GUILTY BY ASSOCIATION: SMALL-WORLD PROBLEM EMPHASIZES CRITICAL NEED FOR BUSINESS STRATEGIES IN RESPONSE TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

Carol M. Bast[*] *and Cynthia A. Brown*[**†]

2014 MICH. ST. L. REV. 1035

TABLE OF CONTENTS

INTRODUCTION....1036
I. MILGRAM'S SMALL-WORLD PROBLEM AND THE SIX DEGREES OF SEPARATION PHENOMENON....1039
II. THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)....1048
A. The Road to FISA....1048
B. Foreign Intelligence Surveillance Act (FISA)....1055
1. *The Church Committee*....1056
2. *Enacting FISA*....1057
C. Electronic Communications Privacy Act of 1986....1062
D. The USA PATRIOT Act and Recent Amendments to FISA....1065
III. CURRENT STATE OF DOMESTIC SURVEILLANCE....1071
A. The Terrorist Surveillance Program....1079
B. The Protect America Act....1081
C. The National Security Agency and Edward Snowden....1083
IV. LARGE WORLD BUSINESS CONSEQUENCES....1091
A. Business-Records Requests....1094
B. National-Security Letters....1097
C. Small-World Theory....1104
V. LESSONS LEARNED....1108
A. Data Breaches....1109
B. Business-Security Planning....1112
C. Chief Privacy Officer....1117
D. Employees....1119

* Associate Professor of Legal Studies, Department of Legal Studies, University of Central Florida, Orlando, Florida 32816.

** Cynthia A. Brown, J.D., Ph.D., is in an attorney in private practice with the law firm of Brown and Associates, PLLC.

† These authors contributed equally to this work.

E. Other Proactive Steps.....1123
CONCLUSION 1127

INTRODUCTION

Indifferent might have once best described the response of business owners upon hearing about the National Security Agency (NSA), the Foreign Intelligence Surveillance Act (FISA),[1] or the Department of Justice's "National Security Letter[s]" (NSLs).[2] If questioned about FISA, or NSLs, the majority of business leaders and their attorneys would have acknowledged a lack of familiarity with these chapters in the annals of federal legislation, and historically, little reason existed for them to have even the briefest exposure to this body of law.[3] It is doubtful that either of these security tools associated with foreign-intelligence surveillance and the prevention of terrorist activity would have alerted further inquiry by the commercial sector, even had they garnered the attention of a business owner or her counsel.[4] Consequently, a meager few of the country's business leaders or their legal counsel were apt to include NSA surveillance, FISA, or NSLs in the company's cache of considerations when contemplating potential risks and exposure.[5]

As is true of most aspects of American government, September 11, 2001 changed things, and domestic surveillance is no exception.[6] FISA, NSLs, business-records requests, and other NSA surveillance in the name of national security are all matters now quite relevant to the American business owner.[7] In fact, FISA's broad, unfettered application since 9/11 and Congress's expansive amendments to it suggest a new and amplified dedication is warranted that entreats businesses to engage in a focused examination of this law and its prescription for, not proscription of, surreptitious surveillance of domestic commercial activities.[8] Likewise, NSLs are a second governmental power, similar to FISA's business-records requests, that were significantly enlarged with the adoption of the USA

1. 50 U.S.C. §§ 1801-1885c (2012).
2. *See* 18 U.S.C. §§ 2709, 3511(d)(1) (2012).
3. *See infra* Part IV.
4. *See infra* Part IV.
5. *See infra* Part IV.
6. *See infra* Section II.D.
7. *See infra* Part IV.
8. *See infra* Section IV.A.

PATRIOT Act (Patriot Act)[9] and are of new import to businesses.[10] The statutory expansion of NSL authority enables the Federal Bureau of Investigation (FBI) and other federal agencies to issue "demand letters" with no court oversight directing commercial recipients to provide information that may include a host of customer-specific information and more.[11] Some reports indicate that since the enactment of the Patriot Act there have been more than 140,000 NSL applications, involving more than 50,000 United States persons.[12] Together, FISA, including its business-records requests, and NSLs punctuate an acute need for increased awareness of the possible business implications of these national-security laws.

Need, however, escalates to something much more akin to demand when today's business interactions are viewed through the lens of the network theory "small-world" problem.[13] Information accumulated through NSA surveillance, FISA, and NSLs dramatically multiplies how much information the government knows about domestic businesses, business owners, their customers and clients, their interactions, and the networks they create.[14] Conversely, the businesses themselves may be unaware of much of what the government knows, and more particularly, the businesses most likely lack any meaningful knowledge of the far-reaching effects of their surface interactions and the networks those interactions generate. Business networks are of great interest to the government's national-security concerns and squarely within their monitoring objectives.[15] Business owners, however, have been largely unaware of the government's efforts and oblivious of the heightened potential for unintended consequences wrought by their businesses' invisible network of acquaintances, colleagues, and friends.

If Stanley Milgram is correct, the average network of acquaintances that connect any of us numbers no more than six.[16] Hardly any of us, however, are cognizant of the numerous networks

9. USA PATRIOT Act, Pub. L. No. 107-56, §§ 201-25, 115 Stat. 272, 278-96 (2001).

10. *See infra* Section IV.B.

11. *See infra* notes 452-68 and accompanying text.

12. *Foreign Intelligence Surveillance Act Court Orders 1979-2014*, ELECTRONIC PRIVACY INFO. CENTER (May 1, 2014), http://epic.org/privacy/wiretap/stats/fisa_stats.html.

13. *See infra* Part I.

14. *See infra* Part I; *see also infra* Part V.

15. *See infra* Part I.

16. *See infra* notes 26-36 and accompanying text.

we create or of which we may be a member.[17] More particularly, we also do not know exactly who is included within our networks.[18] Notwithstanding our own lack of awareness and, perhaps, interest, the networks created through our acquaintance links are receiving a great deal of scholarly attention, and in the wake of 9/11, scholars are not alone.[19] The nation's executive branch, inclusive of federal law enforcement and intelligence agencies, has developed a particularly heightened curiosity in our networks and has evidenced an intensified attentiveness.[20]

Shortly following the twelfth anniversary of September 11, 2001, this Article examines the implications of the terrorists' attacks for American business owners by considering federal domestic-surveillance strategies in light of Milgram's small-world theory and the associated concept of "six degrees of separation."[21] In many respects, the focus is one of risk management, and this Article presents potential new hazards posed by contemporary business interactions, given the latitude FISA and NSLs confer upon American law enforcement agencies.

This Article proposes that the invisible social networks created by employees and business owners may inadvertently position a business and its principals as federal-surveillance targets and the subjects of *permissible* surreptitious wiretapping, eavesdropping, and "sneak and peek" searches.[22] In addition to increased surveillance, business owners and businesses are more prone than ever to receive federal warrantless requests for sensitive information about employees, clients, and customers. Because the legislation does not require disclosure, the business principals who become surveillance targets may never know or learn of the government's monitoring of telephone calls and electronic data.[23] Further, should a business receive NSL requests for information, not only must the business

17. *See infra* note 27 and accompanying text.
18. *See infra* note 27 and accompanying text.
19. *See infra* Section II.D.
20. *See infra* notes 53-65 and accompanying text.
21. *See infra* note 29.
22. A sneak and peak search is a surreptitious entry search that allows "officers to secretly enter, either physically or virtually; conduct a search, observe, take measurements, conduct examinations, smell, take pictures, copy documents, download or transmit computer files, and the like; and depart without taking any tangible evidence or leaving notice of their presence." CHARLES DOYLE, CONG. RESEARCH SERV., RL31377, THE USA PATRIOT ACT: A LEGAL ANALYSIS 62-63 (2002).
23. *See infra* note 452.

comply, but the NSL gagging provision also forbids recipients from disclosing to anyone other than their attorney the government's demand for records.[24] Further still, an employee who becomes the recipient of an NSL request for business records may also be prohibited from revealing the government's request—even to her superiors or the business's owners.[25]

In many ways, post-9/11 national-security efforts are viewed as contributing to the creation of a climate of fear influencing zealous prosecutors and law enforcement officers to see mirages of treasonous conduct by American businesses and thus expanding the number of business-surveillance targets. Routine business-networking and business-development efforts, especially in a burgeoning global economy, could be leading to commercial relationships that place an increased number of American businesses on the government's list of terrorism suspects and squarely within the crosshairs of law enforcement's surreptitious surveillance efforts. As our small world continues to shrink, so does the probability that an American business owner may unwittingly find herself to be a federal surveillance target.

Part I of this Article reviews Milgram's small-world experiment and the NSA study of social networks. Part II presents the FISA legislation and a synopsis of its thirty-five-year evolution. Incorporated here is a comparison of other federal legislation that governs domestic-surveillance procedures. Part III reviews the state of domestic surveillance following 9/11. Part IV considers the potential implications FISA has on American commercial enterprises and urges businesses to recognize the acute need to consider the potential for unintended consequences. Part V suggests proactive measures that businesses should consider.

I. MILGRAM'S SMALL-WORLD PROBLEM AND THE SIX DEGREES OF SEPARATION PHENOMENON

The inaugural social science study of human connectivity is the result of a Harvard social psychologist named Stanley Milgram. Milgram designed the classic experiment that would demonstrate how closely linked earth's inhabitants might be.[26] He named his

24. *See infra* note 452.
25. *See infra* note 452.
26. Stanley Milgram, *The Small-World Problem*, 1 PSYCHOL. TODAY 61, 67 (1967).

study the "Small-World Problem" after the cliché response of strangers who unexpectedly discover they share an acquaintance.[27] Milgram's work provided the initial empirical evidence supporting the theory that any individual may be connected to any other through a short chain of social ties.[28] The small-world experiment received a great deal of attention among academic circles across multiple disciplines, but it would take nearly a quarter of a century and John Guare's play entitled *Six Degrees of Separation*[29] before Milgram's concept fully escaped the bounds of academia and achieved the popular prominence it now holds.

In Milgram's studies, Kansas and Nebraska residents, the "start[ers]," received a packet and the identity of a person in Massachusetts who would serve as the "target" recipient of the packet.[30] The participants received the charge to begin a chain by mailing the packet towards the target, but they were restricted to sending the packet only to individuals they knew on a first-name basis.[31] After receiving the packet, that friend would then repeat the process.[32] Each recipient of the packet would continue the chain by serving as a "degree" or "intermediary" along the packet's path.[33] The total number of intermediaries required to complete the chain and to successfully deliver the packet to the target represented the number of degrees that separated the starter from the Massachusetts target.[34] To maintain a record of the intermediaries in each chain, Milgram instructed each person who received the packet and who then forwarded it to a friend to also mail a business reply or "tracer" card back to Milgram at Harvard University.[35]

Milgram's Kansas and Nebraska studies of social connections revealed that the participants were separated, on average, by six degrees (meaning five intermediaries).[36] In May 1967, Milgram first published the results from his human connectivity experiments in Kansas and Nebraska, studies he referred to as "acquaintance chain[s],"[37] in the premiere issue of *Psychology Today*.

27. *Id.* at 61; *see infra* notes 511-17 and accompanying text.
28. *See* Milgram, *supra* note 26, at 62-63, 67.
29. JOHN GUARE, SIX DEGREES OF SEPARATION: A PLAY (1990).
30. Milgram, *supra* note 26, at 63-64.
31. *Id.* at 64.
32. *Id.*
33. *Id.* at 65.
34. *Id.*
35. *Id.* at 63-64.
36. *Id.* at 65.
37. *Id.* at 62.

In the parlance of network theory, a network such as the social network studied by Milgram is made up of nodes and links.[38] The nodes are the people and entities comprising the network, and the links are the relationships between the nodes.[39] Traversing one link between two nodes is one "hop."[40] A link can be categorized as a "strong tie," a relationship with high intensity, or as a "weak tie," a relationship with low intensity.[41] An example of a strong tie might be a business partner with whom one consults several times a day during the work week, whereas an example of a weak tie might be a customer with whom the business has contact on a very infrequent basis.[42] Some nodes, the "supernodes" or "hubs," may be extremely active in frequently transmitting information to numerous nodes, while some nodes, the "peripherals," have a low level of connectivity to a much fewer number of nodes and transmit information on a much less frequent basis.[43] The office of the chief operating officer is usually a supernode, actively providing information to and receiving information from all of the business divisions. In contrast, a lower-level researcher might be a peripheral, providing research results to a supervisor and very rarely communicating with others in the division or other divisions of the business.

The nodes typically are clustered, with many links among nodes within a cluster and fewer links between clusters or even structural holes between clusters.[44] For example, each business division might be a cluster with many links among division employees, especially if the division is a closely knit one, and a fewer number of ties between that division and other divisions of the business. A particular business division may rarely communicate with other business divisions.[45] A social network is dynamic, with a structure that changes over time or whose function varies depending on the type of information transmitted.[46] For example, "[w]hen the information at issue is highly sensitive, perhaps because it reflects illegal or politically disfavored motivations, network members will

38. Peter J. Denning, *Network Laws*, 47 COMM. ACM 15, 15 (2004).
39. *Id.*
40. *Id.*
41. Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 953 (2005).
42. *See id.*
43. *Id.* at 948.
44. *Id.* at 951-52, 954-55.
45. Denning, *supra* note 38, at 15.
46. Strahilevitz, *supra* note 41, at 951.

have to be quite cautious about sharing information. In such circumstances, weak ties may become totally inactive, as individuals begin sharing information only with well-trusted associates."[47]

When Milgram asked sophisticated audiences to guess the number of personal acquaintances required to link any two randomly selected individuals, it is not surprising that most guessed numbers in the hundreds.[48] It was difficult for any of them to imagine that the number of hops between the two could actually be as low as six, and today, perhaps even lower.[49] The fact is that the number of potential network clusters participated in by each of our acquaintances and the weak ties that may link those clusters with other clusters introduces structural complexity that makes "knowing" the network clusters to which the various clusters in which we operate are weakly linked improbable, if not wholly impossible.[50] We may be cognizant of our strong ties with other nodes because we have so much in common with those nodes and correspond with them regularly, while the weak ties escape our notice because we have little connection with them, and the type of information transmitted may be very distinct from that communicated across strong ties. However, weak ties are important because they function as bridges across which information is transferred from one cluster to another.[51] Limiting information flow to strong ties might produce stagnancy of knowledge, whereas being well informed requires the cross-pollination produced by information traversing weak ties.[52]

The government's intelligence-gathering technology and legislatively expanded authority to utilize its technology with limited constraints allow the executive branch access to information about our networks that even we, as individuals, do not have, and American businesses are not exempt in any respect. A business's networks, as well as the connections, both personal and professional, created by its employees fall soundly within the government's desire to know. Although the government has had access to these networks, the American public has only gained knowledge of some of the

47. *Id.* at 959.
48. Milgram, *supra* note 26, at 65.
49. *Id.*
50. *See id.* at 66-67.
51. Strahilevitz, *supra* note 41, at 955.
52. *Id.* at 954-57.

government methods of mass surveillance in the aftermath of the June 2013 Edward Snowden disclosures.[53]

As revealed with the Snowden disclosures, the federal government has been doing its own study of social networks using telephone metadata produced under § 215 of the Patriot Act.[54] The study begins with a query of information, such as a telephone number, known to be associated with a targeted foreign terrorist organization.[55] This telephone number, the "seed," is used as a starting point for the study,[56] with the possibility of expanding investigation to as much as three hops from the target.[57] This means

---

53. Ewen MacAskill, *Edward Snowden: How the Spy Story of the Age Leaked Out*, GUARDIAN (June 11, 2013), http://www.theguardian.com/world/2013/jun/11/edward-snowden-nsa-whistleblower-profile?guni=Article:in%20body%20link.

54. On August 9, 2013, the United States Department of Justice released an Administration White Paper that provides information on the method used to query the telephone metadata produced under § 215 of the Patriot Act. ADMINISTRATION WHITE PAPER: BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT 1 (2013) [hereinafter WHITE PAPER], *available at* http://s3.documentcloud.org/documents/750210/administration-white-paper-section-215.pdf. In addition, the government has been using information garnered through NSLs under § 505 of the Patriot Act to study social networks. *See infra* Section IV.B.

55. *See* WHITE PAPER, *supra* note 54, at 3.

56. The process begins with one piece of information that can be queried:

> Under the FISC orders authorizing the collection, authorized queries may only begin with an "identifier," such as a telephone number, that is associated with one of the foreign terrorist organizations that was previously identified to and approved by the Court. An identifier used to commence a query of the data is referred to as a "seed." Specifically, under Court-approved rules applicable to the program, there must be a "reasonable, articulable suspicion" that a seed identifier used to query the data for foreign-intelligence purposes is associated with a particular foreign terrorist organization.

Id.

57. The government collects information within "two or three hops" from a suspected terrorist target. Philip Bump, *The NSA Admits It Analyzes More People's Data than Previously Revealed*, WIRE (July 17, 2013, 12:35 PM), http://www.theatlanticwire.com/politics/2013/07/nsa-admits-it-analyzes-more-peoples-data-previously-revealed/67287/ (internal quotation marks omitted). The White Paper explains how this is accomplished:

> Under the FISC's order, the NSA may also obtain information concerning second and third-tier contacts of the identifier (also referred to as "hops"). The first "hop" refers to the set of numbers directly in contact with the seed identifier. The second "hop" refers to the set of numbers found to be in direct contact with the first "hop" numbers, and the third "hop" refers to the set of numbers found to be in direct contact with the second "hop" numbers. Following the trail in this fashion allows focused inquiries on

that the government can begin with a target, take one hop to those with whom the target has connected (a first connection), take a second hop to those with whom the first connections have connected (a second connection), and, finally, take a third hop to those with whom the second connections have connected (a third connection). Sometimes the connections between hops are strong, such as a connection with a close relative or friend, but many times the connection is simply a connection, meaning that the bond between the two individuals was weak to the point of almost being nonexistent. The reach of the government's collection within three hops of a target is extremely significant. As described in the following paragraphs, the government has several methods of constructing models of social networks.

Since November 2010, the NSA has been permitted to paint pictures of the activities of individuals and entities by performing "large-scale graph analysis on very large sets of communications metadata without having to check foreignness" of information in phone call and email logs.[58] Although metadata does not contain the content of telephone calls and email correspondence, it does provide the time when the contacts began, the duration of the contacts, the location of the contacts, and the telephone number or email address of the contacts.[59] In addition, NSA can enrich the "contact chain" by correlating metadata with other information available from third parties, "including bank codes, insurance information, Facebook profiles, passenger manifests, voter registration rolls and GPS location information, as well as property records and unspecified tax data."[60] As described in the following paragraphs, the NSA has gained access to more than just telephone metadata.

The location of one's cellphone can be used by the government to study social networks, as the devices of more than 90% of cellphone users worldwide are located in close proximity to them

---

numbers of interest, thus potentially revealing a contact at the second or third "hop" from the seed telephone number that connects to a different terrorist-associated telephone number already known to the analyst.

WHITE PAPER, *supra* note 54, at 3-4.

58. James Risen & Laura Poitras, *N.S.A. Examines Social Networks of U.S. Citizens Using Giant Databases*, N.Y. TIMES, Sept. 29, 2013, at 1 (internal quotation marks omitted).

59. WHITE PAPER, *supra* note 54, at 3.

60. Risen & Poitras, *supra* note 58, at 1, 22.

throughout the day.[61] The NSA gathers cellphone location information by tapping into cables connecting communications networks worldwide.[62] While gathering location information on foreign targets, the NSA may incidentally gather location information on the cellphones of United States citizens.[63] The location information can be used to track the path of a target and show the relationship of the target with others whose paths cross that of the target, whether a single instance or a recurring basis, or others who travel in tandem with the target.[64] In 2012, Justice Sotomayor noted the intrusiveness of the collection of location information alone, without even considering adding other metadata or third-party data to the mix: "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[65]

Thus, the NSA can employ telephone metadata and location information to diagram social networks. As described below, the NSA has additional methods of collecting information showing linkages among individuals and businesses comprising social networks.

The NSA collects contact-list information from email and instant-messenger users as email and messages pass through Internet switches located outside the United States.[66] This collection method allowed the NSA access to "444,743 e-mail address books from Yahoo, 105,068 from Hotmail, 82,857 from Facebook, 33,697 from Gmail and 22,881 from unspecified other providers" in a single twenty-four hour period.[67] Although the interception occurs outside

---

61. ERIC SCHMIDT & JARED COHEN, THE NEW DIGITAL AGE: RESHAPING THE FUTURE OF PEOPLE, NATIONS AND BUSINESS 172 (2013).

62. Barton Gellman & Ashkan Soltani, *NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show*, WASH. POST (Dec. 4, 2013), http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html.

63. *Id.*

64. *Id.*

65. United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring).

66. Barton Gellman & Ashkan Soltani, *NSA Collects Millions of E-mail Address Books Globally*, WASH. POST (Oct. 14, 2013), http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html.

67. *Id.*

the United States, the contact information collected is not limited to that of users other than United States citizens, as a digital message may take a circuitous global route even if traveling between two points in the United States, and a sizeable number of United States citizens live outside the United States.[68] The contact list information is another tool that the NSA has to map the many connections between individuals and entities, be they professional, social, organizational, personal, or intimate; the interceptions may include personal information on a user's contacts such as names, addresses, telephone numbers, and email addresses, as well as business and familial relationships.[69] At the same time, the contact list information may yield false positives by allowing the NSA to hypothesize about a connection, even if the connection was not brought to fruition or is not ongoing.[70]

In October 2013, it was revealed[71] that the NSA, together with the British intelligence agency Government Communications Headquarters, tapped the fiber-optic cables connecting the data centers of Google and Yahoo.[72] This is a significant feat because of the safeguards built into the data systems of those companies.[73] "To guard against data loss and system slowdowns, Google and Yahoo maintain [fortress-like] data centers across four continents and connect them with thousands of miles of fiber-optic cable."[74] These globe-spanning networks, representing billions of dollars of investment, are known as *clouds* because data moves seamlessly around them.[75] The data flowing on the cables includes both archived and newer information.[76] "For the data centers to operate effectively, they synchronize [high] volumes of information about account holders. Yahoo's internal network, for example, sometimes transmits

68. *Id.*
69. *See id.*
70. *Id.*
71. Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, WASH. POST (Oct. 30, 2013), http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html; Charlie Savage, Claire Cain Miller & Nicole Perlroth, *N.S.A. Said to Tap Google and Yahoo Abroad*, N.Y. TIMES, Oct. 31, 2013, at B1.
72. Savage, Miller & Perlroth, *supra* note 71.
73. Gellman & Soltani, *supra* note 71.
74. *Id.*
75. *Id.*
76. *Id.*

entire e-mail archives—years of messages and attachments—from one data center to another."[77]

This program, referred to as Muscular, copies the data flowing through the cables outside the United States and routes the data into a buffer capable of storing three to five days of data.[78] The data can be decoded, to make the companies' data formats accessible, and filtered, to separate out the potentially useful data.[79] NSA can suggest 100,000 search terms, or *selectors*, to mine the data collected.[80] The data flowing through the cables can include "email, online document and photo storage and search queries."[81] Through this program, NSA gains access to information transmitted by unsuspecting Yahoo and Google users.[82] "NSA's acquisitions directorate sends millions of records every day from . . . Yahoo and Google [internal] networks to data warehouses at the agency's [Fort Meade headquarters]."[83]

United States executive branch officials have provided the NSA with telephone numbers of foreign politicians at the urging of the NSA; in addition, some officials volunteered such numbers.[84] "In one recent case, . . . a US official provided NSA with 200 phone numbers to 35 world leaders."[85] This information became public in the wake of German chancellor Angela Merkel calling President Obama to question him as to whether the United States had conducted surveillance on her mobile telephone and reports that the NSA had targeted European Union senior officials.[86] Thus, the NSA may be able to monitor the communications of other senior officials. "Despite the fact that the majority is probably available via open source, the PCs [intelligence production centers] have noted 43 previously unknown phone numbers. These numbers plus several others have been tasked."[87] À la the Milgram study, the NSA may use the numbers provided to build a chain of connections that can be

77. *Id.*
78. *Id.*
79. *Id.*
80. *Id.*
81. Savage, Miller & Perlroth, *supra* note 71, at B6.
82. Gellman & Soltani, *supra* note 71.
83. *Id.*
84. James Ball, *NSA Monitored Calls of 35 World Leaders After US Official Handed Over Contacts*, GUARDIAN (Oct. 24, 2013), http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls.
85. *Id.* (internal quotation marks omitted).
86. *Id.*
87. *Id.* (internal quotation marks omitted).

monitored. "These numbers have provided lead information to other numbers that have subsequently been tasked."[88]

Our own cognitive limitations, not to mention time constraints and everyday obligations, are factors that hamper what we know about the many network clusters we populate and the people who occupy them with us. This void in knowledge serves, in fact, as the impetus for the premise of this Article. The notable paradox of Milgram's small-world effect is that individuals perceive that they live in a large world of restricted social connectedness, almost always oblivious to the greater probability of connectedness that exists. Today, however, through a process of mutual social mapping and networking tools, our connections are largely determinable. In fact, this paradox and the value of examining the small-world networks we create within the larger world have not escaped the scrutiny of federal authorities. Their keen desire to fully understand our connections, even if we remain indifferent to them, is one catalyst for the creation of surveillance tools that facilitate their understanding. Thus, with social connection mapping using information available from third parties and intelligence gathering tools, such as NSLs, business-records requests, and FISA, all presently available to federal authorities, their knowing is made much easier.

