Science and Technology Law Review

Volume 19 | Number 3 Article 5

2016

Seeking to Promote Security over Privacy and Achieving Neither

Jon M. Garon

Seeking to Promote Security Over Privacy and Achieving Neither

*Jon M. Garon**

The year 2015 proved to be a difficult year for the ideals of a networked world brought together through computers and technology. The year was characterized by a series of terrorist attacks across the globe involving some cyber component (i.e., cyber-attacks). In 2014 policymakers focused on individual privacy and governmental accountability, but the attacks of 2015 have shifted their focus to global terrorism and a search for effective security.

Edward Snowden, the self-appointed whistleblower of 2013, was nearly forgotten as security again took center stage. Cyber-attacks by China and North Korea, terrorist attacks by ISIS,[1] domestic threats from homegrown terrorists, and corporate attacks designed to destroy online companies combined to make a new chapter in the world of cyber law. The year culminated with the enactment of the Cybersecurity Act of 2015.[2] This review highlights a few of the key drivers that shaped the legislation and may help in anticipating the trajectory of regulatory policy in the years to come.

I. TERRORISM IN CYBERSPACE

Looking back on 2015, a predominant cultural theme was the "war on terror" defined by the increase in Islamic State of Iraq and the Levant (ISIS or ISIL) attacks.[3] These attacks have diminished the importance of the revelations related to the unauthorized disclosure by Edward Snowden in 2013 of potentially illegal and excessive government surveillance programs.[4]

---

* Dean and Professor of Law, Nova Southeastern University Shepard Broad College of Law; J.D. Columbia University School of Law 1988. An earlier version of this article was prepared as part of the 2016 Winter Working Meeting of the American Bar Association, Business Law Section Cyberspace Law Committee meeting held at Nova Southeastern University Shepard Broad College of Law, January 30–31, 2016. Available at SSRN: http://ssrn.com/abstract=2707756.

1. ISIS is the acronym for the self-proclaimed Islamic State in Iraq and Syria. Evan Kohlmann, *Everything you need to know about ISIS*, MSNBC (Nov. 20, 2015), http://www.msnbc.com/msnbc/what-you-need-know-about-isis.

2. Cybersecurity Act of 2015, Pub. L. No. 114-113.

3. *See, e.g.*, United States v. Tairod Nathan Webster Pugh, 150 F. Supp. 3d 218, 221 (E.D.N.Y. 2015) ("According to the Government, ISIL is a foreign terrorist organization that has existed, in one form or another, since approximately 2004.").

4. *See* Patrick M. Rahill, *Top Secret-The Defense of National Security Whistleblowers: Introducing A Multi-Factor Balancing Test*, 63 CLEV. ST. L. REV. 237, 238 (2014) ("In the summer of 2013, the United States was hit with what some have called one of the most significant national security leaks in U.S. political history. Beginning in May 2013, Edward Snowden began leaking documents that detailed a massive surveillance program orchestrated by the National Security Agency.").

In late 2015, ISIS coordinated an attack in Paris, France,[5] and motivated a domestic terrorist in San Bernardino, California.[6] The effect of these attacks has been to refocus public and private officials on efforts to reduce the threat of terrorism.[7] ISIS uses the Internet for a great deal of its communications, propaganda, and international coordination efforts.[8] While some of the hyperbole surrounding this issue focuses on anti-Muslim sentiment, others focus on increasing public surveillance,[9] particularly the use of surveillance techniques involving social media.[10]

At least one of the killers involved in the San Bernardino attack "talked openly on social media about her views on violent jihad."[11] Undoubtedly, this will result in new demands for police and national security efforts to increase surveillance on social media, and to link these tools to law enforcement—at least for publicly accessible information. The attacker's use of social media will also likely increase efforts to encourage the public to report such comments.

In the United Kingdom, for example, a new National Cyber Centre is being planned.[12] Government officials expect that most of its focus will be on state-sponsored attacks but efforts will also target loosely organized groups of individuals, like ISIS, who use the Internet and social media to attack critical infrastructure.[13]

5. Adam Nossiter & Rick Gladstone, *Paris Attacks Kill More than 100, Police Say; Border Controls Tightened*, N.Y. TIMES, Nov. 13, 2015, at A1.

6. Michael S. Schmidt & Richard Pérez-Peña, *F.B.I. Treating San Bernardino Attack as Terrorism Case*, N.Y. TIMES, Dec. 4, 2015, at A1.

