to the challenged action, and that can be redressed by a

70. *See* Funk, Shapiro & Weaver, *supra* note 13, at 623.
71. *See* Shane, *supra* note 17, at A10.
72. 133 S. Ct. 1138 (2013).
73. *Id.* at 1145.
74. *Id.*
75. *Id.* at 1143.
76. *Id.* at 1142.

favorable ruling."[77] The Court held that plaintiffs' fear that the Government would target their communications was simply speculative,[78] noting that plaintiffs failed "to offer any evidence that their communications have been monitored under § 1881a." or even that the Government had sought FISC approval for surveillance of their communications.[79]

Of course, the *Clapper* decision placed the plaintiffs in a Catch 22 situation. The Court concluded that plaintiffs could not establish standing because they could not prove that the NSA was subjecting them to surveillance. Of course, how could they satisfy this requirement? The government's processes were secret. As a result, even if the Government was subjecting plaintiffs to surveillance, there is a significant likelihood that they would not know it, or be able to prove it. As a result, plaintiffs asked that the Government be forced to reveal, through *in camera* proceedings, whether it was intercepting respondents' communications and what targeting or minimization procedures it was using.[80] The Court refused to require the Government to make this revelation,[81] noting that plaintiffs were required to establish standing by "pointing to specific facts," and that the Government was not required to "disprove standing by revealing details of its surveillance priorities."[82] The net effect was that, because the government's surveillance program was super-secret, plaintiffs could not prove that they were under surveillance, and therefore they could not meet the case or controversy necessary to proceed with the litigation.

Secrecy pervaded all aspects of the NSA surveillance program. The program was premised on the Foreign Intelligence Surveillance Act (FISA) of 1978[83] which regulates and authorizes the government to engage in electronic surveillance of communications for foreign intelligence purposes. The Act creates two specialized courts. The first court, the Foreign Intelligence Surveillance Court (FISC), was given the power to approve electronic surveillance for foreign intelligence purposes if the court found probable cause to believe that "the target of the electronic surveillance is a foreign power or an agent of a foreign power," and that each of the specific "facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power."[84] The second court, the Foreign Intelligence Surveillance Court of Review, was given review jurisdiction when FISC denied applications for electronic

77. *Id. (Citing Monsanto Co. v. Geertson Seed Farms,* 130 S. Ct. 2743, 2752 (2010)).
78. *Clapper*, 133 S. Ct. at 1148.
79. *Id.*
80. *Id.* at 1149, No. 4.
81. *Id.*
82. *Id.*
83. 50 U.S.C. § 1801 *et seq.*
84. §50 U.S.C. § 105(a)(3).

surveillance.[85] However, the orders of both courts were classified as secret. Following the 9/11 attacks, President George W. Bush expanded the NSA's authority to conduct warrantless wiretapping of telephone and e-mail communications when one party to a communication in located outside the United States and a participant in "the call [is] reasonably believed to be a member or agent of Al Qaeda or an affiliated terrorist organization."[86] By 2007, the FISC had issued orders authorizing the U.S. Government to target international communications into or out of the United States when there is probable cause to believe that one participant to the communication is affiliated with Al Qaeda or an associated terrorist organization.[87] Under the Bush orders, any electronic surveillance under the NSA's program was subject to approval by the FISC.[88]

After a FISC judge issued a decision narrowly construing FISC's authority, Congress enacted the FISA Amendments Act of 2008 (FISA Amendments Act). While these amendments left much of FISA unchanged, they did create a new basis for governmental collection of information.[89] In particular, § 702 of the amendments established a system under which the Government could seek authorization for foreign intelligence surveillance that would target the communications of non-U.S. persons located abroad.[90] The new framework did not require the Government to establish probable cause to believe that the target of the electronic surveillance is a foreign power or agent of a foreign power.[91] The amendments also did not require the Government to specify the location of the particular facilities or places where the electronic surveillance would occur.[92]