In putting together the puzzle of the reach of government surveillance into the affairs of individuals and businesses, it is helpful to have a background on the development of the legal relationship between the United States government and those who might be subject to government surveillance. As the following Part indicates, over the nation's history there has been an ebb and flow in the legal basis and the practical reality of government intrusion into what one might think to be private.

II. THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (FISA)

A. The Road to FISA

By 1844, wire communications offered new mechanisms of communicative exchange and new issues for privacy advocates. Because wiretaps provided a means for officers to gain critical information about criminals without risking confrontation,

88. *Id.* (internal quotation marks omitted).

recognition of the value of wire surveillance was immediate, and wiretapping by the country's executive branch was born.[89]

Early in the twentieth century, in *Olmstead v. United States*[90] the United States Supreme Court applied a very literal interpretation of the Constitution in denying protection against surreptitious eavesdropping by the executive branch.[91] Writing for the five–four majority, Chief Justice Taft opined that voluntary telephone conversations secretly overheard did not equate to "material things" that could be seized.[92] The Court's property-oriented perspective of Fourth Amendment rights was rooted in the reasoning that there could be no physical intrusion when the parties to the telephone conversation intentionally projected their words outside their homes.[93] *Olmstead* vested control of electronic surveillance within the discretion of the executive branch and shielded the intelligence-gathering technique from Fourth Amendment scrutiny for nearly forty years.[94]

In 1967, nearly four decades after *Olmstead*, the Supreme Court accepted the opportunity to address the constitutional concerns surrounding warrantless electronic surveillance.[95] The Court measured the validity of surveillance in terms of privacy expectations rather than property interests and, overruling *Olmstead*, decisively changed surveillance law in the United States.[96] In the landmark case, *Katz v. United States*,[97] the Court abandoned the requirement of physical trespass as a prelude to invoking Fourth

---

89. GINA STEVENS & CHARLES DOYLE, CONG. RESEARCH SERV., 98-326, PRIVACY: AN OVERVIEW OF FEDERAL STATUTES GOVERNING WIRETAPPING AND ELECTRONIC EAVESDROPPING 2 (2012).

90. 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347, 353 (1967).

91. *Id.* at 466.

92. *Id.* at 464.

93. *Id.* at 464-66; *see also* Americo R. Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. PA. L. REV. 793, 795-96 (1989).

94. Cinquegrana, *supra* note 93, at 796-800.

95. *Katz*, 389 U.S. at 347, 353 (overruling *Olmstead*). The Supreme Court reversed a gambling conviction when the government, without prior judicial authority, employed an electronic listening and recording device outside of a telephone booth used by Katz to take and place bets. *Id.* at 348, 359. The Court reversed a finding of guilt because it found that the government's use of warrantless electronic surveillance was a violation of the defendant's Fourth Amendment rights. *Id.* at 358-59.

96. *Id.* at 353.

97. *Id.* at 347.

Amendment protection, heralding a victory for privacy.[98] It also created a presumption against warrantless electronic surveillance when it ruled that wiretaps were sufficiently intrusive to implicate Fourth Amendment concern.[99]

The *Katz* ruling accomplished two significant achievements. First, Justice Stewart's majority opinion established that electronic surveillance constitutes a "search" for the purposes of the Fourth Amendment by shifting the focus of Fourth Amendment protection from places to people.[100] The decision prohibited the government from conducting electronic surveillance without both a showing of probable cause and a warrant issued by a neutral and detached magistrate.[101] Secondly, Justice Harlan's concurrence established "reasonable expectation of privacy" as the doctrinal test for determining when a probable-cause warrant would be required under the Fourth Amendment.[102] "Since [*Katz*], the touchstone of [Fourth] Amendment analysis has been . . . whether a person has a 'constitutionally protected reasonable expectation of privacy'" in the area searched or the thing seized.[103]

Acknowledging law enforcement limits of electronic surveillance, the *Katz* Court also questioned for the first time the executive branch's established practice of conducting warrantless electronic surveillance for the purpose of national security.[104] However, in a very controversial footnote the Court expressly avoided requiring judicial authorization of surveillance in matters

98. *Id.* at 352-53.

99. *Id.* at 356-57.

100. *Id.* at 351, 356-57. Justice Stewart reasoned:

> [T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.

Id. at 351 (internal citations omitted).

101. *Id.* at 355-56.

102. *Id.* at 360-61 (Harlan, J., concurring). Justice Harlan deduced "the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" *Id.* at 361; *see* Kyllo v. United States, 533 U.S. 27, 32-33 (2001); California v. Ciraolo, 476 U.S. 207, 211 (1986).

103. Oliver v. United States, 466 U.S. 170, 177 (1984) (quoting *Katz*, 389 U.S. at 360).

104. 389 U.S. at 358 n.23 (majority opinion).

involving national security.[105] Notably, the decision specifically recognized a distinction between law-enforcement and national-security requirements for electronic surveillance.[106]

Justice Douglas and Justice Brennan concurred with the *Katz* result, but both rejected a national-security exception to the Fourth Amendment's protections.[107] Justice Douglas suggested that such an exception would convey a "green light for the Executive Branch to resort to electronic eavesdropping without a warrant in cases which the Executive Branch itself labels 'national security' matters."[108] Justice Douglas reasoned that "when the President and Attorney General assume both the position of adversary-and-prosecutor and disinterested, neutral magistrate" the Fourth Amendment rights of national-security suspects could not be assured.[109] Justice Douglas argued that it was the judicial branch rather than the executive branch that must serve as the neutral and disinterested party mediating between the needs of law enforcement and the individuals targeted for surveillance.[110]

The lack of consensus on the Court concerning electronic surveillance and national security highlighted concerns of "the efficacy of self-imposed regulation and restraint as a safeguard against executive abuse."[111] The Court deliberately left questions unanswered and, consequently, delivered the opinion absent additional guidance for the executive branch.[112] The decision would, however, eventually provide direction to Congress and would serve as the impetus for subsequent congressional action addressing electronic-surveillance requirements.[113]

In 1968, the legislative branch tackled questions presented by the use of wiretapping and other forms of electronic surveillance, and the procedural distinction between law enforcement and national

105. *Id.* "Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case." *Id.*

106. *Id.*

107. *Id.* at 359-60 (Douglas, J., concurring).

108. *Id.* at 359.

109. *Id.* at 360.

110. *Id.* at 359-60.

111. Elizabeth Gillingham Daily, Comment, *Beyond "Persons, Houses, Papers and Effects": Rewriting the Fourth Amendment for National Security Surveillance*, 10 LEWIS & CLARK L. REV. 641, 647 (2006).

112. *Id.*

113. *Id.* at 647-48.

security.[114] What resulted was comprehensive wiretapping and electronic-eavesdropping legislation that established uniform guidelines through which law enforcement officials could obtain judicial approval to accomplish electronic surveillance.[115] Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Title III) prohibited wiretapping and electronic eavesdropping unless federal and state law enforcement officers adhered to strict limitations, including establishing probable cause before conducting surveillance of wire or oral communication.[116]

Under Title III, wiretap orders were available only in the enforcement of enumerated serious crimes.[117] The statute mandated that government officials satisfy numerous protocols before applying for an order authorizing a wiretap.[118] One such requirement necessitated that applicants indicate that alternative investigative techniques had failed or were reasonably expected to fail.[119] In many respects, Title III's procedures were a heightened departure from the usual probable cause mandates employed for physical searches.[120] Its provisions applied to traditional criminal investigations and did not address the surveillance authority of the President. The statute would later undergo change and emerge anew as the Electronic Communications Privacy Act.[121]

Enacting Title III legislation demonstrated marked movement toward privacy protection by the United States Supreme Court and Congress. Both governmental branches, however, withdrew before addressing the executive branch's use of presidential authority to conduct warrantless electronic surveillance for national-security purposes.[122] While some argue the judicial and legislative branches refrained from regulating the executive branch out of deference, the inaction nevertheless perpetuated the President's continued

---

114. *Id.* at 647.

115. *Id.* at 647-48. *See* George P. Varghese, Comment, *A Sense of Purpose: The Role of Law Enforcement in Foreign Intelligence Surveillance*, 152 U. PA. L. REV. 385, 388-89 (2003).

116. Timothy Casey, *Electronic Surveillance and the Right to Be Secure*, 41 U.C. DAVIS L. REV. 977, 999 (2008) (citing 18 U.S.C. § 2518 (2000)).

117. 18 U.S.C. § 2516.

118. *Id.* § 2518.

119. *Id.* § 2518(1)(c).

120. *See* Casey, *supra* note 116, at 999-1000.

121. The new legislation is discussed later in this Article. *See infra* Section II.C.

122. Cinquegrana, *supra* note 93, at 801.

surveillance without judicial oversight.[123] In 1972, the United States Supreme Court granted appellate review in *United States v. United States District Court*, often referenced as *Keith*, on the narrow issue of whether Fourth Amendment protection applied in surveillance questions involving domestic security.[124]

The *Keith* case, named for the district court judge, revealed that the government had conducted warrantless electronic surveillance of the defendants.[125] When the defendants objected and sought to have the government disclose the evidence collected, the government argued that the surveillance was essential "'to gather intelligence information deemed necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government.'"[126] Further, the government insisted the surveillance was lawful under the national-security exception to the Fourth Amendment and was not subject to disclosure.[127] Contrary to the government's efforts, the trial court found in favor of the defendants and ruled that the government's surreptitious surveillance was a violation of the Fourth Amendment.[128]

Upon review, the Supreme Court scrutinized whether the executive branch possessed inherent constitutional authority to execute warrantless surveillance of domestic organizations for national-security purposes in contradiction of, or as an exception to, the Fourth Amendment.[129] The Court acknowledged that investigations undertaken in the name of national security potentially implicated both First and Fourth Amendment protections and posed "greater [constitutional] jeopardy" than cases involving ordinary crime.[130] Writing for a unanimous Court, Justice Powell concluded that responsibility rested with the Court to balance "the duty of Government to protect the domestic security, and the potential danger posed by unreasonable surveillance to individual privacy and free expression."[131]

---

123. *Id.*

124. 407 U.S. 297, 309 (1972). The case involved the criminal trial of individuals charged with bombing a CIA office in Ann Arbor, Michigan. *Id.* at 299.

125. *Id.* at 299-301.

126. *Id.* at 300 (quoting Att'y Gen. Aff. 20).

127. *Id.* at 300-01 & n.2.

128. *Id.* at 301.

129. *Id.* at 299.

130. *Id.* at 313.

131. *Id.* at 299, 314-15. Eight of the nine Justices voted against the government. *Id.* at 297. Justice Rehnquist did not participate in the discussions or the decision, "presumably because he had worked on the wiretap issue when he served

Adopting Justice Douglas's rationale in *Katz*, the Court warned of

> the tendency of Government—however benevolent and benign its motives—to view with suspicion those who most fervently dispute its policies. Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect "domestic security." Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent.[132]

In the end, the Court found that the President's authority was insufficient to excuse warrantless electronic surveillance of purely domestic threats to national security.[133] Recognizing that the potential for abuse was too great and the rights protected were so fundamental, the Court ruled that, in intelligence-gathering investigations involving surveillance of domestic organizations, the Fourth Amendment required the executive branch to demonstrate probable cause of criminal wrongdoing and to seek judicial

---

as head of the Office of Legal Counsel in the Nixon Justice Department" and publicly supported the government's position. *See* Tracey Maclin, *The Bush Administration's Terrorist Surveillance Program and the Fourth Amendment's Warrant Requirement: Lessons from Justice Powell and the* Keith *Case*, 41 U.C. DAVIS L. REV. 1259, 1264 & n.14 (2008).

132. *Keith*, 407 U.S. at 314. See also James Madison's correspondence to Thomas Jefferson in 1798 at the height of the quasi-war against France in which he penned:

> The management of foreign relations appears to be the most susceptible of abuse, of all the trusts committed to a Government, because they can be concealed or disclosed, or disclosed in such parts and at such times as will best suit particular views; and because the body of the people are less capable of judging, and are more under the influence of prejudices, on that branch of their affairs, than of any other. Perhaps it is a universal truth that the loss of liberty at home is to be charged to provisions against danger, real or pretended, from abroad.

Letter from James Madison to Thomas Jefferson (May 13, 1798), *in* 2 LETTERS AND OTHER WRITINGS OF JAMES MADISON 140-41 (Philadelphia, J.B. Lippincott & Co. 1865).

133. *Keith*, 407 U.S. at 308, 314-15. The Court's decision was particularly startling in light of the fact that four of the Justices were new Nixon appointees considered to be sympathetic to the President's position on wiretapping. *See* Maclin, *supra* note 131, at 1264. Furthermore, Justice Powell had authored a controversial op-ed article supporting wiretapping in national security cases just months prior to the *Keith* decision. *Id.* Consequently, his authoring the *Keith* decision rejecting the government's claim makes the decision all the more astonishing. *Id.*

authorization prior to conducting electronic surveillance.[134] The Court emphasized that its decision did not extend to surveillance involving foreign powers or their agents and in so doing, created a distinction between domestic and foreign-intelligence surveillance that did not previously exist.[135] For the Court, Justice Powell urged Congress to develop legislation codifying standards for national-security surveillance that distinguished it from the criminal surveillance governed by Title III.[136]

B. Foreign Intelligence Surveillance Act (FISA)[137]

Following *Keith*, confusion abounded concerning national-security surveillance,[138] the Fourth Amendment, and the executive branch's authority to conduct warrantless surveillance to inform national-security efforts.[139] Warrantless electronic surveillance conducted by the executive branch had been ongoing for over fifty years when the Supreme Court delivered the *Keith* decision, but the ruling seemed to have little impact on the President's ongoing

134. *Keith*, 407 U.S. at 320.

135. *Id.* at 322 & n.20.

136. *Id.* at 321-24, 322 n.20.

137. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified at 50 U.S.C. §§ 1801-1885c (2012)).

138. It is helpful for one to have some knowledge of the manner in which conversations are monitored to understand government surveillance. Conversations are secretly monitored through what may be referred to as either "targeted surveillance" or "trawling surveillance." CTR. ON LAW & SEC., FOR THE RECORD, THE NSA WIRETAPPING PROGRAM 7 (2007), *available at* http://www.lawandsecurity.org/Portals/0/Documents/NSA_jan_07.pdf (internal quotation marks omitted). A targeted surveillance would be a wiretap monitoring the telephone number or conversations of a particular known terrorist, someone associated with a terrorist, or a suspected terrorist. *Id.* A computer facilitates trawling surveillance by screening the flow of a large body of telecommunications traffic to detect information, such as key words, that might indicate a connection to terrorism. *Id.* For the computer expert, data mining is simply "a relatively narrow process of using algorithms to discover predictive patterns in data sets"; applying those patterns to sift through a database to discover relevant evidence is "automated data analysis." MARY DEROSA, DATA MINING AND DATA ANALYSIS FOR COUNTERTERRORISM 3 (2004). However, the term data mining as used in this paper includes both processes.

139. *See generally* S. REP. NO. 95-604, at 1-15 (1978), *reprinted in* 1978 U.S.C.C.A.N. (1783 Stat.) 3904-17, *available at* http://www.cnss.org/data/files/Surveillance/FISA/Cmte_Reports_on_Original_Act/SJC_FISA_Report_95-604.pdf (describing history of national security surveillance and explaining the need for regulation).

warrantless-surveillance efforts at home and abroad.[140] Antagonism was brewing, if not boiling, in Congress over the executive branch's expansion of objectionable surveillance of American citizens.

1. *The Church Committee*

Congress reacted in 1975 by commissioning an investigation led by Senator Frank Church to examine executive abuses of electronic surveillance.[141] The Church Committee's inquiries uncovered staggering abuses of unregulated electronic surveillance of American citizens by the executive branch.[142] The committee uncovered far-ranging infringements of individual privacy interests, particularly surreptitious domestic surveillance of Americans who were not readily identifiable as sources of foreign-intelligence information.[143]

During a television interview, Senator Church stated:

> That capability at any time could 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. If this government ever became a tyranny, if a dictator ever took charge in this country, the technological capacity that the intelligence community has given the government could enable it to impose total tyranny, and there would be no way to fight back, because the most careful effort to combine together in resistance to the government, no matter how privately it was done, is within the reach of the government to know. Such is the capability of this technology . . . . I don't want to see this country ever go across 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.[144]

The committee's multi-volume report contained findings indicating that constituents of the executive branch, including the FBI and NSA, as well as other government agencies, had used

140. *See infra* note 143 and accompanying text.

141. S. REP. NO. 94-755, at iv-v (1976).

142. *See infra* note 152 and accompanying text.

143. S. REP. NO. 94-755, at 4-7.

144. Senator Frank Church, *Meet the Press* (NBC television broadcast Aug. 17, 1975), *quoted in* James Bamford, *They Know Much More Than You Think*, N.Y. REV. BOOKS (Aug. 15, 2013), http://www.nybooks.com/articles/archives/2013/aug/15/nsa-they-know-much-more-you-think/?pagination=false); *see also* IPA Media, *Frank Church Warns of Govt. Surveillance in 1975*, YOUTUBE (Aug. 8, 2013), http://www.youtube.com/watch?v=9DjJKYYb5-4, for a portion of Senator Church's statement.

perceived threats to national security as the justification to conduct warrantless surveillance targeting American citizens.[145] Disturbing revelations further proved that Americans became surveillance targets not because they were believed to be *real* threats to national security but because of the citizens' membership in certain groups.[146] According to the Church Committee, citizen targets "included political adherents of the right and the left, ranging from activist to casual supporters. Investigations have been directed against proponents of racial causes and women's rights, outspoken apostles of nonviolence and racial harmony; establishment politicians; religious groups; and advocates of new life styles."[147] Civil rights advocates, including Dr. Martin Luther King, Jr., were also popular surveillance targets.[148] In one year alone, the FBI conducted 65,000 domestic-intelligence investigations in utter disregard for the existing legal and constitutional constraints.[149]

In effect, the executive branch had exercised unilateral discretion absent any oversight to secretly select and monitor targets, often without any indication of their involvement in criminal activity.[150] Reporting that "[g]overnment officials—including those whose principal duty is to enforce the law—have violated or ignored the law over long periods of time and have advocated and defended their right to break the law,"[151] the Church Committee concluded:

> Too many people have been spied upon by too many Government agencies and [too] much information has been collected. The Government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts on behalf of a hostile foreign power.[152]

2. *Enacting FISA*

The Church Committee Report wrought a great public outcry, following closely on the heels of the uncertainty brought by the *Keith*

---

145. S. REP. NO. 94-755, at 5-6, 12; Beryl A. Howell & Dana J. Lesemann, *FISA's Fruits in Criminal Cases: An Opportunity for Improved Accountability*, 12 UCLA J. INT'L L. & FOREIGN AFF. 145, 149 (2007).

146. S. REP. NO. 94-755, at 6-9.

147. *Id.* at 7.

148. *Id.* at 7-8, 11-12.

149. *Id.* at 6.

150. *Id.* at 5-6; Howell & Lesemann, *supra* note 145, at 149.

151. S. REP. NO. 94-755, at 5.

152. *Id.*

decision.[153] Congress responded by addressing the executive branch's abuses and the Church Committee's recommendations with legislation.[154] FISA established "a procedure under which the Attorney General can obtain a judicial warrant authorizing the use of electronic surveillance in the United States for *foreign intelligence purposes*."[155] Through FISA, the legislative branch created a legal mechanism authorizing the executive branch to intercept communications of foreign powers,[156] but requiring intelligence agencies to obtain judicial authority in the form of a court order, not a warrant, for the domestic surveillance of Americans.[157] To safeguard the separation between foreign-intelligence surveillance and law-enforcement surveillance, Congress required certification by the Attorney General that "the purpose" of a proposed FISA surveillance was the gathering of foreign-intelligence information.[158]

Judicial oversight under FISA requires the justice department to obtain advance authorization from a congressionally created special court known as the Federal Intelligence Surveillance Court (FISC).[159] Originally, FISC was comprised of seven United States district judges appointed by the Chief Justice of the United States Supreme Court.[160] Later amendments adjusted the number of FISC judges to eleven to address the increased demand for FISA orders.[161]

---

153. Howell & Lesemann, *supra* note 145, at 149.

154. *Id.* at 149-50.

155. S. REP. NO. 95-604, at 5 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3906 (emphasis added), *available at* http://www.cnss.org/data/files/Surveillance/FISA/Cmte_Reports_on_Original_Act/SJC_FISA_Report_95-604.pdf.

156. The original bill's operative provision authorized a judge to "approv[e] electronic surveillance of a foreign power or an agent of a foreign power for the purpose of obtaining foreign intelligence information." *Foreign Intelligence Surveillance Act: Hearings Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice of the Comm. on the Judiciary*, 94th Cong. 3-4 (1976) (text of H.R. 12750, 94th Cong. § 2522 (1976)), *available at* http://www.cnss.org/data/files/Surveillance/FISA/1970s_Cong_Hearings/G_fisa041276_part_1a.pdf. That language remains unchanged. 50 U.S.C. § 1802(b) (2000).

157. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 102(b), 92 Stat. 1783, 1787-88 (1978) (codified at 50 U.S.C. §§ 1801-1885c).

158. 50 U.S.C. §§ 1804(a)(7)(B) (addressing electronic surveillance), 1823(a)(7)(B) (addressing physical evidence).

159. *Id.* § 1803(a), (b). Although the usual precursor to wiretapping is obtaining a court order, FISA permits wiretapping in an emergency situation if application for a court order is made within seven days. *Id.* § 1805(e)-(f).

160. *Id.* § 1803(a). Because the judges are all U.S. district court judges, FISC is deemed a proper Article III court.

161. 50 U.S.C. § 1803(a)(1) (2012).

The appointed judges serve non-renewable, seven-year terms.[162] FISC has jurisdiction only "to hear applications for" FISA surveillance "and grant orders approving electronic surveillance."[163]

Congress also created an appellate court known as the Foreign Intelligence Surveillance Court of Review (FISCR).[164] FISCR is comprised of three federal judges who are designated by the Chief Justice, and the court's jurisdiction is limited solely to reviewing the denial of any FISA application.[165] In its thirty-six-year history, FISCR has heard only one appeal.[166] FISC and FISCR hearings are conducted ex parte and are otherwise closed.[167] Beginning with June 2013, certain "public filings" with FISC are available.[168] In addition, a redacted October 3, 2011 FISC opinion and order are available.[169]

FISA mandates that a surveillance application include a description of the target of the surveillance and a statement of facts justifying the government's belief that the target is a foreign power or agent of a foreign power.[170] Additionally, the government must justify its belief that the target facility "is being used, or is about to be used, by a foreign power or an agent of a foreign power."[171] As originally enacted, a high-level executive official was required to certify that (1) the surveillance objective was foreign-intelligence information; (2) "'the purpose' of the surveillance [was] to obtain foreign intelligence information"; and (3) the information sought could not be obtained by normal investigative techniques.[172] Finally, a successful FISA application must contain a statement of the government's proposed minimization procedures—those procedures

---

162. 50 U.S.C. § 1803(d) (2000).

163. *Id.* § 1803(a).

164. *Id.* § 1803(b).

165. *Id.*

166. *In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002) (per curiam).

167. 50 U.S.C. §§ 1803(c), 1805(a). The ex parte nature of FISC proceedings is not deemed to represent any delegation of judicial authority to the executive branch.