7. *Id.*

8. *See* Larry Greenemeier, *Anonymous's Cyber War with ISIS Could Compromise Terrorism Intelligence*, SCIENTIFIC AM. (Nov. 19, 2015), http://www.scientificamerican.com/article/anonymous-s-cyber-war-with-isis-could-compromise-terrorism-intelligence/.

9. David Downey, *San Bernadino Shootong: People Already Adapting to Increased Surveillance*, THE PRESS ENTERPRISE (Dec. 26, 2015), http://www.pe.com/articles/san-790330-cameras-bernardino.html.

10. Justin Jouvenal, *The new way police are surveilling you: Calculating your threat 'score'*, THE WASHINGTON POST (Jan. 10, 2016), https://www.washingtonpost.com/local/public-safety/the-new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bccac-8e15-11e5-baf4-bdf37355da0c_story.html.

11. Matt Apuzzo et al., *U.S. Visa Process Missed San Bernardino Wife's Zealotry on Social Media*, N.Y. TIMES, Dec. 13, 2015, at A1.

12. *See* Oliver Wright, *ISIS plotting cyber warfare to kill people in UK, claims George Osborne*, INDEPENDENT (Nov. 16, 2015), http://www.independent.co.uk/news/uk/politics/paris-terror-attack-uk-government-to-invest-2bn-in-cyber-force-to-combat-online-terror-threats-a6737071.html.

13. *Id.*

At a minimum, this means an increase in efforts to follow information placed online through public sites. "The International Association of Chiefs of Police reports that 95% of police agencies use social media (mostly Facebook, Twitter and YouTube) in their work. Last year, social media sites helped crack a case for 79% of these agencies."[14] In an MTV interview, Sergeant Adrian Acevedo of New Jersey's South Orange Police Department explained that the police "had a very big problem with flash mobs [which were] designed to come and do crime. We quickly realized that these groups of people, which sometimes could be in excess of 300 people, could mobilize using social media within an hour's time."[15] He noted that obtaining private information requires a subpoena or warrant but that anything shared with friends might be made available to the police by those friends.[16]

Sergeant Acevedo was also asked about the practice of "catfishing."[17] "A catfish is someone who pretends to be someone they're not using Facebook or other social media to create false identities, particularly to pursue deceptive online romances."[18] Sergeant Acevedo acknowledges that it is occasionally done by law enforcement but suggests that it is too much of an investment for normal policing procedures.[19] Still, it does occur, and in January 2015, the Drug Enforcement Agency (DEA) even agreed to settle a catfishing lawsuit brought by Sondra Arquiett after the Justice Department used her photographs and those of her son and niece in a false account for investigative purposes.[20] The DEA settled the matter by paying $134,000 but the agency did not admit wrongdoing.[21]

If intelligence surveillance is extended to discover and preempt terrorist activity from groups like ISIS, it is also likely that many online sites use catfishing techniques to introduce potential terrorists to security officials. Governmental sites could present themselves as sympathetic to extremist positions to identify potential terrorists and learn how social media is being used to recruit new participants.

---

14. Deepa Lakshim, *We Asked a Cop How Police Really Use Social Media to Solve Crimes*, MTV NEWS (Jan. 22, 2015), http://www.mtv.com/news/2056442/police-social-media-interview/.

15. *Id.*

16. *Id.*

17. *Id.*

18. URBAN DICTIONARY, http://www.urbandictionary.com/define.php?term=catfish (last visited Nov. 10, 2016).

19. Lakshim, *supra* note 14.

20. Carl Williott, *Woman Gets a Six-Figure Payday After The DEA Stole Her Identity On Facebook*, MTV NEWS (Jan. 21, 2015), http://www.mtv.com/news/2054976/fake-facebook-account-government-dea-lawsuit-settle/.

21. *Id.*

Perhaps the most tangible effect of this terrorist activity is the momentum it provided to enact the Cybersecurity Act of 2015,[22] a variation of the Cybersecurity Information Sharing Act (CISA) that had earlier stalled in Congress.[23] The omnibus $1.1 trillion spending law[24] also includes hundreds of millions of dollars to increase cybersecurity for the Internal Revenue Service, Environmental Protection Agency, and other agencies.[25]

As described by the House of Representatives, the Cybersecurity Act is merely "a voluntary cybersecurity information sharing process that will encourage public and private sector entities to share cyber threat information, without legal barriers and the threat of unfounded litigation—while protecting private information."[26] The Cybersecurity Act identifies Homeland Security as the primary resource for information sharing and creates a system to encourage real-time threat information reporting.[27]

> [T]he Director of National Intelligence, the Secretary of Homeland Security, the Secretary of Defense, and the Attorney General, in consultation with the heads of the appropriate Federal entities, shall jointly develop and issue procedures to facilitate and promote—
>
> (1) the timely sharing of classified cyber threat indicators and defensive measures in the possession of the Federal Govern-