Under the FISA Amendments, if the FISC issues an order permitting it, "the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to one year[,] the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[93] However, under the Amendments, the Government may not intentionally target any person known to be in the United States or any U.S. citizen living abroad.[94] In addition, any surveillance must be consistent with the Fourth Amendment,[95] and is subject to congressional review as well as Executive Branch review.[96] In particular, the FISC court must approve

85. *Id.*, at § 1803(b).
86. *See American Civil Liberties Union v. NSA*, 493 F.3d 644, 648 (6th Cir. 2007).
87. *See Clapper*, 133 S. Ct. at 1143.
88. *Id.* at 1144.
89. *Id.*
90. 50 U.S.C.A. § 1881(a).
91. *Id.*
92. *Id.*
93. *Id.*
94. 50 U.S.C. § 1881(a)(b)(1)–(3).
95. 50 U.S.C. § 1881(a)(b)(5).
96. 50 U.S.C. § 1881(a).

the Government's "targeting" procedures, "minimization" procedures, and a governmental certification regarding proposed surveillance.[97] The "certification" must attest to several things: (1) that procedures are in place "that have been approved, have been submitted for approval, or will be submitted with the certification for approval by the [FISC] that are reasonably designed" to ensure that an acquisition is "limited to targeting persons reasonably believed to be located outside" the United States; (2) that minimization procedures adequately restrict the acquisition, retention, and dissemination of nonpublic information about unconsenting U.S. persons, as appropriate; (3) that guidelines have been adopted to ensure compliance with targeting limits and the Fourth Amendment; and (4) that the procedures and guidelines referred to above comport with the Fourth Amendment.[98] Additionally, the FISC should determine whether the targeting procedures are "reasonably designed" (1) to "ensure that an acquisition [is] limited to targeting persons reasonably believed to be located outside the United States" and (2) to "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known [to] be located in the United States."[99] The Court analyzes whether the minimization procedures "meet the definition of minimization procedures under section 1801(h)[,] as appropriate."[100] The Court also assesses whether the targeting and minimization procedures are consistent with the statute and the Fourth Amendment.[101]

In regard to the NSA surveillance program, there was a complete absence of openness and transparency, and a complete inability on the part of the public to determine whether the surveillance was being conducted in accordance with U.S. law. Not only the actions of the NSA, but those of the FISC, were shielded from public scrutiny. Thus, the e-mails of Americans were being routinely seized,[102] as were text, audio and video contained in those e-mails,[103] with virtually no transparency or public oversight. Although it may be illegal for the NSA to spy inside the U.S., NSA purportedly acted in compliance with U.S. law.[104] The difficulty is that it was impossible for American citizens to know what the NSA, or the FISC court, were doing. Sometimes, the NSA collaborated with the British government's Communications Headquarters,[105] but it is not clear that foreign governments were subject to restrictions on their use of the NSA data.[106]

97. *Id.*
98. 50 U.S.C. § 1881(a)(c).
99. 50 U.S.C. § 1881a(i)(2)(B).
100. 50 U.S.C. § 1881a(i)(2)(C).
101. 50 U.S.C. § 1881a(i)(3)(A).
102. *See* Mendoza, *supra* note 31, at A10.
103. *Id.*
104. *Id.*
105. *Id.*
106. *Id.*

§ 3 – The Assault on Privacy

The NSA surveillance program also represents an extraordinary assault on individual privacy. As the Brandeis and Warren article suggests, the right to be let alone is an essential element of a free society.[107] Although the privacy protections afforded to Americans have always lagged behind the protections provided by European governments to their citizens, privacy remains a value.