168. *Public Filings – U.S. Foreign Intelligence Surveillance Court*, U.S. FOREIGN INTELLIGENCE SURVEILLANCE CT., http://www.fisc.uscourts.gov/public-filings (last visited Nov. 6, 2014).

169. GOVERNMENT'S EX PARTE SUBMISSION OF REAUTHORIZATION CERTIFICATION AND RELATED PROCEDURES, EX PARTE SUBMISSION OF AMENDED CERTIFICATIONS, AND REQUEST FOR AN ORDER APPROVING SUCH CERTIFICATION AND AMENDED CERTIFICATIONS (FISA Ct. Oct. 3, 2011), *available at* https://www.aclu.org/files/assets/fisc_opinion_10.3.2011.pdf.

170. 50 U.S.C. § 1804(a)(2)-(3) (2012).

171. *Id.* § 1804(a)(3)(B).

172. 50 U.S.C. § 1804(a)(7)(A)-(C) (2000) (internal quotation marks added).

"which shall be adopted by the Attorney General" designed to minimize the acquisition, retention, and dissemination of nonpublic information obtained through FISA surveillance that is not foreign-intelligence information.[173]

Once the FISA surveillance application is certified by the Attorney General and submitted to FISC, FISA *requires* the court to approve an order "as requested or as modified," so long as the court finds "probable cause to believe *that . . . the target of the electronic surveillance is a foreign power or an agent of a foreign power*," and that the target facility "is being used, or is about to be used, by a foreign power or an agent of a foreign power."[174] Of significance is the fact that FISA's probable cause standard is a "foreign-intelligence standard" of probable cause, not a Fourth Amendment standard, requiring only that the government demonstrate that the target *may be* an agent of a foreign government.[175]

Once the appropriate government actor certifies that the purpose of the surveillance is to obtain foreign-intelligence information, FISA prohibits a FISC judge from reviewing the government's certification.[176] The only exception to this bar arises when the target is a United States citizen.[177] In cases where the FISA target is an American, a FISC judge may review the government's certification, but only if "clearly erroneous."[178] Given that applying to FISC for a FISA surveillance order is an ex parte procedure—not the usual adversarial procedure during which opposing counsel may challenge the government's version of the facts—oversight by an

173. *Id.* §§ 1801(h)(1)-(2), 1804(a)(5).

174. *Id.* § 1805(a) (emphasis added).

175. *Id.* FISA defines foreign-intelligence information to include information the federal government would need to guard against acts such as "attack," "sabotage," or "clandestine intelligence activities," all of which concern a foreign power or its agent, and information concerning a foreign power or its agent related to United States defense, security, or foreign affairs. *Id.* § 1801(e). FISA defines foreign power to include a foreign government, a group that is a faction of or directed by a foreign government, a political organization, or an international group engaged in terrorism or proliferation of weapons of mass destruction. 50 U.S.C. § 1801(a) (2012). Many FISA provisions differentiate between a United States person and one not falling within that definition, generally providing more protection for a United States person. *See, e.g.*, 50 U.S.C. § 1805(a)(3)(A), (5) (2000). FISA defines a United States person to include a United States citizen and a resident alien. *Id.* § 1801(i).

176. 50 U.S.C. § 1805(a) (2000).

177. *Id.*

178. *Id.* § 1805(a)(5).

adversary is missing.[179] The presiding FISC judge recently characterized FISC oversight as limited: "'The FISC is forced to rely upon the accuracy of the information that is provided to the Court.'"[180] The presiding judge added: "'The FISC does not have the capacity to investigate issues of noncompliance, and in that respect the FISC is in the same position as any other court when it comes to enforcing [government] compliance with its orders.'"[181]

Surveillance orders authorized by FISC have a statutory duration of up to ninety days when the target is determined to be an agent of a foreign power or up to 120 days when the target is determined to be an agent of a foreign power who is not a United States person.[182] When the target is considered a foreign power, the FISA court order permits surveillance for up to one year.[183] There is no statutory requirement that targets be provided any information regarding the surveillance or the information intercepted, regardless of whether the information is gathered via electronic surveillance or "sneak and peak" searches.[184] The only notification required occurs only if the target is charged with a crime *and* the government intends to use the fruits of the FISA surveillance in his prosecution.[185]

Additionally, Congress wanted to ensure that the legislative branch and the judicial branch were better informed about the executive branch's national-security-surveillance activities. Accordingly, FISA compels a series of reporting measures to be satisfied by the Attorney General.[186] First, in April every year, the Attorney General is expected to deliver an accounting to the Administrative Office of the United States Court and to Congress of the number of applications made to FISC for domestic-wiretap orders and the number of applications granted, modified, or

179. *Id.* § 1805(a).

180. Carol D. Leonnig, *Court: Ability to Police U.S. Spying Program Limited*, WASH. POST (Aug. 15, 2013) (quoting the Honorable Reggie B. Walton), http://www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125_story.html.

181. *Id.* (quoting the Honorable Reggie B. Walton).

182. 50 U.S.C. § 1805(d)(1) (2012). The "United States person" is defined as a citizen, legal permanent resident, an unincorporated association in which a "substantial number" of members are citizens or legal permanent residents, or a corporation incorporated in the United States as long as such association or corporation is not itself a "foreign power." *See* 50 U.S.C. § 1801(i) (2000).

183. 50 U.S.C. § 1805(d)(1) (2012).

184. 50 U.S.C. § 1806(c) (2000).

185. *Id.* In 1994, Congress amended FISA, expanding surveillance to include applications for orders authorizing physical searches. *Id.* §§ 1821-1829.

186. *Id.* §§ 1807-1808.

denied.[187] Additionally, Congress included in FISA the requirement that the Attorney General report to certain congressional committees twice annually.[188] The biannual reports must disclose (1) the number of applications for surveillance where the location of the wiretap is unknown; (2) a description of criminal cases in which wiretap information acquired under FISA is introduced; and (3) the number of emergency wiretap authorizations without court orders and the number of subsequent court orders granting or denying such surveillance.[189]

C. Electronic Communications Privacy Act of 1986[190]

New technologies would, again, draw attention to gaps in the nation's surveillance laws. With the adoption of advancements, such as email, Congress returned to Title III in 1986, replacing it with the new Electronic Communications Privacy Act (ECPA).[191] Almost a decade following FISA, ECPA became the next significant legal change to domestic electronic surveillance.[192] As was true with Title III, Congress attempted to strike a balance between the privacy interests of individuals and the law enforcement concerns of the executive branch.[193] Consistent with the application of Title III, ECPA applies to traditional criminal investigations and controls domestic electronic surveillance initiated for law enforcement purposes.[194] The ECPA list of suspected crimes for which a warrant

187. *Id.* § 1807. For a table containing a summary of FISA annual reports, see *Foreign Intelligence Surveillance Act Court Orders 1979-2014*, *supra* note 12. The information can be found in graph form at *FISA Orders: 1979-2013: FISA Court Orders and National Security Letters Issued*, ELECTRONIC PRIVACY INFO. CENTER, http://epic.org/privacy/wiretap/stats/fisa_graphs.html (last visited Nov. 6, 2014).

188. 50 U.S.C. § 1808(a)(1).

189. 50 U.S.C. § 1808(a)(2) (2012). Other reports are required to certain members of Congress. *Id.* §§ 1802(a)(1)-(2), 1826, 1846, 1862, 1871, 1881f(2), 1885c.

190. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.).

191. *Id.*

192. *Id.*

193. *See supra* Section II.A.

194. 18 U.S.C. § 2516 (2012) (regulating authorization for interception of wire, oral, or electronic communications). Besides applying to actions under color of law, the ECPA applies to individuals. *Id.* § 2511. ECPA permits the government and individuals to secretly tape a conversation as long as the person taping is a party to the conversation or a party to the conversation consents to the conversation being secretly taped. *Id.* § 2511(2)(c)-(d). Otherwise, it is illegal for an individual to

may be obtained increased substantially from Title III's original offenses to a list that includes ninety-six listed crimes, but the requisite court authorization can be issued only to obtain evidence relative to one or more of the listed crimes.[195] By way of example, persons suspected of illicit drug trafficking, white collar crimes, and other felonious conduct are typical targets of criminal surveillance pursuant to ECPA.[196]

ECPA separates electronic surveillance into three fields: the Wiretap Act, which addresses the interception of wire communications;[197] the Stored Communications Act, which includes communications stored during or subsequent to transmission;[198] and the Pen Register Act, which addresses the use of pen registers and trap-and-trace devices.[199] Congress extended the electronic-eavesdropping prohibition to email and other electronic-communication capabilities presented with new technologies.[200] In sum, the ECPA bans wiretapping and electronic eavesdropping; possession of wiretapping or electronic-eavesdropping equipment; use or disclosure of information obtained through illegal wiretapping or electronic eavesdropping; and disclosure of information secured

---

secretly tape a conversation and the individual may be subject to up to a five-year prison term or fine or both. *Id.* § 2511(1), (4)(a). That provision also applies to the government, but the government may obtain a wiretap order, as more fully explained in this Article. *See supra* Section II.A.

195. 18 U.S.C. §§ 2516(1), 2518(3)(a).

196. *Id.* § 2516(1).

197. *Id.* §§ 2510-2522.

198. *Id.* §§ 2701-2712. These provisions of ECPA were another legislative response to earlier judicial action. In *United States v. Miller*, 425 U.S. 435, 442-43 (1976), the Supreme Court ruled that a customer had no Fourth Amendment privacy expectation in the records his bank maintained concerning his transactions with them. The Court reasoned that the bank's records were third-party records, and consequently, they were available to the government under subpoena duces tecum, not requiring the more rigorous requirement of a warrant. *Id.* at 443-46.

199. 18 U.S.C. §§ 3121-3127. These provisions of ECPA were another legislative response to earlier judicial action. In *Smith v. Maryland*, 442 U.S. 735, 745-46 (1979), the Supreme Court refused to require a warrant for the state's use of a pen register or trap-and-trace device employed to identify the telephone numbers for calls made and received from a particular telephone. The Court found no Fourth Amendment search or seizure occurred, ruling that the customer had no expectation of privacy knowing that the telephone company would maintain such information in the regular course of business for billing or service purposes. *Id.* at 741-46; *see infra* notes 399-04 and accompanying text.

200. 18 U.S.C. §§ 2510-2511.

through court-ordered wiretapping or electronic eavesdropping to obstruct justice.[201]

To obtain a court order allowing surreptitious wiretapping under the ECPA, the United States Attorney General, his designee, or a state prosecuting attorney must authorize the application for the order.[202] Typically, an ECPA wiretap order is effective within the territorial jurisdiction of the judge issuing the order, but in its broadest sense, the wiretap is limited to domestic surveillance within the United States.[203]

The statute mandates that the government satisfy the criminal standard of probable cause.[204] In part, an ECPA application must contain a number of specific pieces of information, perhaps the most crucial of which include the government's substantiation of reasonable belief that a warrant-eligible crime has been, is being, or is about to be committed.[205] Other required information includes the location of the planned surveillance, the type of communication to be intercepted, and the name of the target.[206] ECPA applicants must also provide the identity of the person making the application, the identity of the person who authorized the application, the justification for the use of wiretapping over other types of criminal investigation, the requested duration of the wiretap, and information on prior wiretaps conducted of the same target or at the same location.[207] Although the usual precursor to wiretapping is obtaining a court order, ECPA permits wiretapping in an emergency situation if application for a court order is made within forty-eight hours of beginning surveillance.[208]

A judge may issue a wiretap order if the judge finds that the application was properly authorized, that there is probable cause that the target is connected to one of the enumerated crimes, that the wiretap will lead to relevant evidence, and that the specified wiretap location is connected to the crime.[209] Further, the judge must also

---

201. *Id.* §§ 2511-2512.

202. *Id.* § 2516.

203. *Id.* § 2518(3). A federal judge or a properly authorized state court judge may enter a court order authorizing the wiretap. *Id.* §§ 2510(9), 2518.

204. *Id.* § 2518(3).

205. *Id.* § 2518(1)(b).

206. *Id.* Under certain circumstances, the court order may allow a roving wiretap. *Id.* § 2518(11).

207. *Id.* § 2518(1).

208. *Id.* § 2518(7).

209. *Id.* § 2518(3).

find that there is no plausible alternative to the use of wiretapping.[210] ECPA requires that the wiretap order contain much of the information included in the application.[211] Additionally, the judge may order others, including the telecommunications service provider, to provide assistance.[212] The judge may also require reports concerning law enforcement progress in obtaining information concerning the subject crime.[213] Effective for up to thirty days, the wiretap order may warrant additional thirty-day extensions if the court finds continuing probable cause to extend the wiretap's duration.[214]

Although typical applications for ECPA wiretap orders involve ex parte proceedings usually heard in open court, ECPA mandates that both the wiretap application and the orders themselves be sealed.[215] Notwithstanding the statutory seal, ECPA also requires that the target be notified of the wiretap within ninety days of its termination.[216] If the government intends to use the wiretap information as evidence, ECPA compels the government to supply the surveillance target with the wiretap information at least ten days prior to the court proceeding in which the evidence will be presented.[217]

D. The USA PATRIOT Act and Recent Amendments to FISA

On a fateful morning in September 2001, nineteen Muslim extremists hijacked control of four American commercial passenger jets.[218] Employing the passenger-laden aircraft as weapons, the hijackers crashed into the World Trade Center towers in New York City; the Pentagon in Washington, D.C.; and a field in Shanksville,

---

210. *Id.* § 2518(3)(c).
211. *Id.* § 2518(4).
212. *Id.*
213. *Id.* § 2518(6).
214. *Id.* § 2518(5).
215. *Id.* § 2518(8)(b).
216. *Id.* § 2518(8)(d). A judge may delay the date on which the target is required to be provided the wiretap information upon a showing of good cause. *Id.*
217. *Id.* § 2518(9). A judge may waive the ten-day period under certain circumstances. *Id.* The party against whom the government seeks to use the wiretap evidence may move to suppress the evidence on certain grounds. *Id.* § 2518(10)(a).
218. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 1-14 (2004), *available at* http://www.9-11commission.gov/report/911Report.pdf.

Pennsylvania.[219] The massive attack by foreigners on American soil generated a rapid response by Congress aimed at reducing the likelihood that similar assaults could ever occur again. The resulting legislation, passed forty-five days following the attacks on September 11, was intended to "provide[] enhanced investigative tools and improve[] information sharing for the law enforcement and intelligence communities to combat terrorism."[220] Entitled the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001" (Patriot Act),[221] the legislation expanded the powers granted to law enforcement and intelligence agencies. The increased authority allows the executive branch to surreptitiously engage in roving wiretaps, "sneak-and-peak" searches, use of pen registers and trap-and-trace devices, business-record searches, and Internet communication and use tracking.[222] Additionally, the Patriot Act attempted to remove barriers and enhance the exchange of information between the historically segregated intelligence and law enforcement communities.[223]

Though the Patriot Act is a newly enacted piece of legislation, it may be better understood as an extensive list of minor amendments to existing laws.[224] The Patriot Act, which is divided into ten sections, includes a section entitled "Enhanced Surveillance Procedures,"[225] which significantly amends both FISA[226] and ECPA.[227]

---

219. *Id.*

220. H.R. REP. NO. 107-236, pt. 1, at 41 (2001), *available at* http://www.gpo.gov/fdsys/pkg/CRPT-107hrpt236/pdf/CRPT-107hrpt236-pt1.pdf.

221. USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001).

222. *Id.* § 206 (roving surveillance authority), § 213 ("sneak-and-peak" warrants), § 214 (pen register and trap-and-trace authority), § 215 (business-records searches), § 217 (interception of computer trespasser communications). Several Patriot Act provisions, including § 215, were originally scheduled to sunset on December 31, 2005. *Id.* § 224. On March 9, 2006, President Bush signed into law the Reauthorization Act, extending several provisions, of which § 215 was one. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (2006). After several extensions, § 215 is scheduled to sunset on June 1, 2015. PATRIOT Sunsets Extension Act of 2011, Pub. L. No. 112-14, § 2(a), 125 Stat. 216 (2011).

223. USA PATRIOT Act § 504; *see infra* notes 230-31 and accompanying text.

224. *See* Casey, *supra* note 116, at 1003.

225. USA PATRIOT Act §§ 201-225.

226. *Id.* §§ 206-208, 214-215, 218, 225.

227. *Id.* §§ 201-204, 209-210, 212, 216-217, 220, 223.

The Patriot Act amended FISA in two significant ways. First, it altered FISA's national-security probable cause standard, a standard already substantially less stringent from the Fourth Amendment probable cause test, diminishing the FISA standard even further. Prior to the Patriot Act, the gathering of foreign intelligence had to be "the" reason for the executive branch's search and surveillance efforts.[228] After the Patriot Act, FISA required only that foreign intelligence be "a significant purpose" of the government's intrusion.[229] A related amendment, referred to as the "coordination amendment," defined the areas in which federal law enforcement and intelligence agencies were permitted to engage in coordinated foreign-intelligence gathering.[230] This addition allows federal prosecutors to work with intelligence agencies to jointly conduct surveillance operations pursuant to FISA when investigating crimes falling within the "foreign intelligence information" definition.[231]

The Attorney General was able to capitalize on the reduction in the "purpose" standard for conducting FISA surveillance and craft surveillance guidelines that allowed FISC authorization to be granted even when the primary ends of surveillance related to ordinary crime.[232] In essence, the executive branch attempted to completely reverse FISA's original standard by suggesting the FISA surveillance could "be used *primarily* for . . . law enforcement purpose[s], as long as a significant foreign intelligence purpose remain[ed]."[233] Attorney

---

228. 50 U.S.C. § 1804(a)(7)(B) (2000).

229. USA PATRIOT Act § 218 (internal quotation marks omitted).

230. *Id.* § 504. This amendment did not replace any prior FISA language, but added "the coordination with law enforcement" section:

> (k)(1) Federal officers who conduct electronic surveillance to acquire foreign intelligence information under this title may consult with Federal law enforcement officers to coordinate efforts to investigate or protect against—
>
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

Id. (internal quotation marks omitted).

231. *Id.*

232. Memorandum from Attorney Gen. John Ashcroft to FBI Dir., Assistant Attorney Gen., Criminal Div., Counsel for Intelligence Policy, & U.S. Attorneys (Mar. 6, 2002), *available at* http://www.fas.org/irp/agency/doj/fisa/ag030602.html.

233. *Id.* (emphasis added).

General Ashcroft's efforts were intended to break down the "wall" built by Congress and the original FISA.[234]

In May 2002, Ashcroft sought a FISC order utilizing the Department of Justice's newly revised FISA surveillance guidelines.[235] FISC reinforced the "wall" and, for the first time since 1978, required the government's application to be modified.[236] FISC rejected the Department of Justice (DOJ) procedures that would allow federal prosecutors access to the FISA electronic-surveillance process for ordinary criminal investigations.[237] FISC, which had operated in complete secrecy for nearly thirty years, published its first opinion as a protest to Ashcroft's newly proposed procedures for FISA surveillance.[238] The court alluded to governmental abuse, citing the September 2000 government admission that it had made "misstatements and omissions of material facts" in at least seventy-five of its FISA applications.[239] FISC also noted that the DOJ "procedures appear to be designed to . . . substitute the FISA for Title III electronic surveillances and Rule 41 searches."[240] As further justification for its decision, FISC expressed grave concerns that

> criminal prosecutors will tell the FBI when to use FISA (perhaps when they lack probable cause for a Title III electronic surveillance), what techniques to use, what information to look for, what information to keep as evidence and when use of FISA can cease because there is enough evidence to arrest and prosecute.[241]

The DOJ appealed the FISC decision—another first.[242] In its first twenty-three years, FISC had never denied a single government application.[243] It is not surprising that FISC's first denial also engendered the first appeal to FISCR.[244] In its lone decision, FISCR

234. *Id.*

235. *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 613 (FISA Ct.), *rev'd sub nom*. *In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002) (per curiam).

236. *Id.* at 613, 625; Nola K. Breglio, Note, *Leaving FISA Behind: The Need to Return to Warrantless Foreign Intelligence Surveillance*, 113 YALE L.J. 179, 188 (2003).

237. *All Matters Submitted*, 218 F. Supp. 2d at 625.

238. *Id.* at 611.

239. *Id.* at 620.

240. *Id.* at 623.

241. *Id.* at 624.

242. *In re* Sealed Case, 310 F.3d 717, 719 (FISA Ct. Rev. 2002) (per curiam).

243. Breglio, *supra* note 236, at 188.

244. *Sealed Case*, 310 F.3d at 719.

decisively rejected the FISC position, reversing the prior decision.[245] The court ruled, in part, that FISA was never meant to apply only to foreign-intelligence gathering relative to national security, but that it could be used for ordinary criminal cases, in seeming contradiction of the legislative intent.[246] Further, FISCR held that the Fourth Amendment does not require separation between law enforcement and foreign-intelligence operations when federal prosecutors use FISA surveillance to gather criminal evidence in connection with foreign-intelligence crimes.[247]

In essence, FISCR eviscerated the very foundation that previously allowed FISA to pass constitutional muster. FISA's reduced probable cause standard falls far short of satisfying the Fourth Amendment probable cause test, a point FISCR refused to acknowledge. Fourth Amendment jurisprudence requires a warrant issued by a neutral and detached magistrate, a finding of probable cause that a crime has been or is being committed, and the designation of the places to be searched and the things to be seized.[248] By designating FISA's purpose as one serving national security, Congress created a statutory scheme that allowed FISA surveillance to fall outside the Fourth Amendment's warrant requirement and made it significantly easier for federal authorities to acquire surveillance approval.[249]

The relative ease with which a FISA warrant can now be obtained became the subject of attorney Brandon Mayfield's claims against the United States.[250] Mayfield, his family, and his law practice were all subjected to FISA surveillance following the 2004

245. *Id.* at 730-31.

246. *Id.* at 727-36.

247. *Id.* at 736-46.

248. U.S. CONST. amend. IV.

249. *See* Laura K. Donohue, *Anglo-American Privacy and Surveillance*, 96 J. CRIM. L. & CRIMINOLOGY 1059, 1105 (2006).

250. Mayfield v. United States, 504 F. Supp. 2d 1023, 1030 (D. Or. 2007), *vacated*, 599 F.3d 964 (9th Cir. 2010). In a decision that departs from the majority of the constitutional challenges to FISA, the *Mayfield* court declined to adopt the analysis and conclusions of other courts addressing FISA. *Id.* at 1042-43. The United States District Court for the District of Oregon found that FISA, specifically §§ 1804 and 1823, as amended by the Patriot Act, violate the Fourth Amendment and are unconstitutional. *Id.* However, on appeal the United States Court of Appeals for the Ninth Circuit vacated the lower court judgment. *Mayfield*, 599 F.3d at 966. "We hold that, in light of the limited remedy available to Mayfield, he does not have standing to pursue his Fourth Amendment claim because his injuries already have been substantially redressed by the Settlement Agreement, and a declaratory judgment would not likely impact him or his family." *Id.*

terrorist bombing of the commuter trains in Madrid, Spain.[251] Many facts demonstrated that Mayfield had no part in the terrorist attack.[252] For example, at the time the government submitted its certification for a FISC warrant, Mayfield's passport was not current, and he had not left the United States since his service in Germany as a U.S. Army lieutenant approximately ten years prior.[253] The Spanish authorities had determined his fingerprint did not match the fingerprint obtained.[254] Additionally, the Spanish authorities attributed the bombing to individuals from northern Africa, not the United States.[255] Finally, there was no connection found between Mayfield, his family, or his law practice and Spain or North Africa.[256] Nevertheless, the government secured the authorization necessary to conduct continued electronic surveillance of Mayfield's personal and business affairs, repeated physical searches of both his home and his office, and seizure of his personal effects and business files and computers.[257] Eventually, Mayfield was completely exonerated.[258]

After the FISCR panel decision, though, questions continue to arise about whether the ECPA and the Fourth Amendment are any longer effectual. By allowing FISA surveillance in criminal investigations, FISCR paved a path to authorized surveillance with greatly reduced hurdles for government investigators. The expanded availability of FISA suggests that FISA surveillance will be the method of choice, allowing federal prosecutors and law enforcement officers to avoid the Fourth Amendment prescriptions.