22. Cybersecurity Act of 2015, Pub. L. No. 114-113.

23. Everett Rosenfeld, *The controversial 'surveillance' act Obama just signed*, CNBC (Dec. 22, 2015), http://www.cnbc.com/2015/12/22/the-controversial-surveillance-act-obama-just-signed.html ("Oregon Sen. Ron Wyden . . . implied that the information sharing provisions are worse than in previous incarnations . . . . The latest version of CISA is the worst one yet—it contains substantially fewer oversight and reporting provisions than the Senate version did.").

24. *Id.*

25. Pub. Law No. 114-113 (The FDA is to receive at least $28,000,000 for cybersecurity requirements; the IRS is to receive at least $290,000,000 "to improve the identification and prevention of refund fraud and identity theft, and to enhance cybersecurity to safeguard taxpayer data." The Department of Homeland Security is to receive at least $100,000,000 "to safeguard and enhance systems." And "the Environmental Protection Agency, $27,000,000 . . . to be used solely to meet Federal requirements for cybersecurity implementation."). *Id.*

26. *Id.* (quoting HOUSE COMMITTEE ON RULES, https://rules.house.gov/sites/republicans.rules.house.gov/files/114/PDF/114-SAHR2029ca-MP.pdf (last visited Nov. 10, 2016) ("The Cyber Security Act of 2015 (Division N) . . . includes provisions to improve federal network and information system security, provide assessments on the federal cybersecurity workforce, and provide reporting and strategies on cybersecurity industry-related and criminal-related matters."). *Id.*

27. *Id.*

> ment with representatives of relevant Federal entities and non-Federal entities that have appropriate security clearances;
> (2) the timely sharing with relevant Federal entities and non-Federal entities of cyber threat indicators, defensive measures, and information relating to cybersecurity threats or authorized uses under this title, in the possession of the Federal Government that may be declassified and shared at an unclassified level . . . .[28]

The public sector is not mandated by the Cybersecurity Act to reveal threats, but instead granted immunity from tort liability and antitrust actions related to the disclosures.[29] The government's adoption of the Cybersecurity Act incentivizes reporting of "cyber threat indicators" and "defensive measures" the organization is taking to protect against cyber threats.[30] In providing protection from liability, the law now offers explicit authorization for

28. *Id.* at Div. N, § 103.

29. *Id.* at Div. N, § 104(b)(4).

30. *Id.* at Div. N, §§ 102(6)–(7).

> (6) CYBER THREAT INDICATOR.—The term "cyber threat indicator" means information that is necessary to describe or identify—
> (A) malicious reconnaissance, including anomalous patterns of communications that appear to be transmitted for the purpose of gathering technical information related to a cybersecurity threat or security vulnerability;
> (B) a method of defeating a security control or exploitation of a security vulnerability;
> (C) a security vulnerability, including anomalous activity that appears to indicate the existence of a security vulnerability;
> (D) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system to unwittingly enable the defeat of a security control or exploitation of a security vulnerability;
> (E) malicious cyber command and control;
> (F) the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat;
> (G) any other attribute of a cybersecurity threat, if disclosure of such attribute is not otherwise prohibited by law; or
> (H) any combination thereof.
> (7) DEFENSIVE MEASURE.—
> (A) IN GENERAL.—Except as provided in subparagraph (B), the term "defensive measure" means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

employing defensive measures against attacks without fear of legal liability.[31] The law provides little more than a fig leaf for privacy protection,[32] so only the development of final implementing regulations will determine whether there are meaningful safeguards from the potential abuse of the data sharing provisions to intrude on individual privacy.[33]

The ability to use the Cybersecurity Act of 2015 to promote the sharing of information about malicious attacks and the protections the law affords to private actors will have increasing reach over time as companies begin to view the ability to share as a duty to take reasonable precautions. Over time, the Cybersecurity Act of 2015 is likely to set a new corporate standard for threat disclosure and a new paradigm for public–private threat coordination.[34]

> (B) EXCLUSION.—The term "defensive measure" does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by—
> (i) the private entity operating the measure; or
> (ii) another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

31. *Id.* at Div. N, § 104(b)(1).

32. *See* Pub. L. No. 114-113 at Div. N, § 105(b)(3).