The difficulty is that it is not clear that U.S. law provides much protection against the NSA surveillance program. The most obvious source of protection is the Fourth Amendment to the United States Constitution.[108] That Amendment was enacted in response to abuses during the colonial period. British colonial authorities had used Writs of Assistance that allowed them to do no more than specify the object of a search, and thereby obtain a warrant allowing them to search any place where the goods might be found,[109] without limit as to place or duration.[110] Colonial officials had also used "general warrants" that required them only to specify an offense, and then left it to the discretion of executing officials to decide which persons should be arrested and which places should be searched.[111] These British practices stirred up such a high level of anger among the colonists that, when the newly-written U.S. Constitution was sent to the states for ratification, it rapidly became clear that the proposed constitution would not be ratified without explicit protections against similar abuses (as well as protection for various other rights).[112] The demands culminated in an agreement to enact the Constitution as written, but with the understanding that the first Congress would create a Bill of Rights (which turned out to be the first ten amendments to the U.S. Constitution). The Bill of Rights provided protections for various rights, including the Fourth Amendment's prohibition against "unreasonable searches and seizures."[113]

While it can be argued that the NSA's massive surveillance campaign constitutes an "unreasonable" search and seizure of electronic communications, it is not

107. *See* Warren & Brandeis, *supra* note 9.

108. U.S. Const., Amdt. IV.

109. *See Virginia v. Moore*, 553 U.S. 164, 168-169 (2008); *Samson v. California*, 547 U.S. 843, 858 (2006); *Atwater v. City of Lago Vista*, 532 U.S. 318, 339-340 (2001): *see also* Russell L. Weaver, Leslie W. Abramson, John M. Burkoff & Catherine Hancock, Principles of Criminal Procedure 64 (3d ed. 2008).

110. *See Steagald v. United States*, 451 U.S. 204, 221 (1981); *Gilbert v. California*, 388 U.S. 263, 286 (1967) (*quoting Boyd v. United States*, 116 U.S. 616, 625 (1886)).

111. *See Virginia v. Moore*, 553 U.S. 164, 168-169 (2008); *Steagald v. United States*, 451 U.S. 204, 220 (1981); *Payton v. New York*, 445 U.S. 573 (1980).

112. *See Maryland v. Garrison*, 480 U.S. 79, 91 (1987); *see also Marshall v. Barlow's, Inc.*, 436 U.S. 307, 311 (1978); *Boyd v. United States*, 116 U.S. 616, 625 (1886); *see also United States v. Verdugo-Urquidez*, 494 U.S. 259, 266 (1990).

113. U.S. Const., Amdt. IV.

clear that the NSA has transgressed the boundaries of the Constitution under current Fourth Amendment jurisprudence. When the Fourth Amendment was drafted and ratified, the state of surveillance technology was relatively crude and simplistic, and the ability of the government to pry into the lives of private citizens was much more circumscribed. The early Americans were focused on abuses committed by the British in using writs of assistance and general warrants, and actual physical searches of houses or property, and the United States Supreme Court's early definitions of the term "search" tended to track the early understandings and concerns.[114] As a result, most early Fourth Amendment cases used a historical definition of the term "search" by focusing on actual physical searches (intrusion into a "constitutionally protected" space) of people and places.[115] If a place was searched, the question was whether the government had intruded or trespassed into a "constitutionally protected area."[116] Thus, when the police broke into someone's house (a "constitutionally protected area"), and rummaged through its contents, the Court had no difficulty concluding that the Fourth Amendment applied.[117] Likewise, when the police made an unauthorized entry into a car (once automobiles came into existence) to rummage through the trunk, or they seized an individual's briefcase to review its contents, the courts would hold that the police had conducted a search.[118]

The difficulty is that, in the ensuing centuries, police surveillance technologies have gone high tech, and U.S. Fourth Amendment jurisprudence has not kept up with advances in technology. Indeed, modern technologies have created Orwellian possibilities for snooping.[119] For example, the police now have microphones that allow them to overhear conversations from distant locations,[120] as well as devices that allow them to hear through walls,[121] and super-sensitive microphones that allow them to overhear conversations through remotely placed technology.[122] Police can maintain closed circuit

114. *See, e.g.*, *Carroll v. United States*, 267 U.S. 132 (1925); *Hester v. United States*, 265 U.S. 57 (1924) (concluding that "the special protection accorded by the Fourth Amendment to the people in their 'persons, houses, papers and effects,' is not extended to the open fields.").