One indication of this may be the fairly steady increase in the number of FISA applications for FISC orders filed by the federal government and the extremely low number of applications rejected. For the first twenty years, approved FISA applications numbered fewer than 1,000 per year, from a low of 207 to a high of 839.[259] Beginning with 2002 through 2012, there were over 1,000 FISA applications approved annually, with over 2,000 FISA applications

---

251. *Mayfield*, 504 F. Supp. 2d at 1026-28.
252. *Id.* at 1033.
253. *Id.*
254. *Id.*
255. *Id.*
256. *Id.*
257. *Id.* at 1028-29.
258. *Id.* at 1029.
259. *Foreign Intelligence Surveillance Act Court Orders 1979-2014*, *supra* note 12.

approved annually for four of those years.[260] From 1979 through 2002, FISC did not reject a single FISA application.[261] From 2003 through 2012, FISC rejected only twelve FISA applications.[262]

III. CURRENT STATE OF DOMESTIC SURVEILLANCE

> [P]rivacy is what we keep to ourselves; secrecy is what is kept from us. Privacy is a right claimed by citizens. Secrecy is a privilege claimed by government.[263]

In a 1951 speech during the early part of the Cold War, Associate Justice Robert H. Jackson warned that, in the heat of patriotic fervor, the public might willingly cede some of its civil liberties.[264] Justice Jackson stated, "It is easy, by giving way to the passion, intolerance and suspicions of wartime, to reduce our liberties to a shadow, often in answer to exaggerated claims of security."[265] He warned that this was the wrong course to follow:

> The essence of liberty is the rule of law. . . . Because liberty cannot exist apart from the impartial rule of law, it is vulnerable to wartime stresses, for then the rule of law breaks down. The same passions and anxieties may result from a long period of tension which may be almost as demoralizing as actual war."[266]

He added, "Wartime psychology plays no favorites among rights but tends to break down any right which obstructs its path."[267]

Only nine days after the September 11, 2001 terrorist attacks, President Bush declared the War on Terror. "Our war on terror begins with al-Qaida, but it does not end there. It will not end until every terrorist group of global reach has been found, stopped, and defeated. . . . We will take defensive measures against terrorism to protect Americans."[268] The allusion to the country being at war tends to produce a psychological reaction of fear, making the general public more inclined to forego some measure of privacy in light of

---

260. *Id.*
261. *Id.*
262. *Id.*
263. Jeff Jarvis, *Welcome to the End of Secrecy*, GUARDIAN (Sept. 6, 2013, 11:56 AM), http://www.theguardian.com/commentisfree/2013/sep/06/nsa-surveillance-welcome-end-secrecy.
264. Robert H. Jackson, *Wartime Security and Liberty Under Law*, 1 BUFF. L. REV. 103, 116 (1951).
265. *Id.*
266. *Id.* at 104.
267. *Id.* at 112.
268. H.R. DOC. NO. 107-122, at 3-4 (2001).

the threat to national security.[269] President Bush was not the first United States leader to use the war analogy in spearheading the country's drive against some perceived social problem.[270] In so doing, he harkened back to the just-war theory that originated with St. Augustine in the fifth century of engaging in a righteous war sanctioned by religious authority.[271] President Bush stated, "Freedom and fear, justice and cruelty, have always been at war, and we know that God is not neutral between them. Fellow citizens, we'll meet violence with patient justice, assured of the rightness of our cause, and confident of the victories to come."[272] As in wartime, this War on Terror shifted power to the executive branch and away from Congress and the judicial branch, with discussion focusing on national security, often at the expense of civil liberties, and the executive branch cloaking actions, such as the Terrorist Surveillance Program in secrecy.[273] The explosive nature of a terrorist attack on the country was a catalyst sparking a heretofore unimagined expansion of executive authority.

President Obama continued down the path of invoking the just-war theory as the foundation for government surveillance. A mere two weeks prior to the first NSA revelation, President Obama made a major speech concerning the country's continued War on Terror.[274] While still invoking the just-war theory, the President was careful to proclaim that the executive branch's actions were legally

---

269. Jackson, *supra* note 264, at 104, 112, 116.

270. Since World War II, "[w]ar infected language, not only as a metaphor for efforts to ameliorate major social problems but also in the everyday idioms of social life, from sport to business. The United States declared war on cancer, crime, drugs, and poverty; military terms became part of the common vocabulary." Richard H. Kohn, *The Danger of Militarization in an Endless "War" on Terrorism*, 73 J. MIL. HIST. 177, 191 (2009).

271. David Gibson, *ANALYSIS: Is 'Just War' Doctrine Another Victim of the Syrian Conflict?*, U.S. CATHOLIC (Sept. 11, 2013, 1:51 PM), http://www.uscatholic.org/news/201309/analysis-%E2%80%98just-war%E2%80%99-doctrine-another-victim-syrian-conflict-27815; *see also* H.R. DOC. NO. 107-122, at 6.

272. H.R. DOC. NO. 107-122, at 6.

273. *See infra* notes 326-43 and accompanying text. "[T]he Administration went forward without Congress and using its own interpretations of the constitution and legal opinions rendered in secret, took matters into its own hands . . . in wiretapping foreign nationals and even American citizens." Kohn, *supra* note 270, at 198-99.

274. President Barack H. Obama, Address at the National Defense University (May 23, 2013), *available at* http://www.washingtonpost.com/blogs/wonkblog/wp/2013/05/23/read-president-obamas-speech-on-the-future-of-the-war-on-terror/.

sanctioned.[275] "Moreover, America's actions are legal. . . . Within a week, Congress overwhelmingly authorized the use of force. . . . So this is a just war—a war waged proportionally, in last resort, and in self-defense."[276] The President acknowledged that the War on Terror had created a tension between intelligence gathering and citizens' loss of privacy but affirmed the value of surveillance.[277] "[S]ome [measures taken], like expanded surveillance, raised difficult questions about the balance we strike between our interests in security and our values of privacy. . . . Much of our best counter-terrorism cooperation results in the gathering and sharing of intelligence . . . ."[278] He recognized that surveillance has to take into account newly evolving methods of communication.[279] "[W]e will have to keep working hard to strike the appropriate balance between our need for security and preserving those freedoms that make us who we are."[280] He elaborated, "That means reviewing the authorities of law enforcement, so we can intercept new types of communication, and build in privacy protections to prevent abuse."[281]

The wartime-like impassioned atmosphere comes at a time of immense NSA technological capability, as has been revealed throughout the Snowden documents,[282] government secrecy claimed necessary for national security,[283] and almost no oversight by FISC or Congress.[284] These factors must be seen in light of the human temptation of government agents operating within the government's cloak of invisibility to invade what privacy the average citizen or business once thought it had, whether this stealth operation was crucial to gather foreign-intelligence information on terrorists or satisfied some other purpose, such as for political or economic advantage. With immense technological capability there is a natural potential for misuse, and the government would be loath to dismantle such capability once constructed. Besides the potential for misuse, innocent individuals may be targeted due to human error or false positives.

---

275. *Id.*
276. *Id.*
277. *Id.*
278. *Id.*
279. *Id.*
280. *Id.*
281. *Id.*
282. *See infra* Section III.C.
283. *See infra* Section III.A.
284. *See supra* Subsection II.B.2.

One reporter who broke the early Snowden stories stated, "'The . . . United States doesn't actually need, or the NSA doesn't need a specific reason in order to spy on people and collect their communications.'"[285] He continued, "'They do it because they've developed this technology that lets them do it, and their institutional mandate is just to constantly seek out more and more.'"[286] He added, "'I think what we did made the threat much, much worse, and at the same time, destroyed many of the freedoms that we've all been taught define what the United States is all about.'"[287]

The United States district judge who issued a preliminary injunction foreclosing government telephone metadata collection as to two plaintiffs found little evidence of the necessity of the government program.[288]

> [T]he Government does *not* cite a single instance in which analysis of the NSA's bulk metadata collection actually stopped an imminent attack, or otherwise aided the Government in achieving any objective that was time-sensitive in nature. In fact, none of the three recent episodes cited by the Government that supposedly illustrate the role that telephony metadata analysis can play in preventing and protecting against terrorist attack involved any apparent urgency.[289]

Various FISC opinions criticize NSA operations for not abiding by FISC oversight.[290] Not surprisingly, there have been a number of instances in which NSA employees took unfair advantage of NSA surveillance capabilities to satisfy recreational or personal interests.[291] An NSA Inspector General's report identified twelve investigated and substantiated cases of unauthorized employee spying over a ten-year period; however, there are likely many more unauthorized NSA employee spying incidents that were never discovered.[292]

---

285. John Hockenberry, *Glenn Greenwald: The U.S. Is Not Safer Since 9/11*, TAKEAWAY (Dec. 16, 2013) (quoting Glenn Greenwald), http://www.thetakeaway.org/story/glenn-greenwald-us-not-safer-911/.

286. *Id.* (quoting Glenn Greenwald).

287. *Id.* (quoting Glenn Greenwald).

288. Klayman v. Obama, 957 F. Supp. 2d 1, 43 (D.D.C. 2013) (order granting preliminary injunction).

289. *Id.* at 40 (internal quotation marks omitted).

290. *See infra* notes 385-92 and accompanying text.

291. *See* Paul Lewis, *NSA Employee Spied on Nine Women Without Detection, Internal File Shows*, GUARDIAN (Sept. 27, 2013, 5:08 PM), http://www.theguardian.com/world/2013/sep/27/nsa-employee-spied-detection-internal-memo.

292. *Id.* Although all personal, the reasons for the surveillance varied:

Surreptitiously overhearing a conversation otherwise thought to be private has long been thought to be morally wrong, as one is using secrecy to take unfair advantage of the conversants. However wrong, human nature has succumbed to this temptation for centuries, as in the legend of the ring of Gyges.[293] Glaucon, a character in Plato's *The Republic*, is discussing with Socrates the tension between morality and social constraint.[294] During this discussion, Glaucon relates the tale of Gyges as an example of the manner in which one would act if unobserved and removed from social constraints.[295]

As told by Glaucon, Gyges the shepherd climbed down into an opening made by an earthquake where he saw a hollow horse figure.[296] He entered the figure through a door and found a dead body inside with a gold ring on its finger, which he removed from the body before returning to the surface.[297] While he was meeting with the other shepherds, he discovered that he could make himself invisible by turning the ring on his finger and reverse the process by turning the ring once more.[298] Following that discovery, he managed

---

> One of the cases emerged in 2011[,]when an NSA employee based abroad admitted during a lie-detector case that he had obtained details about his girlfriend's telephone calls "out of curiosity[."] He retired last year.
>
> In a similar case, from 2005, an NSA employee admitted to obtaining his partner's phone data to determine whether she was "involved" with any foreign government officials. In a third, a female NSA employee said she listened to calls on an unknown foreign telephone number she discovered stored on his cell phone, suspecting he "had been unfaithful[."]
>
> In another case, from two years ago, which was only discovered during an investigation [sic] another matter, a woman employee of the agency confessed that she had obtained information about the phone of "her foreign-national boyfriend and other foreign nationals[."] She later told investigators she often used the NSA's surveillance tools to investigate the phone numbers of people she met socially, to ensure they were "not shady characters[."]
>
> The case of the male NSA employee who spied on nine women occurred between 1998 and 2003. The letter states that the member of staff twice collected communications of an American, and "tasked nine telephone numbers of female foreign nationals, without a valid foreign intelligence purpose, and listened to collected phone conversations[."]

Id.

293. PLATO, THE REPUBLIC 32 (Benjamin Jowett trans., Dover Thrift ed. 2000) (1894).

294. *Id.* at 30.

295. *Id.* at 32.

296. *Id.*

297. *Id.*

298. *Id.*

to be chosen as a messenger to the court.[299] There at court, Gyges used his new-found power of invisibility to gain control of the kingdom after first winning over the queen and plotting with her to kill the king.[300]

Communication privacy seems to always have been vulnerable, under surveillance ranging from low technology eavesdropping to high technology government digital interception, with the law lagging behind in offering the individual or business much protection. For example, by the late 1800s, technology was facilitating eavesdropping through sound recording, as Louis D. Brandeis and Samuel D. Warren recognized in their 1890 law review article, *The Right to Privacy*.[301] "Recent inventions and business methods . . . have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[302]

For Brandeis and Warren, privacy was important as a fundamental right, with protection for privacy recognized, to some extent, in existing law.[303] "The common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."[304] They advocated that the sweep of the law be enlarged to provide civil redress for invasion of privacy.[305] "[T]he existing law affords a principle which may be invoked to protect the privacy of the individual from invasion . . . by . . . the possessor of any . . . modern device for recording or reproducing scenes or sounds."[306] They broached the creation of the tort of invasion of privacy to secure the individual's "inviolate personality"[307] by the law protecting one's right "to be let alone."[308] To them, creation of the invasion of privacy tort was needed in light of recent technological advances that threatened maintenance of privacy.[309] The authors

299. *Id.*
300. *Id.*
301. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).
302. *Id.*
303. *Id.* at 198.
304. *Id.*
305. *Id.* at 206.
306. *Id.*
307. *Id.* at 204-05.
308. *Id.* at 193, 205.
309. *Id.* at 208, 213.

envisioned this right to privacy "as a part of the more general right to the immunity of the person,—the right to one's personality."[310]

In 1897, Oliver Wendell Holmes, a contemporary of Warren and Brandeis, was present at the Boston University School of Law's dedication of a new lecture hall and gave his address *The Path of the Law*.[311] The "bad man" from this address is somewhat reminiscent of Glaucon's Gyges.[312] Holmes stated:

> If you want to know the law and nothing else, you must look at it as a bad man, who cares only for the material consequences which such knowledge enables him to predict, not as a good one, who finds his reasons for conduct, whether inside the law or outside of it, in the vaguer sanctions of conscience.[313]

Thus, Holmes drew a distinction between the bad man, whose actions are constrained by the law, and the good one, who operates according to ethical principles.[314]

While viewing the law as "systematized prediction,"[315] Holmes stated:

> You can see very plainly that a bad man has as much reason as a good one for wishing to avoid an encounter with the public force, and therefore you can see the practical importance of the distinction between morality and law. A man who cares nothing for an ethical rule which is believed and practised [sic] by his neighbors is likely nevertheless to care a good deal to avoid being made to pay money, and will want to keep out of jail if he can.[316]

This means that the good man acts in accordance with morality and, in so doing, conforms to legal standards; the acts of the bad man may coincide with those of the good one, but the motivation of the bad man is to escape fine or criminal sanction.[317] "But if we take the view of our friend the bad man we shall find that he does not care two straws for the axioms or deductions, but that he does want to know what the . . . courts are likely to do in fact."[318] Holmes then asks, "But what does [legal duty] mean to a bad man?"[319] A bad man looks

---

310. *Id.* at 207.
311. O. W. Holmes, *The Path of the Law*, 10 HARV. L. REV. 457, 457 n.1 (1897).
312. *Id.* at 459; *see supra* text accompanying notes 293-300.
313. Holmes, *supra* note 311, at 459.
314. *Id.*
315. *Id.* at 458.
316. *Id.* at 459.
317. *See id.*
318. *Id.* at 460-61.
319. *Id.* at 461.

to the law as defining the contours of permissible action and as "a prophecy that if he does certain things he will be subjected to disagreeable consequences by way of imprisonment or compulsory payment of money."[320]

One recognizes figures similar to Holmes's bad man and good man in the dialog between Glaucon and Socrates when Glaucon provides Gyges as an example of someone who would not act in a just fashion if given the opportunity and temptation of taking advantage of a situation.[321] After recounting the Gyges legend, Glaucon sounds as if he is discussing Holmes's "bad man" when observing that "a man is just, not willingly or because he thinks that justice is any good to him individually, but of necessity, for wherever any one thinks that he can safely be unjust, there he is unjust."[322] Later, in *The Republic*, Socrates refutes the idea that one acts justly only if compelled to do so because "justice in her own nature has been shown to be best for the soul in her own nature. Let a man do what is just, whether he have the ring of Gyges or not."[323]

In evaluating the appropriate level of oversight of NSA activities, one might consider human propensity to act like Holmes's bad man or Glaucon's Gyges if given the opportunity. "'Human beings are always going to try to develop more technologies to give themselves greater power' . . . ."[324] Under the guise of protecting national security, the executive branch would likely make the most of whatever exception to the privacy ordinarily expected by an individual or business that the law permits in the context of gathering foreign-intelligence information. "'[T]he challenges for [those with technology] is for other human beings to organize on their own to come up with ways to control and limit that technology so it doesn't do massive amounts of harm. And this kind of tension is critical.'"[325] Combining the impassioned rhetoric of the just-war theory, far-reaching technological capability, and minimal oversight by FISC or Congress with the propensity to maximize executive branch power, it is no wonder that loss of communication privacy is the result.

---

320. *Id.*
321. PLATO, *supra* note 293, at 32-33.
322. *Id.* at 33.
323. *Id.* at 269.
324. Hockenberry, *supra* note 285 (quoting Glenn Greenwald).
325. *Id.* (quoting Glenn Greenwald).

A. The Terrorist Surveillance Program[326]

> The government's been in bed with the entire telecommunications industry since the forties. They've infected everything. They get into your bank statements, computer files, email, listen to your phone calls. . . . Every wire, every airwave. The more technology used, the easier it is for them to keep tabs on you.[327]

In 2005, New York Times reporters Risen and Lichtblau reported that the Bush administration had issued a secret executive order authorizing warrantless domestic wiretapping.[328] The reporters revealed that in 2002, President Bush significantly altered American intelligence gathering when he authorized the NSA to conduct warrantless wiretapping within the United States to obtain evidence of terrorist activity.[329] Under the guise of what the White House named the Terrorist Surveillance Program (TSP), the NSA proceeded to monitor simultaneously and without warrants up to 500 people at one time within the United States and approximately 5,000 to 7,000

---

326. *See* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts: Secret Order to Widen Domestic Monitoring*, N.Y. TIMES, Dec. 16, 2005, at A1; s*ee also* OFFICES OF INSPECTORS GEN. OF THE DEP'T OF DEF., DEP'T OF JUSTICE, CENT. INTELLIGENCE AGENCY, NAT'L SEC. AGENCY, OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, REPORT NO. 2009-0013-AS, UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM (2009) [hereinafter OFFICES OF INSPECTORS GEN.], *available at* http://www.justice.gov/oig/special/s0907.pdf.

327. ENEMY OF THE STATE (Jerry Bruckheimer 1998) (quoting retired NSA agent Edward **"**Brill**"** Lyle, played by actor Gene Hackman), *available at* http://www.imdb.com/title/tt0120660/quotes. David Marconi, the movie screenwriter, took his inspiration for the movie from a James Bamford book, *The Puzzle Palace*. Eric Benson, *Will Smith Already Played Edward Snowden*: Enemy of the State *Screenwriter David Marconi Says He Warned Us About the NSA Fifteen Years Ago*, N.Y. MAG., July 1, 2013, *available at* http://nymag.com/news/frank-rich/enemy-of-the-state-2013-7/. Although some thought the movie plot "far-fetched," the Edward Snowden revelations fifteen years later coincide with some of the movie dialog. *Id.* In his interview with *The Guardian*, Snowden stated:

> "The NSA has built an infrastructure that allows it to intercept almost everything. With this capability, the vast majority of human communications are automatically ingested without targeting. If I wanted to see your emails or your wife's phone, all I have to do is use intercepts. I can get your emails, passwords, phone records, credit cards."

Ewen MacAskill, *Edward Snowden, NSA Files Source: 'If They Want to Get You, In Time They Will,'* GUARDIAN (June 9, 2013) (quoting Edward Snowden), http://www.theguardian.com/world/2013/jun/09/nsa-whistleblower-edward-snowden-why.

328. Risen & Lichtblau, *supra* note 326, at A1.

329. *Id.*

people located outside the United States at one time.[330] The aggregate result was that a large number of American email correspondences and telephone calls were secretly monitored without any court or congressional approval.[331] The full extent of the warrantless surveillance is unknown.

After the TSP activities came to light, the Bush Administration admitted the program did not comply with FISA, but defended the legality of the program, stating that the war in which we are engaged is "a different war."[332] In invoking the just-war theory, President Bush claimed broad executive branch warlike freedoms of action. Contravening FISA on many points, the TSP had an NSA employee rather than a federal judge serving as the gatekeeper, wholly contradicting the checks and balances supposed by the original FISA Congress.[333] The NSA employee determined what data-mining results required further targeted surveillance.[334] The standard employed by the NSA employee for commencing further TSP surveillance was allegedly one of "reasonable suspicion," but many questions arose as to whose reasonable suspicion was required—certainly not that of an objective magistrate.[335] Another FISA violation was the failure to fully report the executive branch's intelligence-collection activities.[336] FISA requires annual and biannual reporting to the judicial branch and Congress, respectively.[337] Quite to the contrary, until the TSP was exposed publicly, knowledge of its existence was very limited, and the

330. *Id.* at A16; *see also* William C. Banks, *The Death of FISA*, 91 MINN. L. REV. 1209, 1213 (2007).

331. Risen & Lichtblau, *supra* note 326, at A1, A16.

332. Banks, *supra* note 330, at 1259-60 (internal quotation marks omitted). Deputy Assistant Attorney General John Yoo of the Office of Legal Counsel of the Department of Justice prepared several legal memoranda in support of the TSP. OFFICES OF INSPECTORS GEN., *supra* note 326, at 10-14. Certain of the TSP activities initiated under presidential authority were transitioned to the Foreign Intelligence Surveillance Court, with presidential authority for the TSP lapsing on February 1, 2007. *Id.* at 30. In the Report, the Inspectors General expressed some concern with the widespread data collection. *Id.* at 38. "[T]he collection activities pursued under the [President's Surveillance Program], and under FISA following the PSP's transition to that authority, involved unprecedented collection activities. We believe the retention and use by IC organizations of information collected under the PSP and FISA should be carefully monitored." *Id.*

333. Banks, *supra* note 330, at 1259.

334. *Id.* at 1259-60.

335. *Id.*

336. *Id.* at 1257-58.

337. 50 U.S.C. §§ 1807-1808 (2012).

executive branch staunchly denied any such secret intelligence gathering was being conducted.[338]

TSP was accomplished in large part because of the cooperation of various telecommunications companies who previously had conditioned surveillance assistance on statutory compliance.[339] The cooperation of the telecommunications companies facilitated government data mining of telecommunications, with the government performing computerized searches of massive stores of data.[340] Once the TSP became public knowledge, many telecommunications companies found themselves a target of another type—named as defendants in litigation challenging the warrantless secret surveillance.[341] In fact, one of the most controversial of the 2008 FISA amendments granted a statutory defense to telecommunications companies who had cooperated with the government.[342] The cooperation of the telecommunications companies facilitated government data mining of telecommunications, with the government performing computer searches of vast rivers of data.[343]

B. The Protect America Act[344]

> "The intelligence community has worried about 'going dark' forever, but today they are conducting instant, total invasion of privacy with limited effort . . . . This is the golden age of spying."[345]

Revelations of TSP provided the foundation for Congress's passage of the Protect America Act of 2007 (PAA).[346] The PAA

338. Banks, *supra* note 330, at 1257-58.

339. Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CALIF. L. REV. 901, 910-11, 913 (2008).

340. *See id.* at 912.

341. *See, e.g.*, Hepting v. AT & T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006) (surviving motions to dismiss and motion for summary judgment), *remanded*, 539 F.3d 1157 (9th Cir. 2008) (remanding in light of the FISA Amendments Act of 2008).

342. FISA Amendments Act of 2008, Pub. L. No. 110-261, § 201, 122 Stat. 2436, 2467 (2008) (codified at 50 U.S.C. §§ 1885-1885c).

343. *Cf.* 50 U.S.C. §§ 1885-1885c.

344. Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (2007).