115. *See Draper v. United States*, 358 U.S. 307 (1959).

116. *See, e.g., Goldman v. United States,* 316 U.S. 129 (1942); *Olmstead v. United States*, 277 U.S. 438 (1928); *Ex Parte Jackson*, 96 U. S. 727 (1877); *see also* Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 381 (1974).

117. *See Silverman v. United States*, 365 U.S. 505 (1961).

118. *See, e.g.*, *Carroll v. United States*, 267 U.S. 132 (1925).

119. *See* George Orwell, 1984 (1944).

120. *See Katz v. United States*, 389 U.S. 347 (1967) (involving the attachment of an electronic listening device to the outside of a phone booth so that the police could overhear what was being said inside the phone booth).

121. *See Goldman v. United States,* 316 U.S. 129 (1942) (involving the use of a listening device that allowed the police to overhear what was being said in Goldman's office even though the police were located in an adjoining office).

122. *See Silverman v. United States*, 365 U.S. 505 (1961) (discussing the fact that advanced surveillance technologies were already available in the 1960s).

television systems that allow them to continuously surveil public places,[123] can use global positioning systems (GPS) that allow them to continuously monitor the location of individuals and things,[124] and have devices that allow them to overhear cell and cordless telephone conversations.[125] Moreover, and more relevant to the NSA surveillance program, as PCs and the Internet have come into common usage, governmental officials have devices that allow them to monitor key strokes and other computer uses,[126] and that allow one person to invade the privacy of a person's home and data from distant cyber sources through spyware technology.[127] Or, as the NSA has done, the government can sweep up massive amounts of communications data and information from electronic communications companies.

Even though the U.S. Supreme Court has attempted to update U.S. Fourth Amendment jurisprudence to respond to the onslaught of advancing technology, its efforts have proved unavailing.[128] The Court's landmark decision in *Katz v. United States*[129] shifted the debate, and attempted to come to grips with technology. And, indeed, *Katz* was revolutionary in the sense that it broke from precedent, and laid down a new approach for dealing with technological issues: whether the government had violated a citizen's "reasonable expectation of privacy" (REOP).[130] By shifting the debate from unconstitutional invasions to REOP, *Katz* offered hope to those who were concerned regarding the advance of technology and the potential implications for privacy, and seeking to rein in governmental abuses of technology. The difficulty is that *Katz* has not lived up to expectations because the *Katz* test has been narrowly construed, and has not easily adapted to new technologies.[131]

---

123. *See* Dina Temple-Raston & Robert Smith, *U.S. Eyes U.K.'s Surveillance Cameras*, National Public Radio, Weekend Edition Sunday (July 8, 2007). The article can be found at: http://www.npr.org/templates/story/story.php?storyId=11813693.

124. *See City of Ontario v. Quon*, 130 S. Ct. 2610 (2010); *Devega v. State*, 286 Ga. 448, 689 S.E.2d 293 (2010).

125. *See People v. Ledesma*, 206 Ill. 2d 571, 276 Ill. Dec. 900, 795 N.E.2d 253 (2003) (discussing a private individual's interception of a telephone conversation);
Kimberly R. Thompson, *Cell Phone Snooping: Why Electronic Eavesdropping Goes Unpunished*, 35 Am. Crim. L. Rev. 137, 143-44 (1997).

126. *See* the computer spyware devices sold by the USA Spy Shop at the following URL: http://www.usaspyshop.com/spy-software-c-55.html.

127. *See* Alan F. Blakley, Daniel B. Garrie & Matthew J. Armstrong, *Coddling Spies: Why the Law Doesn't Adequately Address Computer Spyware*, 2005 Duke L. & Tech. Rev. 25, 1 (2005); Jason Broberg, *From Calea to Carnivore: How Uncle Sam Conscripted Private Industry in Order to Wiretape Digital Telecommunications*, 77 N. Dakota L. Rev. 795 (2001); Jayni Foley, *Are Google Searches Private? An Originalist Interpretation of the Fourth Amendment in Online Communication Cases*, 22 Berkeley Tech. L.J. 447 (2007).

128. *See The Fourth Amendment, Privacy and Advancing Technology, supra* note 6.

129. 389 U.S. 347 (1967).

130. *Id.* at 351 ("For the Fourth Amendment protects people, not places.").

131. *See* Weaver, *supra* note 6.

In the NSA context, the *Katz* test is unhelpful because of subsequent glosses placed on that test. In particular, the U.S. Supreme Court has held that individuals retain no "expectation of privacy" in information that they voluntarily convey to third parties. For example, in *Smith v. Maryland,*[132] the police used a pen register to record the numbers dialed from Smith's home phone in order to investigate his possible participation in a robbery. The pen register is a device, in this case installed by the phone company at its central offices, that can record the phone numbers dialed from a phone, but which does not record the contents of the telephone conversations themselves.[133] Smith argued that he had a REOP in the phone numbers because he dialed them from the privacy of his home, and he contended that a reasonable person would expect privacy in such information. Applying the *Katz* test, the Court disagreed, emphasizing that people realize that the phone company has the capacity to record the numbers they call,[134] that the phone company exercises that capability when it records the numbers called for long distance billing purposes,[135] and that the phone company also uses call records to help protect customers against unwelcome or harassing phone calls.[136] As a result, the Court concluded that telephone users do not have a REOP in the telephone numbers that they dial.[137] The troubling aspect of the decision was that the Court went on to make a sweeping generalization to the effect that an individual has "no legitimate expectation of privacy" in information that he "voluntarily turns over to third parties,"[138] including information turned over to the company's mechanical equipment.[139]

Smith sparked considerable debate between the justices regarding the meaning of the REOP concept. For example, Justice Stewart, dissenting, found it difficult to reconcile the decision with the holding in *Katz* (that a conversation was protected even though it went through the same third party, the phone company), and he argued that Smith was in a comparable position to Katz (if not in a position even more deserving of protection) because he made calls from a phone in his own home.[140] Smith had no choice but to convey the phone numbers to the phone company,[141] if he

132. 442 U.S. 735 (1979).
133. *Id.* at 741.
134. *Id.* at 742.
135. *Id.*
136. *Id.* at 742-743.
137. *Id.* at 743.
138. *Id.* at 744.
139. *Id.* at 745 ("[P]etitioner voluntarily conveyed to [the phone company] information that it had facilities for recording and that it was free to record. In these circumstances, petitioner assumed the risk that the information would be divulged to police.").
140. *Id.* at 746 ("The role played by a private telephone is even more vital, and since *Katz* it has been abundantly clear that telephone conversations carried on by people in their homes or offices are fully protected by the Fourth and Fourteenth Amendments.").
141. *Id.* at 746-747.

wanted to use his phone, and Justice Stewart speculated that not many people would be happy to know that the numbers they dial (and thereby send to the phone company), have no constitutional protection against searches and seizures, especially given that such calls might reveal the intimate details of the individual's life.[142] Justice Marshall also dissented, arguing that people expect privacy, not only in the contents of their telephone conversations, but also regarding the phone numbers that they dial.[143] Even if individuals disclose those numbers to the phone company for a limited purpose (*e.g.*, to make phone calls), he argued that people do not expect that this information will be released to other persons for other reasons, and they certainly do not contemplate that they are releasing the information for general distribution to the public.[144] Moreover, when people make phone communications, they had little choice (at that time anyway) but to use that mode of communication, and therefore he argued that they did not assume the risk that the information will be made public.[145] Nevertheless, the majority concluded that there was no violation of Smith's REOP.