345. Nicole Perlroth, Jeff Larson & Scott Shane, *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, N.Y. TIMES, Sept. 6, 2013, at A1 (quoting Paul Kocher, a cryptographer, commenting on NSA capability), *available at* http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?_r=0.

preempted a Patriot Act-expanded FISA, further enlarging presidential authority and reducing the vestiges of constitutional protection, when electronic surveillance was "*directed at* a person reasonably believed to be located outside of the United States."[347] The Director of National Intelligence and the Attorney General received the task of shaping the meaning of "directed at" through the development of "reasonable procedures."[348] More troubling still, the legislation required only that "a significant purpose of the acquisition [be] to obtain foreign intelligence information."[349] Congress mandated no greater link between the person targeted for surveillance and an agent of a foreign power (or terrorist).[350]

Although Congress passed the PAA, it did so with a 180-day sunset provision before recessing for the summer.[351] The legislation subsequently expired when congressional representatives balked at extending immunity to the telecommunications companies that had assisted the executive branch with its TSP monitoring.[352] Granting these corporations a statutory defense proved to be a sticking point and one of the more controversial issues,[353] ultimately preventing the PAA's extended duration. Upon the expiration of the PAA, FISA was reinstated until the FISA Amendments Act of 2008 became effective in July 2008.[354]

---

346. James Risen, *Bush Signs Law to Widen Reach for Wiretapping*, N.Y. TIMES, Aug. 6, 2007, at A1, *available at* http://www.nytimes.com/2007/08/06/washington/06nsa.html. Kate Martin, director of the Center for National Security Studies in Washington commented, "'This more or less legalizes the N.S.A. program.'" *Id.* (quoting Kate Martin).

347. Protect America Act § 2 (emphasis added).

348. *Id.*; *see* Paul M. Schwartz, *Warrantless Wiretapping, FISA Reform, and the Lessons of Public Liberty: A Comment on Holmes's Jorde Lecture*, 97 CALIF. L. REV. 407, 414 (2009).

349. Protect America Act § 2.

350. *See id.*

351. *Id.* § 6.

352. Eric Lichtblau, *More Sharp Words Traded over Lapsed Wiretap Law*, N.Y. TIMES (Feb. 23, 2008), http://www.nytimes.com/2008/02/23/washington/23fisa.html.

353. *Id.*

354. FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (2008). Section 201 of the 2008 Act reinstated the immunity provisions. *Id.* § 201. Those provisions are codified at 50 U.S.C. §§ 1885-1885c (2012). At the end of 2012, Congress extended for an additional five years certain provisions of the 2008 amendments that otherwise would have been subject to sunset provisions on December 31, 2012. FISA Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238, 126 Stat. 1631 (2012).

Prior to recent FISA amendments, FISA remained the "exclusive means" for conducting foreign-intelligence surveillance by the executive branch; however, in the 2008 FISA amendments, Congress included ECPA and other federal statutes with FISA as the "exclusive means" for conducting foreign-intelligence surveillance.[355] In part, this FISA amendment was a response to the unpopular and much criticized TSP, and served as a congressional attempt to eliminate warrantless wiretapping by the executive branch.

C. The National Security Agency and Edward Snowden

> You are being watched. The government has a secret system, a machine that spies on you every hour of every day. I know because I built it. I designed the machine to detect acts of terror but it sees everything. Violent crimes involving ordinary people, people like you. Crimes the government considered "irrelevant." They wouldn't act, so I decided I would. But I needed a partner, someone with the skills to intervene. Hunted by the authorities, we work in secret. You'll never find us, but victim or perpetrator, if your number's up . . . we'll find *you*.[356]

Early in the Obama administration, which began in January 2009, there was reason to believe that the executive branch was continuing the Bush administration's warrantless wiretapping in some form.[357] This suspicion was confirmed with Edward Snowden's leak of NSA information during the summer of 2013.[358]

As revealed over the summer of 2013 and into the fall, public knowledge of government activity under the ECPA and FISA is just the tip of the iceberg concerning government surveillance of Americans. An anti-secrecy blog author noted, "Already we've seen a more extensive disclosure of classified information about current intelligence programs than we've seen for at least 40 years, and

---

355. 50 U.S.C. § 1812.

356. *Person of Interest* (CBS television broadcast Sept. 22, 2011), *available at* http://www.imdb.com/title/tt1839578/quotes. Actor Kevin Chapman, who plays one of the characters in the hit television show, commented on the parallels between the show and United States government intelligence, "'Look at the NSA—they're making us look like a reality show! We've been talking about that for three seasons, and it's now just coming to light.'" Ashley Lee, *'Person of Interest' Actor Says the NSA Is 'Making Us Look Like a Reality Show*,*'* HOLLYWOOD REP. (Oct. 4, 2013, 1:15 PM) (quoting Kevin Chapman), http://www.hollywoodreporter.com/news/person-interest-cast-creator-jonathan-643386.

357. Marc Ambinder, *Shut Up: It's Still a Secret*, ATLANTIC (Apr. 7, 2009, 12:35 PM), http://politics.theatlantic.com/2009/04/shut_up_its_still_a_secret.php.

358. MacAskill, *supra* note 53.

maybe ever."[359] The author added, "One revelation led to another, just like pulling a thread on a sweater and unraveling an entire sleeve."[360]

On June 5, 2013, *The Guardian* broke the news of an April 25, 2013 FISC order requiring the telecommunications company Verizon to provide the NSA with telephone metadata on all calls, whether domestic or international; the metadata, considered a business record under § 215 of the Patriot Act, includes the telephone numbers of the individuals participating in a call, the location of the participants, the time of the call, and the duration of the call.[361] Within the following two days, two newspapers, *The Washington Post* and *The Guardian*, disclosed information on Prism, a program providing access to the systems of a number of large Internet companies: Microsoft since 2007; Yahoo since 2008; Google, Facebook, and PalTalk since 2009; YouTube since 2010; Skype and AOL since 2011; and Apple since 2012.[362] Prism allows the NSA to collect data such as the content of the user's emails, audio and video chats, and file transfers as well as the user's search history.[363]

In addition, NSA uses the Upstream program to collect information from the fiber optic cables that form the backbone of the Internet.[364] The information, which includes communication content

---

359. Carrie Johnson, *Snowden's Leaks Lead to More Disclosure from Feds*, NPR (Oct. 11, 2013, 4:00 AM) (quoting Steven Aftergood), http://www.npr.org/2013/10/11/231899987/snowdens-leaks-lead-to-more-disclosure-from-feds.

360. *Id.* (quoting Carrie Johnson).

361. Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 5, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; *see A Guardian Guide to Your Metadata*, GUARDIAN (June 12, 2013, 11:52 AM), http://www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance#meta=0000000.

362. Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data?guni=Article:in%20body%20link.

363. Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 7, 2013), http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html; Greenwald & MacAskill, *supra* note 362.

364. James Ball, *Edward Snowden NSA Files: Secret Surveillance and Our Revelations so Far*, GUARDIAN (Aug. 21, 2013, 3:36 PM),

as well as metadata, is collected with the cooperation of four telecommunications companies that NSA references "by the codenames STROMBREW, FAIRVIEW, BLARNEY, and OAKSTAR."[365] One computer expert speculated as to the various methods that could be employed to access data flowing through the cables: "The N.S.A. could physically install a device that clips on the cable and listens to electric signals, or insert a splitter in the cable through which data would travel."[366] He added that "someone with remote login access to the cable's switch or router could also redirect data flowing through the cables."[367]

As explained below, NSA obtained access to at least one AT&T communications switch, located in San Francisco, in 2002 to 2003, and reportedly obtained access to other AT&T switches, allowing NSA "'vacuum-cleaner surveillance of all the data crossing the internet—whether that be peoples' e-mail, web surfing or any other data.'"[368] Although that information about the San Francisco switch is at least ten years old, NSA access to information traveling on fiber optic cables may have continued, with circumstantial evidence indicating that the two companies whose cooperation allows NSA access to fiber optic cables may be AT&T and Verizon.[369]

Much of the world's international communications is transmitted on a relatively small number of undersea cables.[370] In the United States, these cables, containing great rivers of communications, emerge from the sea floor at approximately half a dozen locations on the Atlantic coast and another half a dozen locations on the Pacific coast, traveling through telecommunications switches before being dispersed to disparate points in the United States.[371] At some point, NSA gained the cooperation of AT&T to

---

http://www.theguardian.com/world/2013/aug/21/edward-snowden-nsa-files-revelations.

365. *Id.*

366. Savage, Miller & Perlroth, *supra* note 71, at B1 (quoting Nicholas McKeowen).

367. *Id.* (quoting Nicholas McKeowen).

368. Justin Elliot, *Does the NSA Tap That? What We Still Don't Know About the Agency's Internet Surveillance*, PROPUBLICA (July 22, 2013, 1:41 PM) (quoting Mark Klein), http://www.propublica.org/article/what-we-still-dont-know-about-the-nsa-secret-internet-tapping.

369. *Id.*

370. JAMES BAMFORD, THE SHADOW FACTORY: THE ULTRA-SECRET NSA FROM 9/11 TO THE EAVESDROPPING ON AMERICA 175 (2008).

371. *Id.* at 176-77.

install a splitter in the building housing at least one of these switches, which was located in San Francisco.[372] Equipment installed in the building created a mirror image of the flood of communications moving through the switch, screened the communications for key information, and routed this information to NSA.[373] A similar system to allow NSA to monitor communications was apparently in place at AT&T facilities in other locations.[374]

AT&T and a number of other telecommunications companies have "'peering' arrangements" that allow them to cut costs by sharing telecommunications cables at various points.[375] This allows the executive branch to gain access to communications carried by a number of telecommunications companies in addition to AT&T. Further, because the San Francisco switch carried domestic as well as international telecommunications traffic, the splitter installed there gave the government access to both domestic and international communications flowing through the switch.[376]

In July 2013, *The Guardian* disclosed information on XKeyscore, a program that allows an NSA analyst to search NSA databases containing email content, Facebook chats, and information on the online activity of a target by using "selectors" such as an individual's email account, name, telephone number, keywords, search terms, websites visited, and metadata.[377] NSA analyst collection of communications of foreign targets permits access to the communications of others in contact with a foreign target.[378]

In September 2013, *The Guardian*, *The New York Times*, and *ProPublica* disclosed that the NSA used a multi-pronged approach to evading the encryption of much information traveling on the Internet, such as emails, banking, and medical data.[379] One approach is to infiltrate target computers prior to data being encrypted; a second approach is to break encryption codes; a third approach is to induce technology companies to allow "back doors" into technology products or to take advantage of security flaws in technology

372. *Id.* at 188, 190.

373. *Id.* at 189-90, 193.

374. ERIC LICHTBLAU, BUSH'S LAW: THE REMAKING OF AMERICAN JUSTICE 139 (1st Anchor Books ed. 2009) (2008).

375. BAMFORD, *supra* note 370, at 186.

376. *Id.* at 194-95.

377. Glenn Greenwald, *XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet*,' GUARDIAN (July 31, 2013, 8:56 AM), http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

378. *Id.*

379. Perlroth, Larson & Shane, *supra* note 345.

products; and a final approach is to insert weaknesses into encryption standards.[380] In addition, the NSA maintains a library of encryption keys and is permitted to store encrypted data as long as necessary to decipher it; however, there is some encryption that NSA has not succeeded in breaking.[381]

In October 2013, *The Washington Post* disclosed that the NSA had been attempting to identify Tor users and their locations.[382] Tor, which "originally stood for The Onion Router," is a network of servers scattered across the globe, together with software to communicate with the network, providing anonymity to a user to communicate and browse the Web.[383] Although the NSA apparently was unsuccessful in conducting surveillance on communication traveling on the Tor network, NSA was successful in learning the identity of a small number of Tor users by sending malware to a Tor user's browser.[384]

In the wake of the Snowden disclosures, FISC released several opinions concerning NSA mass surveillance. One opinion, dated October 3, 2011, and authored by Judge John D. Bates concerned "'upstream collection' of Internet communications," which "refers to NSA's interception of Internet communications as they transit [redacted], rather than to acquisitions directly from Internet service providers."[385] Judge Bates held that certain NSA targeting and

---

380. *Id.*

381. *Id.*

382. Timothy B. Lee, *Everything You Need to Know About the NSA and Tor in One FAQ*, WASH. POST (Oct. 4, 2013), http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/04/everything-you-need-to-know-about-the-nsa-and-tor-in-one-faq/.

383. *Id.*

384. *Id.* For a description of how Tor works, see Eric Geier, *How (and Why) to Set Up a VPN Today*, PCWORLD (Mar. 19, 2013, 3:01 AM), http://www.pcworld.com/article/2030763/how-and-why-to-set-up-a-vpn-today.html.

385. [Redacted], No. [redacted], at 5 & n.3, 81 (FISA Ct. Oct. 3, 2011) [hereinafter Bates opinion] (declassified and redacted) (footnote omitted), *available at* https://www.eff.org/files/filenode/fisc_opinion_-_unconstitutional_surveillance_0.pdf.

> The Court now understands that each year, NSA's upstream collection likely results in the acquisition of roughly two to ten thousand discrete wholly domestic communications that are neither to, from, nor about a targeted selector, as well as tens of thousands of other communications that are to or from a United States person or a person in the United States but that are neither to, from, nor about a targeted selector.

Id. at 72. The opinion and accompanying order were released on August 21, 2013. Bill Chappell, *Secret Court: NSA Surveillance Program Was Unconstitutional*, NPR

minimization procedures were unconstitutional and that the minimization procedures did not comply with FISA.[386] "NSA's collection of MCTs [multiple communications] results in the acquisition of a very large number of Fourth Amendment-protected communications that have no direct connection to any targeted facility and thus do not serve the national security needs underlying the Section 702 collection as a whole."[387]

Judge Bates recognized that the NSA had been collecting Internet data since at least 2008, but that the NSA had delayed until 2011 in bringing this collection information to the court's attention.[388] The judge pointed out that this was not the first time that the government had misrepresented its surveillance activities.[389] "The Court is troubled that the government's revelations regarding NSA's acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program."[390] Judge Bates referenced earlier NSA activities: "Contrary to the government's repeated assurances, NSA had been routinely running queries of the metadata using querying terms that did not meet the required standard for querying."[391] Judge Bates quoted from an earlier opinion of FISC concerning the query standard, which "had been 'so frequently and systemically violated that it can fairly be said that this critical element of the overall . . . regime never functioned effectively.'"[392]

Another opinion, dated August 29, 2013, and authored by Judge Claire V. Eagan,[393] concerned NSA collection of telephone

---

(Aug. 21, 2013, 4:52 PM), http://www.npr.org/blogs/thetwo-way/2013/08/21/214212847/nsa-culled-tens-of-thousands-of-u-s-emails-yearly-fisa-opinion-says.

386. Bates opinion, *supra* note 385, at 80.

387. *Id.* at 78-79.

388. *Id.* at 5, 17.

389. *Id.* at 16 n.14.

390. *Id.*

391. *Id.*

392. *Id.* (citation omitted).

393. *In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [Redacted], No. BR 13-109, at 29 (FISA Ct. Aug. 29, 2013) [hereinafter Eagan opinion] (declassified and redacted), *available at* http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf. The Amended Memorandum Opinion and accompanying Primary Order were released on September 17, 2013. Ellen Nakashima, *FISA Court Releases Opinion Upholding NSA Phone Program*, WASH. POST (Sept. 17, 2013), http://www.washingtonpost.com/world/national-security/fisa-court-releases-opinion-

metadata under section 215 of the Patriot Act.[394] Judge Eagan found that the NSA collection complied with both the Fourth Amendment and with § 215, and that the NSA could formulate a query based on "a reasonable, articulable suspicion" that the query term "is associated with one of the identified international terrorist organizations."[395] Judge Eagan reasoned that the relevance standard of § 215 had been met "[b]ecause known and unknown international terrorist operatives are using telephone communications, and because it is necessary to obtain the bulk collection of a telephone company's metadata to determine those connections between known and unknown international terrorist operatives."[396] Judge Eagan explained:

> Because the subset of terrorist communications is ultimately contained within the whole of the metadata produced, but can only be found after the production is aggregated and then queried using identifiers determined to be associated with identified international terrorist organizations, the whole production is relevant to the ongoing investigation out of necessity.[397]

The opinion cited[398] to a 1979 United States Supreme Court opinion, *Smith v. Maryland*, in concluding that the government collection of telephone metadata was not within the reach of the Fourth Amendment.[399]

In *Smith*, in affirming the lower court's conclusion that use of the pen register did not constitute a search, the United States Supreme Court invoked the third-party doctrine "that a person has no legitimate expectation of privacy in information he voluntarily turns

---

upholding-nsa-phone-program/2013/09/17/66660718-1fd3-11e3-b7d1-7153ad47b549_story.html.

394. Eagan opinion, *supra* note 393, at 1-2.

395. *Id.* at 3, 5.

396. *Id.* at 18.

397. *Id.* at 22.

398. *Id.* at 9.

399. 442 U.S. 735 (1979). *Smith v. Maryland* was a fairly straightforward robbery case in which Smith allegedly grabbed the victim's pocketbook. *Id.* at 737. After the robbery, the victim received a number of threatening telephone calls from someone identifying himself as the robber. *Id.* Through the victim's description of the alleged robber's car, a police officer obtained the vehicle license plate number and, from that, Smith's home telephone number. *Id.* At police request, the telephone company installed a pen register at the company's office to record the numbers dialed from Smith's telephone. *Id.* After the pen register showed a call from Smith's telephone to the victim's, the police obtained a search warrant for Smith's residence. *Id.* Smith filed a motion to suppress claiming that the use of the pen register violated his Fourth Amendment right. *Id.* at 737-38.

over to third parties."[400] The two dissenting opinions in *Smith* were more cognizant of the intrusive nature of the information that could be gleaned from the telephone numbers one calls.[401] In his dissent, Justice Stewart stated:

> 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 not because such a list might in some sense be incriminating, but 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.[402]

In his dissent in *Smith*, Justice Marshall was even more adamant in emphasizing the intrusiveness of pen-register information:

> The prospect of unregulated governmental monitoring will undoubtedly prove disturbing even to those with nothing illicit to hide. Many individuals, including members of unpopular political organizations or journalists with confidential sources, may legitimately wish to avoid disclosure of their personal contacts. Permitting governmental access to telephone records on less than probable cause may thus impede certain forms of political affiliation and journalistic endeavor that are the hallmark of a truly free society. Particularly given the Government's previous reliance on warrantless telephonic surveillance to trace reporters' sources and monitor protected political activity, I am unwilling to insulate use of pen registers from independent judicial review.[403]

In addition, the dissent in the lower court in *Smith* brought up the potential for government abuse that the nation had most recently observed during the Watergate era:

> The majority fails to give due weight to the impact of Watergate and its progeny, the recent revelations of illicit surveillance conducted by the F.B.I. upon activities of various civil rights, labor and political leaders, or indeed, the potential abuse to which the pen register may be put by police authorities. These factors and others have created an environment of distrust, fear and lack of confidence.[404]

---

400. *Id.* at 743-44.

401. *Id.* at 747-48 (Stewart, J., dissenting); *Id.* at 751 (Marshall, J., dissenting).

402. *Id.* at 748 (Stewart, J., dissenting).

403. *Id.* at 751 (Marshall, J., dissenting) (footnote omitted) (citations omitted).

404. Smith v. State, 389 A.2d 858, 874 (Md. 1978) (Cole, J., dissenting) (footnote omitted). The dissent also foreshadowed NSA study of social networks. "The pen register also has the potential of inhibiting freedom of association. If pen-register data were fed into a central computer on a widespread basis, patterns of acquaintances and dealings among a substantial group of people would be available to the government." *Id.* at 874 n.4.

On December 16, 2013, a United States district court judge for the District of Columbia granted a preliminary injunction to two individual plaintiffs challenging the government's collection of telephone metadata on Fourth Amendment grounds.[405] In distinguishing *Smith v. Maryland*, the judge stated:

> When do present-day circumstances—the evolutions in the Government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies—become so thoroughly unlike those considered by the Supreme Court thirty-four years ago that a precedent like *Smith* simply does not apply? The answer, unfortunately for the Government, is now.[406]

On December 27, 2013, a United States district court judge for the Southern District of New York denied a similar motion for preliminary injunction, finding that the government's collection of metadata did not violate the Fourth Amendment.[407] In so doing, the judge found *Smith* controlling: "Clear precedent applies because *Smith* held that a subscriber has no legitimate expectation of privacy in telephony metadata created by third parties."[408]

IV. LARGE WORLD BUSINESS CONSEQUENCES

> "I have been forced to make a difficult decision: to become complicit in crimes against the American people or walk away from nearly 10 years of hard work by shutting down Lavabit. . . . After significant soul searching, I have decided to suspend operations."[409]

In 1978, when Congress first adopted FISA, its intent was to place significant restrictions on the executive branch's authority to

---

405. Klayman v. Obama, 957 F. Supp. 2d 1, 9-10 (D.D.C. 2013) (order granting preliminary injunction).

406. *Id.* at 31.

407. Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 730 (S.D.N.Y. 2013) (order denying preliminary injunction).

408. *Id.* at 752. "Bulk telephony metadata collection under FISA is subject to extensive oversight by all three branches of government. It is monitored by the Department of Justice, the intelligence Community, the FISC, and Congress." *Id.* at 732. In addition, "[s]ince the initiation of the program, a number of compliance and implementation issues were discovered and self-reported by the Government to the FISC and Congress." *Id.*

409. This was the message posted by the owner of Edward Snowden's email service provider when shutting Lavabit. Kevin Poulsen, *Edward Snowden's E-Mail Provider Defied FBI Demands to Turn Over Crypto Keys, Documents Show*, WIRED (Oct. 2, 2013, 5:27 PM) (quoting Ladar Levison), http://www.wired.com/threatlevel/2013/10/lavabit_unsealed/; *see infra* notes 489-495 and accompanying text.

conduct domestic surveillance, not enlarge the powers available to the President.[410] Likewise, when Congress enacted the original NSL statutes, telephone companies and banks served as the contemplated recipients for these limited information requests allowable only in very narrowly defined situations.[411] There is more than a little irony in the fact that both FISA and NSLs began as protective devices to ensure individual privacies and limit government intrusion, and today, both have morphed into something quite different from their predecessors. It is of little surprise that many of the consequences that now threaten American businesses were unimaginable over three decades ago when the government first introduced these tools, and when considered through the "small-world" theory of networking, these consequences have an impact with a magnitude wholly incomprehensible in 1978.

The business consequences of the government's domestic-surveillance practices in the last decade include a laundry list of costs exacted by federal authorities, not the least of which is the expense of complying with authorities' requests for information. Often, these requests are voluminous, requiring days and weeks to compile and copy, necessitating countless demands on human capital as well. All expenses related to complying with federal requests are the responsibility of the business under demand to disclose information. The government's use of its domestic-surveillance tools may also undermine the ethical and contractual privacy obligations a business owes its clients and customers. A business that receives government demands for information or, at worst, becomes an actual surveillance target risks loss of clients or customers. If customers do not leave they may choose to withhold vital information fearing its disclosure. Commercial enterprises may suffer damage to their firms' goodwill or reputation. Some government requests may actually be in conflict with foreign-data-protection laws and result in a domestic business's violation of those foreign regulations.[412]

Many consequences were, perhaps, predictable in 2001 when Congress piloted the Patriot Act into law, but contemplating the

410. *See supra* Subsection II.B.2.

411. *See* JULIAN SANCHEZ, LEASHING THE SURVEILLANCE STATE: HOW TO REFORM PATRIOT ACT SURVEILLANCE AUTHORITIES, POLICY ANALYSIS 10 (2011), *available at* http://object.cato.org/sites/cato.org/files/pubs/pdf/PA675.pdf.

412. *See* Andrew Charlesworth, *Europe's New Data Protection Laws Will Cause Conflict with the US, Warn Legal Experts*, COMPUTING NEWS (Mar. 23, 2012), http://www.computing.co.uk/ctg/news/2162386/europe-s-protection-laws-cause-conflict-warn-legal-experts.

statute's impact on American businesses was not then a priority.[413] In October 2001, the nation was singularly focused on combating terrorism.[414] The open wounds still exposed from 9/11 and the pervasive fear of multiple home-front attacks produced a national climate that welcomed the notions of expanded federal surveillance authority, increased penalties for individuals believed to be associated with terror-related acts, and enhanced policing strategies to prevent conduct that could lead to terrorist attacks.[415] The proponents of the Patriot Act described the proposed legislation as necessary to equip the U.S. government with the tools it required to combat terrorism.[416] With little dissent and an absence of consideration of any commercial ramifications, the Patriot Act became law.[417]

More than ten years removed since its adoption, opposition to the Patriot Act is growing, as numerous state and local governments, civil liberties groups, and business organizations[418] battle to limit the breadth of the legislation. The conflict between Americans' civil liberties and the nation's domestic-surveillance practices authorized by the Patriot Act have received and are continuing to receive significant attention. Unfortunately, examinations of the hardships imposed upon the average American business by the Patriot Act's domestic-surveillance powers are far less numerous, and until the start of the Snowden disclosures, almost non-existent was consideration of the government's use of domestic surveillance of businesses and their employees to map citizens' social networks.