Smith is hardly the only decision in which the Court has held that an individual does not retain an expectation of privacy in information turned over to a third party. For example, in *United States v. Miller*,[146] the Court held that copies of checks and other bank records turned over to a bank were not accompanied by a REOP, especially since a federal law (Bank Secrecy Act of 1970) required that the records be maintained by the bank. *Miller* provided a clear opportunity for the Court to show that *Katz* had altered the Court's Fourth Amendment jurisprudence. Nevertheless, *Miller* rejected the Fourth Amendment claim noting "that there was no intrusion into any area in which respondent had a protected Fourth Amendment interest,"[147] and holding that Miller could not assert either ownership or possession over the papers because the bank kept those records pursuant to its statutory obligations.[148] Moreover, the Court concluded that a "depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[149] Justice Brennan dissented arguing that Miller had a legitimate expectation of privacy in the copies of his checks and other records held by his bank.

142. *Id.* at 748 ("I doubt there are any who would be happy to have broadcast to the world a list of the local or long distance numbers they have called. This is ... because it easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life.").
143. *Id.* at 748-749.
144. *Id.* at 749-750.
145. *Id.* at 750.
146. 425 U.S. 435 (1976).
147. *Id.* at 440.
148. *Id.* at 442.
149. *Id.*

Miller was followed by the holding in *Couch v. United States*,[150] a case that involved a summons issued to Couch's accountant for the production of documents, including "books, records, bank statements, cancelled checks, deposit ticket copies, work papers and all other pertinent documents pertaining to the tax liability of the above taxpayer." Although the case focused primarily on whether Couch could assert her Fifth Amendment privilege against self-incrimination, the case also involved Fourth Amendment claims. In particular, Couch attempted to rely on an alleged "accountant-client relationship" to establish a REOP in documents held by the accountant on her behalf.[151] The Court rejected the idea of a confidential accountant-client privilege, and held that "there can be little expectation of privacy where records are handed to an accountant, knowing that mandatory disclosure of much of the information therein is required in an income tax return."[152] Like *Miller*, *Couch* provided the Court with an opportunity to clearly establish that its Fourth Amendment jurisprudence had changed. As with bank records, when one turns records over to an accountant, one assumes that they will be used for a limited purpose, and not disclosed generally to the public, and therefore arguably maintains an expectation of privacy in the records. The Court did not adopt that approach.

Pushed to their logical extremes, decisions like *Smith*, *Miller* and *Couch* suggest that the Fourth Amendment imposes few limitations on the NSA's authority to collect phone, SMS and e-mail information from communications companies. Since all of this information is voluntarily conveyed by the individuals to the companies, the company's customers may not be protected under U.S. Fourth Amendment jurisprudence. Of course, the Court may choose to shift course and to conclude that these types of communications are fundamentally different than the transactions involved in cases like *Smith*, *Miller* and *Couch* because of the broad-based privacy implications. However, for now, there seem to be few Fourth Amendment limitations on the NSA's Fourth Amendment surveillance of data held by technology and communications companies.

Conclusion

Despite movements in the United States towards greater transparency and openness, and greater protections for individual privacy, the Snowden affair produced startling revelations regarding the scope of governmental surveillance of ordinary people. Snowden revealed that, not only is the government involved in widespread surveillance of electronic communications, but the government is collecting and storing large

150. 409 U.S. 322 (1973).
151. *Id.* at 336.
152. *Id.*

amounts of information. The sheer magnitude and scope of the data collection effort is staggering.

Snowden's revelations have sparked a debate regarding the propriety of the NSA surveillance program,[153] especially the scope of that program,[154] as well as frank discussions between the U.S. and its allies regarding the propriety of spying on allies.[155] Indeed, within the United States, the revelations touched off a fire storm of controversy. Even though President Obama tried to assure that the NSA surveillance program was directed at foreigners rather than at U.S. citizens, many were skeptical. Obama admitted that, when Americans communicate with foreigners, the NSA may be able to target their communications.[156] As a result, the Snowden revelations have led to frank discussions regarding the individual and policy implications of maintaining an intrusive surveillance program in a democratic society,[157] and the possibility that the data collection program will be turned against American citizens.[158]

Unquestionably, Snowden has been divisive. Some view Snowden as a hero who brought important issues into public view. In a video that he released to the public,[159] Snowden sought to justify his disclosures based on the public's right to know: "the public needs to decide whether these programs and policies are right or wrong."[160] By contrast, the U.S. government has attacked Snowden, claiming that his disclosures seriously damaged American interests. James R. Clapper Jr., director of the NSA, stated that the disclosures created serious risks to national security, and were "literally gut-wrenching ... because of the huge, grave damage it does to our intelligence capabilities."[161] In addition, the NSA has dismissed objections to the surveillance program on the grounds that virtually every nation engages in similar types of surveillance,[162] a position that has some validity,[163] and it has claimed that the NSA surveillance program has foiled some 50 terrorist plots, at least 10 of which had targeted the U.S. homeland.[164] Indeed, the NSA claims that the New York Stock Exchange, and the New York subway

153. *See* Shane, *supra* note 17, at A1 & A10.
154. *Id.*
155. *See* Alison Smale and David E. Sanger, *Spying Scandal Alters Ties With Allies and Leads to Talk of U.S. Policy Shift*, The New York Times, A4 (Nov. 12, 2013).
156. *See* Kevin Johnson, *NSA: Surveillance Foiled 50 Terrorist Plots; Director Says NYSE Was Among Targets*, USA Today, 5A (June 20, 2013).
157. *See* Shane, *supra* note 17, at A11.
158. *See id.*
159. *See How Laura Poitras Helped Sowden, supra* note 19.
160. *See* Mazzetti & Schmidt, *supra* note 16, at A1.
161. *See id.*
162. *See* Shane, *supra* note 17, at A1.
163. *See id.*, at A11.
164. *See* Johnson, *supra* note 156; *see also* Shane, *supra* note 17, at A10.

system, had been targets of terrorist attacks.[165] As a result, the NSA argues that the surveillance program has effectively thwarted additional 9/11 type attacks.[166] Of course, it is impossible to confirm or refute the NSA's allegations because of the intense secrecy surrounding the surveillance program. In addition, it is unclear how many of these plots would have been thwarted anyway through normal law enforcement processes. While the government claims that the NSA surveillance program is subject to rigorous oversight,[167] it is impossible to confirm that fact since the review process is secret.

It is likely that the Snowden revelations will lead to restrictions on the NSA's surveillance practices;[168] the only issue is the nature and substance of those restrictions. As the prior discussion of the Fourth Amendment reveals, technology has "outrun" policy in this area of the law,[169] and the NSA's targeting of ordinary citizens has produced a backlash, especially over the targeting of allied nations which some regard as "bad politics" and "foolish."[170] The program is tied up in new litigation.[171] In addition, a task force, appointed by President Obama, ultimately recommended sweeping revisions to the NSA's surveillance authority.[172] Among the suggested changes were to shift the NSA from military to civilian control, as well as changes to how the NSA gathers and stores information.[173] The panel also suggested restrictions on the NSA's ability to access information.[174] President Obama accepted some of these proposals,[175] but many have questioned whether Obama's restrictions went far enough.[176] Recently, a report by the Privacy and

165. *See* Johnson, *supra* note 156.

166. *Id.* (NSA's Director, Keith Alexander, stated before Congress that "I would much rather be here today debating this than explaining why we were unable to prevent another 9/11" attack.).

167. *Id.*

168. *Id.*

169. *See* Shane, *supra* note 17, at A11.

170. *Id.*

171. *See* Andrew Grossman, *Lawyers Win Right to See Secret Court Files,* THE WALL STREET JOURNAL, A5 (Jan. 30, 2014).

172. *See* Siobhan Gorman, *Panel Pushes Revamp of NSA,* THE NEW YORK TIMES, A1, c.6 (Dec. 13, 2013).

173. *Id.*

174. *Id.*

175. *See* Peter Baker & Jeremy W. Peters, *With Plan to Overhaul Spying, the Divisiveness is in the Details,* THE NEW YORK TIMES, A13 (Jan. 19, 2014); Peter Baker & Charlie Savage, *Obama to Place Some Restraints on Surveillance: Keeps Many Programs,* THE NEW YORK TIMES, A1 (Jan. 15, 2014).