---

413. *See supra* Section II.D.

414. *See supra* Section II.D.

415. *See supra* Section II.D.

416. *See supra* Section II.D.

417. USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 372 (2001).

418. *See* Michael Sniffen, *Major Business Groups Split with Bush Administration over Patriot Act*, ASSOCIATED PRESS (Oct. 6, 2005), http://www.commondreams.org/headlines05/1006-06.htm. The first organized criticism of the Patriot Act from the business sector included the U.S. Chamber of Commerce, the National Association of Manufacturers, and the National Association of Realtors, all frequently named in Forbes' list of twenty-five most influential lobbying entities. *Id.* These groups and others opposed the Bush Administration supporting amendments that would require investigators to explain how the information requested is linked to individuals suspected of terrorism and that would allow businesses to challenge the government's requests in courts. *Id.* The business sector also campaigned for the removal of the gag orders associated with administrative demands for information. *Id.*

A. Business-Records Requests

With the passage of the Patriot Act in 2001, Congress included the business-records provision, § 215, and greatly expanded the scope of the FBI's investigative authority concerning business records.[419] The original business-records provision limited the FBI's reach to request records from only those four types of entities or businesses outlined by statute.[420] Section 215 removed all such limitations relative to the types of entities or businesses who could be subject to a records request.[421] In addition, the new amendment simultaneously lowered the standard of proof necessary to obtain business records and dramatically enlarged the categories of documents that the FBI can attain under this FISA provision.[422] The pertinent part of § 215 provides:

> [T]he Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of *any tangible things* (including books, records, papers, documents, and other items) *for an investigation* to obtain foreign intelligence information not concerning a United States person or *to protect against international terrorism or clandestine intelligence activities*, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.[423]

The Patriot Act amendment to FISA's business-records provision authorizes the FBI to compel any type of business to produce "any tangible things."[424] Now, the FBI's request need not be related to a person whom the FBI is investigating.[425] Rather, the request for records need only *be associated* with "an authorized investigation . . . conducted in accordance with [applicable law and guidelines] . . . to protect against international terrorism or clandestine intelligence activities."[426] This is known as the

419. 50 U.S.C. § 1861(a)(1) (2012).

420. 50 U.S.C. § 1862(a) (1998).

421. 50 U.S.C. § 1861(a)(1) (2012).

422. *Compare* 50 U.S.C. § 1862(a) (1998), *with* 50 U.S.C. § 1861(a)(1) (2012).

423. 50 U.S.C. § 1861(a)(1) (2012) (emphasis added). The "United States person" is defined as a citizen, legal permanent resident, an unincorporated association in which a "substantial number" of members are citizens or legal permanent residents, or a corporation incorporated in the United States as long as such association or corporation is not itself a "foreign power." *Id.* § 1801(i).

424. *Id.* § 1861(a)(1).

425. *Id.* § 1861(b)(2).

426. *Id.*

"relevance standard" and allows the FBI to request information concerning persons not under investigation but who may have a connection to someone or some entity that is under investigation.[427]

Librarians were among the most vocal critics of § 215.[428] Although the FBI asserts that it has not used § 215 to demand records from libraries, librarians suggest otherwise.[429] Unfortunately, the gag provisions of § 215 prohibit the disclosure of all such requests.[430] The protestations of § 215 by librarians earned the business-records provision a new name. It is now most often referred to as the "library" provision.[431] The library provision has proven to be one of the more contentious measures debated in the Patriot Act, and much concern has been voiced over the expansiveness of the FBI's authority to request private information with no meaningful judicial oversight.[432]

Section 215 business-records requests, for instance, received early criticism because it allowed the federal government access to private records, more particularly "*any tangible thing*," previously inaccessible without a subpoena or other court order.[433] If requested, businesses must now produce customers' personal data, transaction records, account histories, and even genetic information.[434] Under FISA, if law enforcement represents that the request is "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities,"[435] the judge has no discretion and *must* approve the request.[436] The recipient business must comply with the request, with little or no meaningful mechanism to challenge

427. *Id.*

428. Paul Coggins, *It Doesn't Stay in Vegas: National Security Letters Under the PATRIOT Act Pose a Significant Threat to U.S. Business*, LEGAL TIMES (Mar. 27, 2006), http://www.nationallawjournal.com/id=900005449669? .

429. *Id.*

430. *Id.*

431. *Id.*

432. *See id.*; *see also* Michael J. Woods, *Counterintelligence and Access to Transactional Records: A Practical History of USA PATRIOT Act Section 215*, 1 J. NAT'L SECURITY L. & POL'Y 37, 57-58 (2005).

433. Am. Civil Liberties Union, *ACLU Says Justice Dept.'s PATRIOT Act Website Creates New Myths About Controversial Law*, ACLU (Aug. 26, 2003), http://www.aclu.org/safefree/patriot/16760prs20030826.html.

434. *Id.*

435. 18 U.S.C. § 2709(a)-(b) (2012).

436. 50 U.S.C. § 1861(c)(1) (2012).

a request.[437] FISA court proceedings are closed, meaning neither the business owner nor her counsel is allowed access.[438]

Initially, the burden on American business is a significant increase in both the direct and the indirect costs to a business.[439] It is the responsibility of the recipient to provide the labor, management, materials, supplies, and anything else necessary to fulfill a Section 215 Order for Business Records, not to mention the necessity of some businesses being forced to hire additional employees to address government requests.[440] Additional employees require additional oversight, further straining management demands. The direct costs associated with large requests can be astronomical, with the security industry estimated to spend $700 million over the first few years.[441] Large security firms are estimated to spend $25 million to $30 million each.[442] These issues are compounded given the lack of meaningful judicial oversight that increases the likelihood of frivolous and counterproductive requests by law enforcement.[443]

The constitutionality of § 215 continues to seek challenges through litigation leaving companies vulnerable to suit from customers whose information the company has revealed.[444] Increasing numbers of § 215 requests only serve to increase a company's exposure.[445] Firms are also exposed to lawsuits advocacy groups may bring on behalf of customers who feel their civil liberties and privacy have been violated by the company's disclosure.[446] By

---

437. 18 U.S.C. § 2709(a).

438. Breglio, *supra* note 243, at 188-90.

439. Tamara Loomis, *The Rising Costs of Patriot Act Compliance*, LEGAL INTELLIGENCER (June 24, 2003), http://www.thelegalintelligencer.com/id=900005389398?.

440. *Cf.* 18 U.S.C. § 2709(a).

441. Loomis, *supra* note 439.

442. *Id.*

443. *See* Breglio, *supra* note 243, at 190.

444. *See id.* at 190-91.

445. After Congress amended FISA in 1998, authorizing the business-records provision, and prior to the passage of the Patriot Act in 2001, the FBI made only one FISA request for business records. *See* OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, A REVIEW OF THE FBI'S USE OF SECTION 215 ORDERS FOR BUSINESS RECORDS IN 2006, at 8 (2008), *available at* http://www.justice.gov/oig/special/s0803a/final.pdf. The number of requests picked up thereafter, with thirty-six § 215 applications processed between 2002 and 2006 (including fifteen applications processed in 2006). *Id.* at 15.

446. BILL OF RIGHTS DEF. COMM., THE USA PATRIOT ACT AND AMERICAN BUSINESS: WHAT YOU CAN DO TO PROTECT YOUR BUSINESS AND YOUR CLIENTS' PRIVACY 4 (2008).

complying with government requests for information, businesses undermine both their ethical and contractual privacy obligations to their clients and customers.[447] In addition to litigation, companies risk customers' withholding of information.[448] Fear of exposure may prompt customers to withhold data needed by the business for general operations, customer service, retention, and marketing.[449]

There are additional risks for companies conducting business overseas. In the world of global commerce, an American firm could find itself in conflict with foreign-data-protection laws.[450] Violation of these international regulations would place a business in the unenviable position of suffering higher legal costs, lost business, and most assuredly, damage to the firm's goodwill or brand reputation.[451]

B. National-Security Letters

An NSL is quite simply a form letter demanding third parties provide information to the requesting enforcement agency.[452] Major congressional consideration dedicated to NSLs occurred in 2001, with the enactment of § 505 of the Patriot Act.[453] Section 505 expanded the FBI's NSL authority when requesting communications records, financial records, and credit agency records.[454] Congress justified its dramatic enlargement of the FBI's NSL provision as a means of "streamlin[ing] the process of obtaining NSL authority."[455] First, the Patriot Act amendments reduce the level of administrative certification required for NSL requests.[456] Now, rather than requiring a high-ranking official at FBI headquarters to certify an NSL request, NSLs certified by agents in charge of field offices suffice.[457] The

447. *Id.*
448. *Id.*
449. *Id.*
450. *Id.*
451. *Id.*
452. One author describes NSLs as "formal demands to surrender certain records and refrain from disclosing the fact of the request." Andrew E. Nieland, Note, *National Security Letters and the Amended Patriot Act*, 92 CORNELL L. REV. 1201, 1201 (2007); *see* 18 U.S.C. § 2709(b) (2012).
453. USA PATRIOT Act, Pub. L. No. 107-56, § 505, 115 Stat. 272, 365 (2001) (codified at 18 U.S.C. § 2709(b)).
454. *Id.*
455. *Administration's Draft Anti-terrorism Act of 2001: Hearing Before the H. Comm. on the Judiciary*, 107th Cong. 57 (2001) (consultation draft).
456. USA PATRIOT Act, § 505.
457. *Id.* E.g., compare 18 U.S.C. § 2709(b) after the amendment by § 505 ("The Director of the Federal Bureau of Investigation, or his designee in a position

second change of note is Congress's substitution of a relevancy standard for the earlier "reason to believe" standard.[458] The change allows an FBI agent to issue a demand for information upon internal certification that the information sought is "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities."[459] A third revision expands the population of individuals whose records may be requested.[460] Section 505 eliminates the requirement that NSLs address only those records of an individual engaged in international terrorism or clandestine intelligence activities or an individual who is or is in communication with a foreign power or an agent of a foreign power.[461] Finally, the Patriot Act amendments authorize records requests of American citizens in connection with FBI investigations, so long as the investigation is not based solely on the exercise of First Amendment rights.[462]

Through the Patriot Act, Congress also created a new NSL provision providing other federal agencies with NSL authority comparable to that held by the FBI.[463] Subsection 358(g) of the Patriot Act adds a section within the Fair Credit Reporting Act authorizing any agency that "conduct[s] investigations of, or intelligence or counterintelligence activities or analysis related to, international terrorism"[464] to issue an NSL request for "a consumer report . . . and all other information in a consumer's file."[465] The new NSL section includes both a non-disclosure[466] and an immunity provision,[467] but, again, fails to delineate any means of enforcement

---

not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director . . . ."), with 18 U.S.C. § 2709(b) prior to the amendment by § 505 ("The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director . . . .").

458. *Compare* 18 U.S.C. § 2709(b) (after the amendment by § 505), *with* 18 U.S.C. § 2709(b) (prior to the amendment by § 505).

459. *Id.* § 2709(b)(1).

460. *Compare id.* § 2709(b) (after the amendment by § 505), *with id.* § 2709(b) (prior to the amendment by § 505).

461. *Id.* § 2709(b)(2).

462. *Id.* § 2709(b).

463. *See* 15 U.S.C. § 1681v(a) (2012).

464. *Id.*

465. *Id.*

466. *Id.* § 1681v(c).

467. *Id.* § 1681v(e).

or penalties for the improper disclosure of an agency's request for information under the section.[468]

Few can doubt the laudability of preventing terrorism, but the post-9/11 tools facilitating domestic surveillance thwart effective oversight and promote opportunities for abuse. The increase in § 215 requests has been significant since the Patriot Act's passage. While this is certainly the case with § 215 business-record requests,[469] it is even more pervasive with NSLs.[470] The Patriot Act amendments to § 505 addressing NSLs removed the requirement that issuing agencies present "specific and articulable facts giving reason to

---

468. *Id.* § 1681v(c).

469. *See* OFFICE OF THE INSPECTOR GEN., *supra* note 445, at 8, 15.

470. Pursuant to the USA PATRIOT Improvement and Reauthorization Act of 2005, the Department of Justice's Inspector General conducted two reviews of the FBI's use of NSLs. *See* OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF NATIONAL SECURITY LETTERS 1 (2007), *available at* http://www.justice.gov/oig/special/s0703b/final.pdf. The first review examined calendar years 2003 through 2005 and culminated in a report issued in early March 2007. *Id.* The Inspector General's review reported a drastic increase in the number of NSL requests, increasing from 8,500 in 2002, to 39,000 in 2003, to 56,000 in 2004, and to 47,000 in 2005. *Id.* at xvi. In addition, the number of NSL requests reported to Congress was inaccurate because of several flaws in the method of collection. *Id.* at xvi-xvii. The review estimated that some 8,850 NSL requests for 2003 through 2005, amounting to approximately 6% of the requests, were not included in the database. *Id.* at xvii.

Investigations of Americans also increased from approximately 39% in 2003 to approximately 53% in 2005. *Id.* at xx. The report also noted that a substantial majority of the FBI's requests pertained to telephone and email communications. *Id.* at xviii.

> [W]e found that that [sic] the FBI used NSLs in violation of applicable NSL statutes, Attorney General Guidelines, and internal FBI policies. In addition, we found that the FBI circumvented the requirements of the ECPA NSL statute when it used at least 739 "exigent letters" to obtain telephone toll billing records and subscriber information from three telephone companies without first issuing NSLs.

Id. at 124. The second Inspector General report examined calendar year 2006 and was issued in March 2008. *See* OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, A REVIEW OF THE FBI'S USE OF NATIONAL SECURITY LETTERS: ASSESSMENT OF CORRECTIVE ACTIONS AND EXAMINATION OF NSL USAGE IN 2006, at 1 (2008), *available at* http://www.justice.gov/oig/special/s0803b/final.pdf. The second examination pays particular attention to the corrective measures taken by the FBI following the Inspector General's first report. *Id.* at 6-8. The 2006 review revealed that NSL requests continued to increase to 49,425 in 2006, a 4.7% increase over the prior year, and a total of 192,499 for 2003 through 2006. *Id.* at 9. The report concluded that it was premature to determine whether the corrective measures will resolve the pervasive problems identified in the prior report and issued additional recommendations. *Id.* at 161-63.

believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power."[471] The objective was to remove obstacles that would prevent the federal government from obtaining personal records, such as financial records, Internet-communication-transaction records, telephone records, and other information, that could assist in preventing a terrorist act. After October 2001, all that is required for a government agency to obtain personal confidential information is a form letter presented to any business requesting information relevant to an ongoing investigation.[472]

NSLs require no judicial oversight, which significantly increases the potential for frivolous and counterproductive requests by law enforcement.[473] Similar to § 215 business-records requests, companies must take time and resources away from their normal operations to gather data to provide information and records to requesting agencies.[474] The direct and indirect costs are substantial.[475] Just as is the case with § 215, it is the responsibility of the recipient to provide the labor, management, materials, supplies, and anything else necessary to comply with the § 505/NSL demand.[476]

Like § 215, by complying with NSL requests for information, businesses undermine both their ethical and contractual privacy obligations to their clients and customers.[477] Again, businesses face the threat of litigation, as well as withholding of information by customers.[478] The same fear of exposure presented in § 215 is present with NSLs and may prompt customers to withhold data needed by the business for general operations, customer service, retention, and marketing.[479] The following paragraphs provide two examples of NSL requests that placed serious strains on businesses.

In the first example, hotels and casinos in Las Vegas, Nevada, served as the unwitting subjects of an intensive and invasive data-mining operation conducted by the FBI through NSLs.[480] In

471. 18 U.S.C. § 2709(b) (2012).
472. *See supra* notes 452-62 and accompanying text.
473. BILL OF RIGHTS DEF. COMM., *supra* note 446, at 5.
474. *Id.*
475. *Id.*
476. Nieland, *supra* note 452, at 1213.
477. BILL OF RIGHTS DEF. COMM., *supra* note 446, at 5.
478. *Id.*
479. *Id.*
480. Barton Gellman, *The FBI's Secret Scrutiny: In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans*, WASH. POST (Nov. 6, 2005), http://www.washingtonpost.com/wp-dyn/content/article/2005/11/05/AR2005110501

December 2003, information revealed that Las Vegas was a potential target for a New Year's Eve terror attack.[481] The FBI began requesting information from Las Vegas businesses on everyone who would be staying in a hotel, renting a vehicle, leasing storage space, or arriving by airplane during the two weeks prior to New Year's Day.[482] Although some businesses complied immediately with the FBI's request, many prominent casino properties refused to disclose the information.[483] To compel disclosure, FBI agents issued NSLs requesting massive amounts of sensitive information.[484] Unable to challenge the NSL demands, casino executives were left no choice but to produce the records, and the information provided more data for the FBI's permanent databases.[485] The amount of data demanded by the FBI was so extensive that some Las Vegas properties feared closure would be required in order to comply with the requests.[486]

The second example followed the Snowden disclosures. The aftermath of the Snowden disclosures apparently resulted in Lavabit, Snowden's email service provider, closing its business after fighting compliance with an NSL.[487] In contrast to other email service providers, a Lavabit customer could encrypt incoming emails with a secret encryption key known to the customer but not to the service provider.[488] Thus, government access to emails of a Lavabit customer was dependent on government knowledge of the customer's encryption key. On August 1, 2013, a federal district judge ordered the service provider to turn over the encryption keys that would

---

366_pf.html. Information gained through NSLs can be used by the government for "contact chaining," "link analysis," and "data mining," enabling a study of social networks. *Id.* (internal quotation marks omitted). "'Starting with your bad guy and his telephone number and looking at who he's calling, and [then] who they're calling,' the number of people surveilled 'goes up exponentially,' acknowledged Caproni, the FBI's general counsel." *Id.* (quoting Valerie Caproni). After the Patriot Act, Attorney General Ashcroft "directed the FBI to develop 'data mining' technology to probe for hidden links among the people in its growing cache of electronic files." *Id.* Data mining allows the government to scour already-gathered information to study social networks; "[d]ata mining intensifies the impact of national security letters, because anyone's personal files can be scrutinized again and again without a fresh need to establish relevance." *Id.*

481. *Id.*
482. *Id.*
483. *Id.*
484. *Id.*
485. *Id.*
486. *See id.*
487. Poulsen, *supra* note 409.
488. *Id.*

allow the government access to the emails of all Lavabit customers rather than just the target's emails.[489]

The federal government had first requested pen-register information on one Lavabit user and, later, the encryption key that would permit the government access to the encrypted emails of all Lavabit customers.[490] Levison equated the government's request for the encryption key to "'asking Coca-Cola to hand over its secret formula.'"[491] On August 2, 2013, Ladar Levison, the Lavabit owner, provided the government with an eleven-page print document, printed in four-point-size font, containing "five, 2,560 SSL encryption keys."[492] Recognizing that the encryption keys were almost illegible in that form, the judge ordered Lavabit to provide the government with the encryption keys in electronic form or risk a fine of $5,000 per day.[493] Levison closed his business on August 8, 2013, rather than comply and appealed the district judge's decision to the United States Court of Appeals for the Fourth Circuit.[494] Levinson commented, "'How as a small business do you hire the lawyers to appeal this and change public opinion to get the laws changed when Congress doesn't even know what is going on?'"[495]

Earlier in the year, in *In re National Security Letter* an unnamed electronic communication service provider successfully challenged the FBI's request for subscriber information and the related requirement prohibiting the provider from disclosing information regarding the request.[496] The court noted that few NSL recipients have contested the NSL disclosure restrictions even though nondisclosure orders accompany some 97% of the NSLs.[497] The district court held "that the nondisclosure provision of 18 U.S.C. § 2709(c) violates the First Amendment and 18 U.S.C. § 3511(b)(2)

489. *Id.*

490. *Id.*

491. Nicole Perlroth & Scott Shane, *As F.B.I. Pursued Snowden, an E-Mail Service Stood Firm*, N.Y. TIMES (Oct. 2, 2013) (quoting Ladar Levison), http://www.nytimes.com/2013/10/03/us/snowdens-e-mail-provider-discusses-pressure-from-fbi-to-disclose-data.html?pagewanted=all&_r=2&.

492. Eyder Peralta, *How Snowden's Email Provider Tried to Foil the FBI Using Tiny Font*, NPR (Oct. 3, 2013, 9:07 PM), http://www.npr.org/blogs/thetwo-way/2013/10/03/228878659/how-snowdens-email-provider-tried-to-foil-the-fbi-using-tiny-font.

493. Perlroth & Shane, *supra* note 491.

494. Poulsen, *supra* note 409.

495. Perlroth & Shane, *supra* note 491 (quoting Ladar Levison).

496. *See* 930 F. Supp. 2d 1064, 1065-67 (N.D. Cal. 2013).

497. *Id.* at 1074.

and (b)(3) violate the First Amendment and separation of powers principles" and imposed an injunction forbidding the government from issuing other NSLs or from enforcing nondisclosure provisions.[498]

In reaching this holding, the court was troubled by the First Amendment concerns that the statutory authority for NSLs do not limit their duration and that "the NSL nondisclosure provisions are not narrowly tailored on their face [to serve a compelling governmental interest], since they apply, without distinction, to both the content of the NSLs and to the very fact of having received one."[499] As far as separation of powers was concerned, the court found that "the statute impermissibly attempts to circumscribe a court's ability to review the necessity of nondisclosure orders."[500] The court explained:

> As written, the statute expressly limits a court's powers to modify or set aside a nondisclosure order to situations where there is "no reason to believe" that disclosure "may" lead to an enumerated harm; and if a specified official has certified that such a harm "may" occur, that determination is "conclusive." The statute's intent—to circumscribe a court's ability to modify or set aside nondisclosure NSLs unless the essentially insurmountable standard "no reason to believe" that a harm "may" result is satisfied—is incompatible with the court's duty to searchingly test restrictions on speech.[501]

The risks associated with conducting businesses overseas are present with NSLs as well. An American firm could, again, find itself in conflict with foreign-data-protection laws. Just as is true with § 215 business-records requests, violation of these international regulations could subject a business to "higher legal costs, lost

---

498. *Id.* at 1081. The court added "given the significant constitutional and national security issues at stake, enforcement of the Court's judgment will be stayed pending appeal, or if no appeal is filed, for 90 days." *Id.*

499. *Id.* at 1075. The court explained:

> This pervasive use of nondisclosure orders, coupled with the government's failure to demonstrate that a blanket prohibition on recipients' ability to disclose the mere fact of receipt of an NSL is necessary to serve the compelling need of national security, creates too large a danger that speech is being unnecessarily restricted.

Id. at 1076.

500. *Id.* at 1077.

501. *Id.* at 1077-78. "Courts necessarily give significant deference to the government's national security determinations. However, that deference must be based on a reasoned explanation from an official that directly supports the assertion of national security interests." *Id.* at 1078 (footnote omitted).

business, and damage to [the firm's] goodwill or brand reputation."[502]

C. Small-World Theory

> In our view, the bulk collection and aggregation of Americans' phone records has a significant impact on Americans' privacy that exceeds the issues considered by the Supreme Court in *Smith v. Maryland*. That decision was based on the technology of the rotary-dial era and did not address the type of ongoing, broad surveillance of phone records that the government is now conducting. These records can reveal personal relationships, family medical issues, political and religious affiliations, and a variety of other private personal information. This is particularly true if these records are collected in a manner that includes cell phone locational data, effectively turning Americans' cell phones into tracking devices. We are concerned that officials have told the press that the collection of this location data is currently authorized.[503]

This Article suggests that Milgram's small-world theory presents additional indirect costs exacted from FISA surveillance, § 215 business requests, and § 505 NSLs, and that these costs have not yet been closely examined. Over the last forty years, Milgram's hypotheses and experiments have provided intriguing fodder for literary works,[504] dinner conversations, and parlor games.[505] Determining who may be connected to whom and through whom proffers entertaining aspects, none of which were lost on Milgram. There are, however, potentially sobering implications of Milgram's small-world studies meriting consideration by American businesses given the current trend of our nation's domestic-surveillance practices. For instance, the significance for Milgram of the small-world problem rested in his theory that a network structure underlies society.[506] He conjectured that there exists an underlying connective

---

502. BILL OF RIGHTS DEF. COMM., *supra* note 446, at 4, 5.

503. Letter from twenty-six United States Senators to James R. Clapper, U.S. Dir. of Nat'l Intelligence 1 (June 27, 2013), *available at* http://www.theguardian.com/world/interactive/2013/jun/28/senators-letter-james-clapper.

504. *See* GUARE, *supra* note 29.

505. *Six Degrees of Kevin Bacon* is another social connectivity game that gained great popularity on college campuses in the late 1990s. Players attempt to link the actor Kevin Bacon to some other actor through films in which they both appeared or through a chain of co-stars in different films but with whom both Bacon and the target appeared. The goal is to link Bacon directly or indirectly with the target actor through as few common films or co-stars as possible. *See* CRAIG FASS, MIKE GINELLI & BRIAN TURTLE, SIX DEGREES OF KEVIN BACON (1996).

506. Milgram, *supra* note 26, at 63.

network comprised of two small worlds.[507] The first, the *actual* small world, is the realm in which two individuals unknowingly share a connection.[508] Arguably, this is the realm most people inhabit—a domain in which individuals are rarely cognizant of everyone to whom and through whom they are connected and even less aware of the multiple, far-reaching networks they populate.[509] The second is the *actualized* small world in which two individuals anticipate, research, and discover their connection—the sphere that gave birth to the cliché "it's a small world."[510]

Using Milgram's example, Fred Jones and an Englishman meet for the first time by happenstance at a café in Tunis; the two engage in light conversational banter; and they pass away a moment in time together while they dine.[511] Not a unique occurrence, similar chance meetings occur countless times each day around the globe. The realm shared by these individuals portrays Milgram's actual small world in which someone like Jones and another, not unlike the Englishman, regardless of their relationship or lack thereof, share a connection that has not been revealed to or recognized by either.[512] The association they unknowingly share is part of a connective network of which they are both participants in an actual small world.[513]

Milgram's sketch continues, and Jones learns that the Englishman has spent some time in Detroit.[514] Jones inquires whether the Englishman knows his friend Ben Arkadian.[515] The Englishman recognizes the name, describes Arkadian, and receives confirmation that the individual recalled is, indeed, the Arkadian about whom Jones is inquiring.[516] Both gentlemen have discovered that they share an association through Arkadian. At the point Jones and the Englishman discover the mutual acquaintance and the link among them is revealed, the *actual* realm in which they exist transforms into Milgram's *actualized* small world. By chance, Milgram's two strangers became more aware of their connectedness to each other

507. *Id.* at 62. "[W]hile persons X and Z may not know each other directly, they may share a mutual acquaintance—that is, a person who knows both of them." *Id.*
508. *Id.* at 61-63.
509. *Id.* at 62.
510. *Id.* at 61 (internal quotation marks omitted).
511. *Id.*
512. *Id.*
513. *Id.* at 62.
514. *Id.* at 61.
515. *Id.*
516. *Id.*

through their mutual acquaintance and, hence, more aware of the underlying network of which they each provide a node and share linkages.[517]

Milgram sought to uncover the connections that define the structure underlying both of the dimensions he denominated as actual (unknown connectivity) and actualized (known connectivity) small worlds.[518] One of Milgram's objectives was to determine how individuals are connected within the networks existing in society, thus identifying an individual's friends and acquaintances.[519] Another larger objective of the small-world experiments was to determine the forces within society that connect, inform, and influence an individual's network.[520] The realization came later of just how little any particular individual knows and appreciates of the networks of which he is a part.[521]

The United States, too, is interested in who may be connected to whom and through whom. This Article suggests that the executive branch shares Milgram's objectives in at least this respect—to determine how individuals may be connected to terrorist cells and their accompanying plots to cause injury and destruction. In the War on Terror, the United States actively seeks to identify and neutralize national-security threats. The executive branch and the federal law enforcement agencies within that branch employ techniques that help determine the forces that connect, inform, and influence terrorists and their organizations. Information gathered through FISA surveillance, § 215 business-records requests, and NSLs inform the FBI and make their analyses possible. Government officials are actively employing techniques to use this information to determine, at a minimum, who is connected to terrorism and what influences those connections, but the information, once collected, is there to make other connections as well.[522] Most of us need not be worried that government officials will wrongfully identify us as connected to terrorists because we are not of a race, religion, or nationality that the counterterrorism investigations might consider inherently suspicious; however, if concern is warranted, it lies in the fact that the executive

---

517. *Id.*

518. Kathryn James, *Six Degrees of Information Seeking: Stanley Milgram and the Small World of the Library*, 32 J. ACAD. LIBRARIANSHIP 527, 527-28 (2006).

519. Milgram, *supra* note 26, at 62.

520. James, *supra* note 518, at 527.

521. Milgram, *supra* note 26, at 66.

522. *See* Sahar F. Aziz, *Caught in a Preventive Dragnet: Selective Counterterrorism in a Post-9/11 America*, 47 GONZ. L. REV. 429, 437-43 (2011).

branch has the capacity to monitor every transaction and communication of any individual without judicial oversight in its attempts. Post-9/11 tools like FISA, § 215, and NSLs ease data collection and exponentially increase the administration's ability to conduct monitoring activities. Information gathered through such domestic monitoring tools can facilitate linking individuals to terrorism. In a small world, the links between any individual and terrorism could be as few as between three and four.[523]

The new goal is to prevent terrorist attacks by interrupting terrorist activities in the making. Thus, the government seeks to identify terrorist suspects and make them targets before they have the opportunity to act.[524] Counterterrorism has shifted the goal from convicting someone of a crime committed in the past to preventing terrorism at almost any cost. Terrorism has supplied a justification for government action once believed to be outside the bounds of the Constitution. This approach could prove particularly problematic for American businesses that may be unaware of all of the individuals, entities, and organizations within their small worlds. The government, however, has the ability to make connections that are beyond a firm's capacity. Given the data-gathering tools available to federal authorities coupled with the lack of judicial oversight, in their haste, federal officials could actualize connections that are not in fact actual.

In the wake of the Snowden-instigated disclosures, the government has defended itself by claiming that information gathered through FISA surveillance, § 215 business-records requests, and NSLs is necessary to thwart incipient terrorist plots and has in fact "disrupted dozens of terrorist plots."[525] That claim may not necessarily be supportable, as "[u]pon scrutiny, however, many of these plots appear in fact to have been uncovered not because of the mass collection of our metadata but through more traditional surveillance of particular phone numbers or email addresses"; information obtained through these "targeted inquiries" could have been collected after securing a court order to do so.[526] Moreover, it is

523. *See* LARS BACKSTROM ET AL., FOUR DEGREES OF SEPARATION 12 (2012), *available at* http://arxiv.org/pdf/1111.4570v3.pdf.

524. Aziz, *supra* note 522, at 430-31.

525. Kenneth Roth, *Rethinking Surveillance*, N.Y. REV. BOOKS (July 2, 2013, 11:17 AM), http://www.nybooks.com/blogs/nyrblog/2013/jul/02/electronic-surveillance-missing-laws/.

526. *Id.* Roth, a former federal prosecutor adds:

unlikely that hardened terrorists will change their methods of communication following the Snowden revelations, given that Osama bin Laden and his associates were careful to leave no digital footprint.[527]

V. LESSONS LEARNED

> [T]he mid-1990s [was] a transformative period for information and communication technology use and policy in the United States and globally. The birth of the Internet as a commercial medium and the need to respond to privacy challenges created by its global and data-driven nature altered the political discourse about privacy protection.[528]

Lessons can be learned from the Snowden disclosures, with a business taking steps to protect the privacy of business property, employees, and clients.

Wherever a business is on the range from low technology to high technology, it should be concerned about protecting consumer data and its own proprietary information from data breaches. Although preventing business-data breaches has been on the horizon for quite some time, the 2013 revelations of NSA surveillance highlighted the timeliness and urgency of a business taking proactive steps to safeguard sensitive data. In a 2013 survey of technology,

---

> Consider the NSA's two most publicized cases, a plot to bomb the New York Stock Exchange and an effort to send money to the Somali Islamist group al-Shabaab. The NYSE case was said to have unraveled beginning with a foreign email captured from the monitoring of a foreign website; the al-Shabaab case was apparently discovered when someone in San Diego called a known terrorist number in East Africa. Neither seems to have depended on the mass vacuuming up of our metadata. In view of the weakness of these "best" cases, twenty-six senators have written to the National Intelligence Director asking him to "provide examples of [the NSA program's] effectiveness in providing unique intelligence, if such examples exist."

Id.

527. *See* John Cassidy, *Why Edward Snowden is a Hero*, NEW YORKER (June 10, 2013), http://www.newyorker.com/online/blogs/johncassidy/2013/06/why-edward-snowden-is-a-hero.html. "Conceivably, the fact that Uncle Sam is watching their Facebook and Google accounts could come as news to some dimwit would-be jihadis in foreign locales, prompting them to communicate in ways that are harder for the N.S.A. to track." *Id.* In contrast, "it will hardly surprise the organized terrorist groups, which already go to great lengths to avoid being monitored. Not for nothing did Osama bin Laden's compound in Abbottabad go without a phone or Internet connection." *Id.*

528. Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 280 (2011).

directors and chief technology officers of some of the country's largest law firms "say they are more concerned about security threats now than they were two years ago. An array of factors, the chiefs say, are driving the heightened focus: tougher regulatory requirements, more security-conscious clients, and the more sophisticated techniques used by cyber-criminals, who are increasingly targeting law firms."[529] The following sections provide information on data breaches, business security planning, the role of the chief privacy officer, safeguards to take with employees, and other proactive steps.

A. Data Breaches

A business cannot chart a successful plan to defend itself against data breaches without learning more about data breaches that have been reported, with a 2013 report from Verizon providing a fairly comprehensive snapshot of data breaches worldwide.[530] The report states that "motive correlates very highly with country of origin," and "[t]he majority of financially motivated incidents involved actors in either the U.S. or Eastern European countries (e.g., Romania, Bulgaria, and the Russian Federation). 96% of espionage cases were attributed to threat actors in China and the remaining 4% were unknown."[531] Financial gain was the motive in 75% of the breaches, while 19% of the breaches were caused by state-affiliated actors, perhaps with an espionage motive in mind.[532]

Of the breaches, 25% were "targeted," meaning that the business was selected to be a potential target and then the perpetrator studied the business to identify weakness in technology that could be exploited; the remaining 75% of the breaches were "opportunistic,"

529. Alan Cohen, *2013 Am Law Tech Survey: Firms' Data Security Fears Rise*, AM. LAW. (Nov. 10, 2013), http://www.americanlawyer.com/id=1202473327555?slreturn=20140112124252.

530. VERIZON, 2013 DATA BREACH INVESTIGATIONS REPORT (2013), *available at* http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf. The report was successful in associating around 75% of the breaches with the particular country of the forty countries in which the breaches were discovered. *Id.* at 21.

531. *Id.*

532. *Id.* at 5, 6. In the report, "espionage" was defined as "state-sponsored or affiliated actors seeking classified information, trade secrets, and intellectual property in order to gain national, strategic, or competitive advantage. The only exception is when it is used for internal actors, where it refers to industrial espionage perpetrated by the employees of the victim." *Id.* at 11 n.9.

meaning that the perpetrator took advantage of a weakness in technology.[533] "[S]ome organizations will be a target *regardless* of what they do, but most become a target *because* of what they do (or don't do)."[534] Law firms may be a type of business vulnerable to targeted attacks, with one FBI agent commenting, "'Law firms are often targeted [since] they store information on clients' pending deals and litigation.'"[535] It is interesting to note that the breakdown of targeted breaches versus opportunistic breaches differed little when considering the size of the business that experienced the breach. Small business experienced 26% of the breaches as targeted and 74% as opportunistic, while large businesses experienced 27% of the breaches as targeted and 73% as opportunistic.[536]

There are a number of common causes of data breaches, with multiple causes of certain breaches.[537] Fifty-two percent of the breaches were attributed to hacking,[538] 40% to malware,[539] 35% to physical threats,[540] 29% to social engineering,[541] 13% to misuse,[542]

---

533. *Id.* at 48.

534. *Id.* at 48.

535. Cohen, *supra* note 529 (quoting Austin Berglas).

536. VERIZON, *supra* note 530, at 48.

537. *Id.* at 25, 26.

538. *Id.* at 34. "Hacking includes all attempts to intentionally access or harm information assets without (or in excess of) authorization by circumventing or thwarting logical security mechanisms." *Id.*

539. *Id.* at 29. "Malware is any malicious software, script, or code added to an asset that alters its state or function without permission." *Id.*; *see also* MICROSOFT CORP., MICROSOFT SECURITY INTELLIGENCE REPORT (2013), *available at* http://www.microsoft.com/security/sir/default.aspx. Lower-level employees are not the only ones to have malware discovered on their computers. A survey of malware analysts reported a high incidence of malware on the computers of senior executives, with a mere 14% of the analysts never having had to remove malware from these computers. THREATTRACK SEC., MALWARE ANALYSTS HAVE THE TOOLS TO DEFEND AGAINST CYBER-ATTACKS, BUT CHALLENGES REMAIN 2 (2013), *available at* http://www.threattracksecurity.com/resources/white-papers/cyber-attacks-internal-challenges-malware-analysts-face.aspx. The source of the malware on senior executives' computers ranged from clicking a link in a phishing email (56%); to attaching an infected device, such as a USB drive or smartphone (47%); to a family member using a business device (45%); to accessing an infected pornographic site (approximately 40%). *Id.*

540. VERIZON, *supra* note 530, at 40. "Physical threats encompass deliberate actions that involve proximity, possession, or force." *Id.*

541. *Id.* at 36. Many businesses constantly warn employees not to click on a hyperlink in an email or otherwise provide confidential information in response to an email. This type of email is called a "phishing" email because the sender is counting on human nature that some recipient will be lured into taking the "bait" and will provide personal information that can be used to compromise one tricked into

and 2% to error.[543] Although the percentage of data breaches attributed to social engineering was lower than those attributed to other factors, many would say that data breach incursions caused by a perpetrator tricking a business employee are the key to many incursions. "Targeted attacks can be particularly hard to defend against because they often exploit the weakest link in any security net: the humans sitting in front of the computers."[544]

The Verizon report examined the level of difficulty involved in the initial data breach of a business and follow-up breaches of the same business.[545] A high percentage of the initial breaches (78%) were of very low or low difficulty, with the rest of moderate difficulty (22%) and less than 1% of high difficulty.[546] In a follow-up breach of the same business, nearly the same percent (73%) were of very low or low difficulty, with the rest of moderate difficulty (7%) or high difficulty (21%).[547] Other factors tabulated were the length of time between the data breach and its discovery, and the person who discovered the breach.[548] Reviewing 2012 information, a large number of the data breaches (66%) were not discovered until months or more following the initial breach, with a high percentage (70%) of the data breaches discovered by someone outside the business, such

---

providing personal information. GREG AARON, ANTI-PHISHING WORKING GRP., PHISHING ACTIVITY TRENDS REPORT 2 (2013), *available at* http://docs.apwg.org/reports/apwg_trends_report_q2_2013.pdf. Phishing is included as one type of social engineering that relies on the trust of the victim to in some way compromise the victim or the victim's business. VERIZON, *supra* note 530, at 36. Multiple attempts at social engineering may ultimately provide the desired result:

> Running a campaign with just three e-mails gives the attacker a better than 50% chance of getting at least one click. Run that campaign twice and that probability goes up to 80%, and sending 10 phishing e-mails approaches the point where most attackers would be able to slap a "guaranteed" sticker on getting a click. To add some urgency to this, about half of the clicks occur within 12 hours of the phishing e-mail being sent.

Id. at 38; *see also* AARON, *supra*.

542. VERIZON, *supra* note 530, at 38. Misuse is "[w]hen privileged parties maliciously or inappropriately use organizational resources in ways they should not." *Id.*

543. *Id.* at 41. "We record an error as a threat action only if it deviates from normal processes within an organization and directly causes or significantly contributes to the incident." *Id.*

544. Cohen, *supra* note 529.

545. VERIZON, *supra* note 530, at 49.

546. *Id.*

547. VERIZON, *supra* note 530, at 49. The Verizon report comments, "Would you fire a guided missile at an unlocked screen door?" *Id.*

548. *Id.* at 52-54.

as third parties, auditors, customers, and law enforcement personnel.[549]

B. Business-Security Planning

Business planning appropriately undertaken may prevent or lessen damage from a data breach; basic business-planning measures should include the business adopting both a privacy policy and a crisis-management plan.

The business-privacy policy should be inclusive and tailored as to the nature of the business, technology used in the business (both software and hardware), business confidential and proprietary information, acceptable use of business property by employees and others interacting with the business, and business location. It is vital to review and update the privacy policy so as to cover any changes in these factors.[550]

As part of developing and updating the privacy policy, the business should inventory its confidential and proprietary data as well as its electronic devices and software, with care taken to ascertain that the data is appropriately secured and devices and software are appropriately current and secured. "'Organizations who do not protect their "crown jewels," or proprietary information, and segregate it from any external facing network, run the risk of having this important information stolen during a cyber attack.'"[551] Securing business assets normally involves seeking the advice of a security professional who, at a minimum, will recommend use of strong passwords, firewalls, virtual private networks, encryption, and anti-malware software.[552] One such professional stated, "'Any data-

549. *Id.*

550. *See* City of Ontario, Cal. v. Quon, 560 U.S. 746 (2010). In this case, the city police department issued members of its SWAT team pagers in 2001 without updating the 2000 city computer policy to specifically cover the pagers. *Id.* at 750-51. The computer policy arguably applied to the texting capability of the pagers, and the SWAT team members were informed in 2002 meeting that the computer policy applied to the pagers, with this information provided in a follow-up memorandum; even so, a department lieutenant's later statement conflicted with the written memorandum. *Id.* at 751-52. Thus, one question before the United States Supreme Court was whether Quon had a reasonable expectation of privacy in his text messages, given that the pagers were acquired subsequent to the computer policy, and there were conflicting facts as to whether the computer policy applied to the pagers. *Id.* at 758.

551. Cohen, *supra* note 529 (quoting Austin Berglas).

552. Illena Armstrong, *Preparing for the New Norm: 2013 Guarding Against a Data Breach Survey*, SC MAG., Mar. 2013, at 24, 27.

centric approach must incorporate encryption, [cryptographic] key management, strong access controls and file monitoring to protect data in physical data centers, virtual and public clouds, and provide the requisite level of security.'"[553] The professional added, "'Today, it is table stakes to 'firewall the data'. By implementing a layered approach that includes these critical elements, organizations can improve their security posture more effectively and efficiently than by focusing exclusively on traditional network-centric security methods.'"[554]

One trend is the employer allowing or even requiring employees to use their own mobile devices for business purposes. One 2013 chief information officer survey showed an expectation that 38% of businesses will end providing mobile devices to employees by 2016, and by 2017, 50% of businesses will expect employees to provide mobile devices for business purposes.[555] While cutting business costs to the employer, this trend of employee-provided devices must be considered in developing the business privacy policy. The business must monitor the business information accessible on the devices and must audit the security of the devices to guard against data breaches by unauthorized outsiders or inadvertent disclosure of sensitive information by mobile device users.[556] The business privacy policy should clearly define ownership of information accessible on employee mobile devices, taking into account the vulnerability of the information to discovery requests.[557] Employees must be trained in the acceptable treatment of business information accessible via employee-owned mobile devices.[558]

One factor brought to light in the Snowden revelations was the location in which business data is stored and the advisability of cloud computing.[559] "It is important to reiterate that jurisdiction still matters. Where the infrastructure underpinning cloud computing (i.e., data centers) is located, and the legal framework that cloud

553. *Id.* at 27 (quoting Tina Stewart).

554. *Id.* (quoting Tina Stewart).

555. Fabio E. Marino & Teri H.P. Nguyen, *Perils of the 'Bring Your Own Device' Workplace: Relying on Employees to Furnish Their Own Smartphones and Tablets Makes It Tricky to Control Data*, NAT'L L.J., Nov. 18, 2013, at 12.

556. *See id.*

557. *See id.* at 13.

558. *Id.*

559. Maija Palmer, *Cyber Security: Privacy Experts Profit from Prism Uproar*, FIN. TIMES (Oct. 15, 2013, 11:47 PM), http://www.ft.com/intl/cms/s/0/742baacc-25f7-11e3-8ef6-00144feab7de.html#axzz3HMixSwGZ.

service providers are subject to, are key issues."[560] Some businesses may choose an alternative to cloud computing for all business information, eschewing remote storage of business data for traditional on-site storage. Another solution to the cloud computing dilemma is to store the sensitive information most crucial to the business on-site, while continuing with cloud computing for the rest of the business data.[561] Businesses worldwide are considering the advantages and disadvantages of cloud storage of business data,[562] with an estimated 10% to 20% of cloud customers located outside the United States diverting their business to clouds not run by United States cloud providers.[563]

It is wise for a business to both prevent a data breach and to deal with a data breach, should the need arise by developing an information-technology-crisis-management plan. The business's IT-crisis-management plan might include the following elements:

1. **Damage Assessment-** How you intend to ascertain exactly what has happened.

2. **Public Relations-** How you intend to respond (since timeliness is critical).

3. **Need for Outside assistance-** Who is needed to assist you with this highly technical problem.

---

560. *Id.* (internal quotation marks omitted).

561. A 2013 law firm survey showed that many law firms split firm data between cloud storage and on-site storage:

> While more than two-thirds of responding firms (69 percent) are using hosted solutions in some fashion, few are trusting them with their most sensitive information. Just 12 percent use the cloud for storage, and a mere 5 percent use it for document management (numbers that were close to last year's results). Where are firms using the cloud? E-discovery and litigation support (with 62 percent of responding firms) and human resources (56 percent) were the most common uses.

Cohen, *supra* note 529.

562. For example, law firm Chief Information Officers expressed client concern with the law firm storing information on a cloud maintained by a company outside the law firm:

> "The cloud isn't just magic and smoke; data is in a physical location, highly secured, with redundant backups. But law firms want to be able to say that the data a client entrusted to it is on their server, in their office—not on a server they can't even tell you where it is. They just can't get comfortable with that."

Id. (quoting Brett Burney). An option might be a private cloud over which the business does maintain control.

563. Palmer, *supra* note 559.

4. **Resources needed to cure** defects that allowed this breach to happen.

5. **How you intend to monitor** & prevent future reoccurrences.[564]

In developing the IT-crisis-management plan, the business might find it requires business personnel on-site who are trained to function as an Incident Response Team (IRT).[565] The goals of the IRT are "to identify, react to and remediate cyber-attacks launched against their network."[566]

In this digital age, especially following the Snowden disclosures, sophisticated potential customers may question a business about its privacy policy and IT crisis-management plan. Law firms, among other businesses, are receiving this inquiry. A law firm chief information officer stated, "'We'll get requests about our response plan in the event of a cyber-breach[.] . . . So [now] we have a cyber-response plan.'"[567]

One measure increasingly taken by a number of businesses is to undergo "penetration testing."[568] Penetration testing involves the business employing a consultant or a team inside the business to run a mock data breach "to break in and steal data, and home in on any [technology] weaknesses."[569] One chief technology officer for a major law firm commented that the firm formerly staged a penetration testing "every year or two" but now is "'doing it very religiously every year.'"[570]

As part of the IT-crisis-management plan, a business may consider the likelihood of advanced persistent threats (APT).[571] These are "highly targeted, long-term, international espionage and sabotage campaigns by covert state actors."[572] APTs are thought of as

564. Lawrence J. Trautman, Jason Triche & James C. Wetherbe, *Corporate Information Technology Governance Under Fire*, 8 J. STRATEGIC & INT'L STUD. 105, 110 (2013).

565. THREATTRACK SEC., *supra* note 539, at 2.

566. *Id.* Of the malware analysts participating in the October 2013 ThreatTrack Security survey, 86.5% worked for a business with an IRT in place. *Id.*

567. Cohen, *supra* note 529 (quoting Lisa Mayo).

568. *Id.*

569. *Id.*

570. *Id.* (quoting Laurence Liss).

571. SYMANTEC CORP., ADVANCED PERSISTENT THREATS: A SYMANTEC PERSPECTIVE 1 (2011), *available at* http://www.symantec.com/content/en/us/enterprise/white_papers/b-advanced_persistent_threats_WP_21215957.en-us.pdf.