176. *See* Mark Landler & Charlie Savage, *Keeping Wide Net, Obama Sets Limits on Phone Spying: Calibrated Plan Cubs Bulk Data Access but Disappoints Critics of NSA,* THE NEW YORK TIMES, A1 (Jan. 18, 2014); *Obama's Spying Overhaul Criticized: Congress' Intelligence Panel Members Wary of Proposal,* THE COURIER-JOURNAL, A1 (Jan. 20, 2014).

Civil Liberties Oversight Board questioned the legality of the NSA program.[177]

Restrictions on the surveillance program may come from the U.S. Congress.[178] However, within Congress, the traditional conflict between transparency and security continues to play itself out.[179] Even though some senators are pressing for quick action (in particular, Ron Wyden and Rand Paul), the Speaker of the House (John Boehner) is wary of moving too hastily, as is the Majority Leader in the U.S. Senate, Harry Reid.[180] Indeed, as a number of lawmakers have suggested, the NSA surveillance program is designed to protect Americans.[181] Of course, the question is whether the intrusiveness of the program, and the obvious threats to privacy, justify such widespread surveillance and data collection.[182] Whatever compromise emerges is unlikely to ban NSA surveillance practices completely, but may promote greater transparency.[183] For example, one proposal would impose disclosure requirements on intelligence agencies, and require the submission of reports on the use of mass surveillance techniques, and the number of instances in which the agencies have violated privacy rules or safeguards.[184]

The ultimate check on governmental abuse may come from the electronic communications companies themselves. As the Snowden disclosures became public, U.S. technology and communication companies became increasingly concerned that foreigners would stop doing business with them in an effort to minimize NSA surveillance of their activities.[185] As a result, a number of technology companies have been at the forefront in terms of demanding restrictions on NSA surveillance activities.[186] For example, companies like Google, Microsoft, Yahoo, Facebook, Twitter, AOL and Linkedin, have presented their own plans for regulating online spying, and have taken out full page advertisements in various newspapers articulating their concerns.[187] As one technology executive stated, "People

177. *See* Alexei Alexis, *NSA Bulk Collection of Phone Data Not Lawful, Privacy Board Concludes*, BNA Privacy and Data Security Law Resource Center (Jan. 23, 2014).
178. *See* Adam Liptak & Jeremy W. Peters, *Congress and the Courts Weigh New Attempts to Scale Back NSA Spying*, The New York Times, A16 (Nov. 19, 2013).
179. *Id.*
180. *Id.*
181. See Johnson, *supra* note 156.
182. *Id.*
183. *See* Liptak & Peters, *supra* note 178 (Noting that Senator Wyden drafted legislation in an effort "to appeal to both ends of the spectrum on surveillance. It purposely contains nothing about banning NSA data collection methods so it does not alienate those who are generally supportive of current intelligence practices.").
184. *Id.*
185. *See* Shane, *supra* note 17, at A10.
186. *See* Edward Wyatt & Claire Cain Miller, *Tech Giants Call for Surveillance Curbs*, The New York Times, B1.
187. *Id.*

won't use technology they don't trust."[188] Of course, the technology companies are part of the problem because they collect so much personal information about people, and the government simply seeks to access that information.[189] Nevertheless, the technology companies push for greater transparency regarding the government's surveillance program is likely to succeed.[190] They achieved some success in a recent settlement with the NSA which provided that electronic communications companies could publicly reveal some surveillance data.[191]

188. *Id.* at B5 (Quoting Mr. Brad Smith, Microsoft's General Counsel).
189. *Id.* at B5.
190. *Id.*
191. *See* Alexei Alexis, *DOJ Gives Web E-Giants Nod to Publish Surveillance Data*, Privacy & Data Security Law Resource Center (Jan. 27, 2014).