572. *Id.*

occurring in four stages: "incursion, discovery, capture, and exfiltration."[573] Incursion is the stage during which the perpetrator enters through a break in the business electronic network, with social engineering being a likely avenue to access.[574] Discovery is the stage during which the perpetrator inventories the network to determine information to be taken and the most fruitful manner of attack.[575] Capture is the stage, perhaps fairly lengthy, during which the perpetrator robs targeted data.[576] Exfiltration is the stage during which the perpetrator removes the data from the business.[577]

The IT-crisis-management plan may encompass a kill-chain approach to security, especially for a business likely to experience an APT. The kill-chain-security approach is borrowed from the military kill chain, the idea being that an attack occurs in stages and can be thwarted if blocked at any stage.[578] The idea of successive stages in an operation can be understood by considering "a stereotypical burglary—the thief will perform reconnaissance on a building before trying to infiltrate it, and then go through several more steps before actually making off with the loot."[579] The goal of the kill-chain approach is to thwart a data breach at as early a stage as possible so as to minimize damage and obviate as much of the time and expense to repair the damage as possible.[580] Though proven to be very effective, the kill-chain approach to security is intensive as to the time and cost needed to implement it. These expenses make the kill-chain approach more likely to be implemented by the business known to be or strongly suspected to be a target of a cyber-attack because of the significant investment in bringing it to fruition. "Using the Cyber Kill Chain to keep attackers from stealthily entering your network requires quite a bit of intelligence and visibility into what's happening in your network. You need to know

573. *Id.* at 2.
574. *Id.* at 2-3.
575. *Id.* at 4.
576. *Id.* at 5.
577. *Id.* at 6.
578. Lysa Myers, *The Practicality of the Cyber Kill Chain Approach to Security*, CSO (Oct. 4, 2013, 8:00 AM), http://www.csoonline.com/article/740970/the-practicality-of-the-cyber-kill-chain-approach-to-security?page=1.
579. *Id.*
580. *Id.* The author comments, "If you don't stop the attack until it's already in your network, you'll have to fix those machines and do a whole lot of forensics work to find out what information they've made off with." *Id.*

when something is there that shouldn't be, so you can set the alarms to thwart the attack."[581]

C. Chief Privacy Officer

A vital tool in the arsenal of many leading businesses is the professionalization of the role of the chief privacy officer (sometimes referred to as the chief security officer or chief technology officer) heading up a privacy office within the business.[582] Other businesses may entrust this role to a privacy consultant. Leading businesses have recognized that the prevalence of technology vital to business has "required the implementation of privacy practices that were dynamic and forward-looking" with those businesses taking "a harm-avoidance approach" in safeguarding the continued trust of business stakeholders.[583]

Privacy practices have become integral to doing business. Thus, "privacy within the firm has moved out of the closet and become a strategic concern" of doing business.[584] One measure of the importance of business privacy is the addition of a chief privacy officer as an officer near the top of the corporate ladder.[585] The role of the chief privacy officer is "'to take a much more forward look' aimed at identifying 'solutions that we could think about to develop that are not even on perhaps the drawing board right now.'"[586]

Privacy professionals internal to the business are often supplemented by consultants who undertake the tasks of conducting privacy audits and ensuring compliance with business privacy policies.[587] Current business strategies include preventing data breaches of business proprietary and confidential information and, in so doing, garnering the continued trust of the business customer.[588] "Privacy . . . has evolved over the last several years to be defined in

581. *Id.*

582. Bamberger & Mulligan, *supra* note 528, at 252, 273, 279.

583. *Id.* at 269. The survey highlighted "identifying consumer expectations as a touchstone for developing corporate privacy practices beyond strict regulatory compliance." *Id.* at 270.

584. Kenneth A. Bamberger & Deirdre K. Mulligan, *New Governance, Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States: An Initial Inquiry*, 33 LAW & POL'Y 477, 504 (2011).

585. Bamberger & Mulligan, *supra* note 528, at 251-52, 262.

586. Bamberger & Mulligan, *supra* note 584, at 490 (quoting CPO respondents).

587. Bamberger & Mulligan, *supra* note 528, at 262-63.

588. *Id.* at 252.

large part by respect for what consumers expect regarding the treatment of their personal sphere."[589]

The role of the chief privacy officer must be outward looking as well as inward looking. "Faced with uncertainty as to external demands on the firm resulting from the interplay between norms, technical and business changes, and flexible regulatory authority, they spend up to half of their time interacting with external stakeholders including regulators, advocates, and professional peers."[590] The chief privacy officer must gauge factors outside the business that have an effect on privacy within the business and, at the same time, must ensure compliance with the business privacy practices.[591]

In certain respects, the chief privacy officer, members of the media pressing privacy concerns, and other organizations and individuals advocating an increased emphasis on privacy have formed a "'privacy community'" that has "pressed privacy as an issue."[592] It stands to reason that the increasing frequency with which privacy issues are reflected in the financial news and the manner in which technology is increasingly integral to doing business place additional pressure on the top corporate officers to emphasize privacy implementation within the business.[593] Even if privacy was not consistently one of the agenda items prior to June 2013, privacy has since been at the top of the agenda for many meetings of corporate executives.[594]

Networking on privacy concerns plays a vital role in dealing with safeguarding privacy in the face of rapidly emerging technology, with networking occurring among privacy professionals and business leaders on a collegial rather than competitive basis. The International Association of Privacy Professionals, with over 13,000 members in seventy-eight countries, provides one forum for such

589. *Id.* at 270.
590. Bamberger & Mulligan, *supra* note 584, at 479.
591. *Id.* at 489, 491, 501.
592. Bamberger & Mulligan, *supra* note 528, at 277.
593. *Id.* One survey respondent noted:

> [R]ight now, you see the P word all over the place. [I]t used to be like once a week I'd cut out an article and say, 'Look, they're talking about privacy in the paper on page twenty-two of the *Wall Street Journal*.' And now it's pretty much every day. So I think we've won the battle of actually being noticed.

Id.
594. *See id.*

networking.[595] In fact, privacy officers "reported that helping competitors make better privacy decisions was in their interest."[596] One privacy officer explained that "[h]elping 'my competitor at XYZ Company do better,' one described, is not 'about competitive advantage.' Rather, '[t]hat's about doing the right thing because if they screw up . . . it screws up all of us.'"[597] It benefits all to share strategies in the prevention, detection, and reporting of data breaches. One report urges a "focus on better and faster detection through a blend of people, processes, and technology" coupled with a call to "[c]ollect, analyze and share incident data to create a rich data source that can drive security program effectiveness."[598]

A business would do well to have employees responsible for technology security meet with all other facets of the business on a regular basis to create an ongoing dialog throughout the business.[599] These meetings can be used for an ongoing discussion of the business privacy policy and IT-crisis-management plan as well as providing the occasion to review the business's continuity and recovery plans.[600] A security consultant commented, "'Security is not a department, it's an architecture.' . . . 'These links are part of your everyday security program—an evolving part of your ability to respond. It's observe, orient, decide, act. It's a living thing.'"[601]

D. Employees

Internal-security compliance, as overseen by a chief privacy officer or outside privacy consultant, necessarily involves careful hiring as well as ongoing employee training to ensure that employees can effectively identify and handle privacy concerns that may arise. The 2013 Verizon report shows that insiders were involved in more

595. *About the IAPP*, IAPP, https://www.privacyassociation.org/about_iapp (last visited Nov. 6, 2014); Andrew Clearwater & J. Trevor Hughes, *In the Beginning . . . An Early History of the Privacy Profession*, 74 OHIO ST. L.J. 897, 919 (2013). This organization provides education, certification, and networking opportunities for privacy professionals. *IAPP Mission and Background*, IAPP, https://privacyassociation.org/about/mission-and-background/ (last visited Nov. 6, 2014).

596. Bamberger & Mulligan, *supra* note 528, at 278.

597. *Id.*

598. VERIZON, *supra* note 530, at 7.

599. Armstrong, *supra* note 552, at 28.

600. *Id.*

601. *Id.* (quoting Jennifer Bayuk).

than two-thirds of reported security incidents.[602] When combining this percentage with the high percentage (75%) of opportunistic data breaches and the high percentage (75%) of initial data breaches being of very low to low difficulty,[603] there may be some reason to believe that proper employee training and penetration testing at regular intervals may pay sizable rewards in decreasing data breach loss. One law firm chief technology officer stated, "'The biggest gap in security is people,'" and then added, "'That's where you are vulnerable.'"[604]

An appropriate background investigation should be part of the employment process. Once hired, an employee should be educated to understand the business-privacy policy and IT-crisis-management plan, and should undergo training necessary to understand the employee's role in carrying out business technology security, with the expectations tailored to the particular business.[605] Standard security procedures may include any constraints on formulating secure passwords; accessing Internet sites; downloading online software or information; storing of sensitive information on portable devices; printing sensitive information; dealing with emails, email contents, and email attachments; allowing others to use business devices or access business sensitive information; using business devices; and accessing business proprietary or confidential information.

It is good security practice for the business to categorize sensitive information by topic or by some other method and partition off the different types of sensitive information, with the network updated and audited on a regular basis.[606] A comprehensive audit and review of the network by a privacy professional should alert the business to any "open door" in the business's network.[607] "[T]his open door may come in the form of insecure remote-access services that are public-Internet-facing and are not locked down" and "may

602. VERIZON, *supra* note 530, at 20.

603. *Id.* at 48-49.

604. Cohen, *supra* note 529. Phishing attacks have evolved into "spear phishing," which targets a particular organization or individual. Eric Basu, *Spear Phishing 101 - Who Is Sending You Those Scam Emails and Why?*, FORBES (Oct. 7, 2013, 6:39 AM), http://www.forbes.com/sites/ericbasu/2013/10/07/spear-phishing-101-who-is-sending-you-those-scam-emails-and-why. Senior management is not immune from phishing attacks, and "whaling" is a term coined to identify these phishing attacks. *Id.*

605. Trautman, Triche & Wetherbe, *supra* note 564, at 111.

606. *Id.*

607. *Id.*

also be exposed through vulnerabilities in the company's software or through an inexcusably weak password for a system that has been long forgotten."[608] Another open door may be discarded business devices and data not undergoing digital and physical shredding.

The business should limit physical access to each type of business sensitive information to the smallest number of employees with a need to know, with such information limited to certain employees, at certain times, and at a certain frequency and access limits reviewed and updated regularly. In addition, data flow of sensitive information should be analyzed to spot unusual data flow.[609]

Lessons are to be learned from the Snowden disclosures, one of which is the special role of the system analyst in contrast to the typical employee cleared to handle sensitive business information. "'In the classified world, there is a sharp distinction between insiders and outsiders. If you've been cleared and especially if you've been polygraphed, you're an insider and you are presumed to be trustworthy . . . .'"[610] Thus, an NSA intelligence agent is intensively vetted prior to receiving a high level clearance to access classified material.[611] Others with similar access are system analysts, members of the information technology staff, who have "'godlike access to systems they manage,'" so as to ensure smooth running of the technology system.[612] Because of the role played by the system analyst in managing data flow, a system analyst, even though lacking a high level clearance similar to that of an intelligence officer, may be a "'super user'" having "'root access'" to the same classified information.[613] The privileged position of the system analyst with respect to the technology system may make an intelligence officer view a system analyst as trustworthy.

---

608. *Id.* at 112.

609. *Id.*

610. Mark Hosenball & Warren Strobel, *EXCLUSIVE-Snowden Persuaded Other NSA Workers to Give up Passwords -Sources*, WASH. POST (Nov. 7, 2013) (quoting Steven Aftergood), http://www.washingtonpost.com/world/national-security/exclusive-snowden-persuaded-other-nsa-workers-to-give-up-passwords--sources/2013/11/07/6bfa9a54-4828-11e3-bf0c-cebf37c6f484_story.html.

611. *Hiring Requirements*, NAT'L SEC. AGENCY/CENT. SEC. SERV., https://www.nsa.gov/careers/jobs_search_apply/hirerequire.shtml (last visited Nov. 6, 2014).

612. Christopher Drew & Somini Sengupta, *N.S.A. Leak Puts Focus on System Administrators*, N.Y. TIMES (June 23, 2013) (quoting Eric Chiu), http://www.nytimes.com/2013/06/24/technology/nsa-leak-puts-focus-on-system-administrators.html?_r=0.

613. *Id.*

Snowden gained access to NSA material when employed by Dell Inc. in the spring of 2012[614] and when employed by Booz Allen Hamilton at the NSA facility in Hawaii in the spring of 2013.[615] The government previously had installed the anti-leak software at other facilities, but the narrow bandwidth at the Hawaii NSA facility was the reason for not installing software that could have detected retrieval of restricted information by an unauthorized insider.[616] Aside from the software issue, Snowden's role as a system analyst may have caused intelligence officers to view him with trust. Apparently, Snowden gained access to the usernames and passwords of approximately twenty to twenty-five of his co-workers after telling them the information was required for him to make the technology run smoothly.[617] Another example in which the trust accorded Snowden worked to his favor was obtaining information on Bullrun, the NSA decryption program.[618] NSA carefully guarded information on Bullrun, with analysts told, "'Do not ask about or speculate on sources or methods underpinning Bullrun.'"[619] Those cleared to a certain extent "were warned: 'There will be no need to know,'"[620] and agencies were warned "to be 'selective in which contractors are given exposure to this information.'"[621]

Thus, learning from Snowden, a business would do well to carefully consider the special, privileged role of the system analyst beginning with the hiring process and continuing while the system analyst is on the job. When hiring, a thorough background check is essential, which would include an examination of any online posting. A business contemplating outsourcing technology staff through a

614. Mark Hosenball, *Snowden Downloaded NSA Secrets While Working for Dell, Sources Say*, REUTERS (Aug. 15, 2013, 5:50 PM), http://www.reuters.com/article/2013/08/15/usa-security-snowden-dell-idUSL2N0GF11220130815.

615. John Bacon, *Contractor Fires Snowden from $122,000-a-Year Job*, USA TODAY (Jun. 11, 2013, 5:36 PM), http://www.usatoday.com/story/news/nation/2013/06/11/booz-allen-snowden-fired/2411231.

616. Hosenball & Strobel, *supra* note 610; Mark Hosenball & Warren Strobel, *Exclusive: NSA Delayed Anti-leak Software at Base Where Snowden Worked*, REUTERS (Oct. 18, 2013), http://uk.reuters.com/article/2013/10/18/usa-security-snowden-software-idUKL1N0I71ZG20131018.

617. Hosenball & Strobel, *supra* note 610.

618. James Ball, Julian Borger, & Glenn Greenwald, *Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security*, GUARDIAN (Sept. 5, 2013), http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

619. *Id.*

620. *Id.* (internal quotation marks omitted).

621. *Id.*

consultant should consider that the business may have less control over a system analyst who is other than a direct employee.[622] During employment, the business may scrutinize the system analyst's behavior more closely and on a more continuous basis for any sign of disloyalty than is done with other employees, especially should the system analyst have access to business confidential or proprietary information.[623] The business may decide to require the approval of two system analysts prior to a system analyst accessing particularly sensitive information.[624]

E. Other Proactive Steps

A technology expert claimed that NSA can take advantage of its "huge capabilities" to conduct surveillance of a business seen to be a "high-value target"; "if it wants in to your computer, it's in."[625] Even so, there are some practical limits on the number of targets NSA can pursue. "The NSA has turned the fabric of the internet into a vast surveillance platform, but they are not magical. They're limited by the same economic realities as the rest of us, and our best defense is to make surveillance of us as expensive as possible."[626]

One strategy to avoid NSA surveillance is for the business to remain low profile. Tactics to surf online anonymously include using Tor,[627] or something similar, or using a virtual private network, which masks the user's computer IP address.[628]

Another strategy is to use encryption, both for online traffic and at the endpoint, perhaps taking the added precaution of performing endpoint encryption of sensitive data on a computer

622. Drew & Sengupta, *supra* note 612.

623. *Id.*

624. *Id.*

625. Bruce Schneier, *NSA Surveillance: A Guide to Staying Secure*, GUARDIAN (Sept. 6, 2013, 9:09 AM), http://www.theguardian.com/world/2013/sep/05/nsa-how-to-remain-secure-surveillance.

626. *Id.*

627. *Id.* Tor (originally "the Onion Router") allows one to anonymously navigate the Internet by routing communication randomly through servers located in various parts of the world. Lee, *supra* note 382. For a description of how Tor works, see Geier, *supra* note 384.

628. Jon Matonis, *5 Essential Privacy Tools for the Next Crypto War*, FORBES (July 19, 2012, 10:47 AM), http://www.forbes.com/sites/jonmatonis/2012/07/19/5-essential-privacy-tools-for-the-next-crypto-war/. Virtual private networks are sometimes used to link computers within a particular business; however, they can also be used to create a secure encrypted tunnel through the Internet. *See* Geier, *supra* note 384.

separated by an air gap from a computer network.[629] Encryption can extend to emails, stored data, telephone conversations over the Internet, and online chat or instant messaging.[630] Snowden stated in an interview, "'Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on.'"[631] With NSA reportedly having access to many commercial software programs, it may be wise to use open-source software and public-domain encryption.[632]

Care should be taken to secure the endpoint of communication, the user's computer, software, and network, as this may be the weak link in the communication chain.[633] Snowden stated, "'Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it.'"[634] Accessing communication through the endpoint may be far easier than breaking encryption.[635]

In addition to protecting the endpoints, the links between networks must also be secured. For example, NSA found weak spots in the cables linking Google and Yahoo data centers.[636] "Those data centers are kept highly secure using heat-sensitive cameras and biometric authentication, and companies believed the data flowing among centers was secure."[637] Even so, "Google . . . began the process of encrypting this internal traffic before reports of N.S.A. spying leaked during the summer, and accelerated the effort since then."[638] The chief attorney for Google stated, "'We have long been concerned about the possibility of this kind of snooping, which is why we have continued to extend encryption across more and more Google services and links.'"[639] The attorney added, "'We are outraged at the lengths to which the government seems to have gone

629. *See* Schneier, *supra* note 625.
630. *Id.*
631. *Id.* (quoting Edward Snowden).
632. *Id.* The choice of the encryption method used is crucial as indicated by the following comment of Ladar Levison: "'Without Congressional action or a strong judicial precedent' . . . 'I would strongly recommend against anyone trusting their private data to a company with physical ties to the United States.'" Perlroth, Larson & Shane, *supra* note 345 (quoting Ladar Levison).
633. Schneier, *supra* note 625.
634. *Id.* (quoting Edward Snowden).
635. *See id.*
636. Savage, Miller & Perlroth, *supra* note 71.
637. *Id.*
638. *Id.*
639. *Id.* (quoting David Drummond).

to intercept data from our private fiber networks, and it underscores the need for urgent reform.'"[640]

One idea discussed by some countries and regions since the Snowden disclosures is to imitate China's electronic "great firewall" that partitions electronic communications within the country from those taking place elsewhere in the world.[641] One example of this is Brazil, which proposes to contain communication in the local area and to establish a secure email system within the country.[642] The reason to restrict an electronic communication to a particular geographic area is to have control over the legal environment through which the communication travels. In contrast, the benefits of unrestricted global online communication have been to promote worldwide communication and technological innovation; "Balkanization" of worldwide communication may slow these benefits.[643] Partitioning communication in this way may also be expensive, as it may be necessary to set up regional data centers and networks.[644]

The discussion of communicating on a network separated from the worldwide one has led to some communities establishing alternative private mesh networks.[645] A mesh network is comprised of numerous nodes, with each wireless radio node programmed to work with the other nodes in the network.[646] In certain circumstances, a community established a mesh network after waiting a considerable length of time for a commercial provider to bridge the "last mile" to the community from the Internet backbone.[647] Over time, some mesh networks have grown to a considerable size, with the Athens Wireless Metropolitan Network having more than 1,000

---

640. *Id.* (quoting David Drummond).

641. Ian Brown, *Will NSA Revelations Lead to the Balkanisation of the Internet?*, GUARDIAN (Nov. 1, 2013, 2:05 PM), http://www.theguardian.com/world/2013/nov/01/nsa-revelations-balkanisation-internet.

642. *Id.*

643. *Id.*

644. *Id.*

645. Clive Thompson, *How to Keep the NSA Out of Your Computer*, MOTHER JONES, http://www.motherjones.com/politics/2013/08/mesh-internet-privacy-nsa-isp (last visited Nov. 6, 2014).

646. *See* Dave Roos, *How Wireless Mesh Networks Work*, HOWSTUFFWORKS, http://www.howstuffworks.com/how-wireless-mesh-networks-work.htm (last visited Nov. 6, 2014).

647. Thompson, *supra* note 645.

members and the Guifi Spanish network having more than 21,000 members.[648]

Other than being attractive to an under-served community, a mesh network might be used by one who wishes to escape persecution by a repressive regime or avoid NSA surveillance.[649] New America Foundation's Open Technology Institute developed Commotion, "internet in a suitcase" software.[650] Commotion enables one to set up private mesh network that remains secure.[651] A Commotion mesh network would remain secure as long as its encryption remains unbroken and the mesh network remains separate from the Internet.[652]

Another technology being explored is quantum cryptography using fiber optic cables and quantum servers.[653] An advantage of quantum cryptography is that a communication breach is easily detected because a breach would alter the light stream carrying the communication.[654] The disadvantage is the hardware required: a fiber optic cable flanked by a secure node on either end, making quantum cryptography best used at this point for internal communication.[655]

Another proactive option is for the business to take a political stand supporting a push in Congress to protect communication privacy by reining in NSA activities and requiring effective oversight of NSA activities.[656] Political activity encompasses a whole range of options from writing letters to elected officials, to meeting with elected officials, to becoming active in a political action committee, to becoming a campaign contributor, to contributing to a campaign of an incumbent challenger.[657]

---

648. *Id.*

649. *See id.*

650. *Id.* (internal quotation marks omitted).

651. *Id.*

652. *See id.*

653. Russell Brandom, *After NSA Leaks, Businesses Seek Security in Quantum Physics*, VERGE (Oct. 15, 2013, 7:30 AM), http://www.theverge.com/2013/10/15/4839072/after-nsa-leaks-businesses-seek-security-in-quantum-physics.

654. *Id.*

655. *Id.*

656. *See* Heather Long, *Fed Up with Congress over the NSA or Shutdown? 5 Tips to Get Your Voice Heard*, GUARDIAN (Oct. 27, 2013, 10:11 AM), http://www.theguardian.com/commentisfree/2013/oct/27/how-to-contact-congress-tips.

657. *Id.*

CONCLUSION

> Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.[658]

Americans' civil liberties and America's security have long presented polar values coexisting sometimes in harmony and sometimes in discord. Since 9/11, the imbalance of their dichotomous existence has been extremely controversial, resting on the far end of discord.[659] Business concerns have in many ways found themselves in the unenviable middle. Because businesses are private in nature, as opposed to a public or governmental entity, and not an individual, per se, they are left outside many constitutional protections.[660] Further, the federal domestic-surveillance tools enacted since 9/11 leave precious little room for challenge.[661]

> Congress may need to weigh in to require the federal government to disclose information on a regular schedule to help restore public confidence. Other veterans in the intelligence community say only an independent arbiter, like Congress or the courts, can balance the need to protect legitimate secrets against the public's right to know.[662]

Consequently, tens of thousands of American businesses have been recipients or targets of the government's intelligence gathering efforts with numerous negative consequences. Hundreds of thousands of their clients and customers have unknowingly had information disclosed through FISA surreptitious surveillance practices, § 215 business-records requests, and § 505 NSLs.[663] These clients and customers about whom information is sought may enjoy constitutional protections and the mechanism to lodge objections but

---

658. United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) (footnote omitted) (adopting the mosaic theory), *aff'd in part sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

659. *See supra* Part III.

660. *See supra* Part IV.

661. *See supra* Part IV.

662. Johnson, *supra* note 359.

663. *See supra* Part IV.

not the knowledge that their information has been disclosed. This essentially allows authorities to avoid bothersome challenges. Armed with unimaginable volumes of data, federal authorities possess necessary information to map and monitor Americans' social networks, webs of friends, acquaintances, and others about which the networks' members lack information required for their own familiarity. Now, this information is available not only for use in national-security prosecutions to prevent further terrorist attacks, but also in ordinary, everyday criminal prosecutions very much accountable to the U.S. Constitution. Further examination and review is needed to fully understand the magnitude of the small-world implications for big-world consequences in post-9/11 America.