> [C]onsistent with the need to protect information systems from cybersecurity threats and mitigate cybersecurity threats—
> (A) limit the effect on privacy and civil liberties of activities by the Federal Government under this title;
> (B) limit the receipt, retention, use, and dissemination of cyber threat indicators containing personal information of specific individuals or information that identifies specific individuals, including by establishing—
> (i) a process for the timely destruction of such information that is known not to be directly related to uses authorized under this title; and
> (ii) specific limitations on the length of any period in which a cyber threat indicator may be retained;
> (C) include requirements to safeguard cyber threat indicators containing personal information of specific individuals or information that identifies specific individuals from unauthorized access or acquisition, including appropriate sanctions for activities by officers, employees, or agents of the Federal Government in contravention of such guidelines . . . .

33. *See id.* at Div. N, § 202.

34. *Cybersecurity Act of 2015 Signed Into Law*, SIDLEY AUSTIN (Dec. 22, 2015), http://www.sidley.com/news/2015-12-21_privacy_update ("The Cybersecurity Act emphasizes that participation in the information sharing framework is vol-

Commercial enterprises and governmental agencies are not alone in these efforts. Hacktivist organizations such as Anonymous have actively engaged ISIS.[35] They "can make legitimate communications and business difficult to carry out, or even interfere with the intelligence community's efforts . . . . If Anonymous shuts down a terrorist Web site or online forum that government agents have already infiltrated, this could hinder valuable counterterrorism surveillance and data collection."[36]

The U.S. government, like many throughout the world, recognizes that much of the recruiting, coordinating, and collaborating is taking place in Cyberspace.[37] President Barack Obama made this statement regarding these efforts:

> Terrorist groups like al Qaeda and ISIL deliberately target their propaganda in the hopes of reaching and brainwashing young Muslims, especially those who may be disillusioned or wrestling with their identity. That's the truth. The high-quality videos, the online magazines, the use of social media, terrorist Twitter accounts—it's all designed to target today's young people online, in cyberspace.[38]

President Obama called upon the public to get involved in identifying these potential terrorists before attacks have occurred, even before these individuals are fully committed to acts of terrorism: "We have to recognize that our best partners in all these efforts, the best people to help protect individuals from falling victim to extremist ideologies are their own communities, their own family members."[39]

Organizations such as Anonymous have taken up the challenge. In February 2015, the self-proclaimed hacktivist collective released 9,200 ISIS Twitter account handles to the public.[40] Anonymous used the hashtag "#CtrlSec" to flag ISIS accounts and allow Twitter sufficient information to shut these accounts down.[41]

---

untary and prohibits conditioning any government benefit on participating. Participation may nevertheless become industry standard or be required through contractual or other legal obligations.").

35. Greenemeier, *supra* note 8.

36. *Id.*

37. Michael Howard, *Is Twitter Catfishing ISIS?*, DAILY BEAST (Mar. 17, 2015 7:40 AM), http://www.thedailybeast.com/articles/2015/03/17/is-twitter-catfishing-isis.html.

38. *Id.*

39. *Id.*

40. *Id.*

41. *Id.*

"Social media is not the only online platform for terrorists . . . . There have been countless blogs, sites, and social media profiles devoted to promoting terrorist ideals, but Al Qaeda's Inspire Magazine is the first to combine propaganda with how-to killing guides."[42] As a result, the ideals of an open, information-based global village took a very dark turn in 2015 as the central focus on online attention has been combatting terrorism and the highly efficient use terrorists make of cyberspace to stage attacks.

A. Privacy in Cyberspace and Mobile: The Short-Lived Impact of Edward Snowden

The tone of public discourse in privacy and anti-terrorist activity has vacillated significantly from 2013 through much of 2016. In June 2013, Edward Snowden, a government contractor, revealed to the Guardian newspaper and other media sources that he had illicitly copied classified materials and was making them available to the press to highlight what Snowden believed were illegal surveillance activities by the U.S. government.[43] Snowden stole and released the information because he believed "the public needs to decide whether these programs and policies are right or wrong."[44]

As the scope of the stolen cache of information was revealed, Snowden elected to flee the United States, and currently resides in Russia under a temporary visitor status.[45] Reports vary widely on the scope of the information released, but credible estimates suggest at least 58,000 documents were copied and disclosed, though vastly fewer were published by media sources.[46]

Three years later, officials have shed little light on the characterization and impact of Snowden's disclosures. In September 2015, James Clapper, the Director of National Intelligence, acknowledged that Snowden's leaks

42. *Id.*

43. *See, e.g.*, Mark Mazzetti & Michael Schmidt, *Ex-Worker at C.I.A. Says He Leaked Data on Surveillance*, N.Y. TIMES (Jun. 10, 2013), http://www.nytimes.com/2013/06/10/us/former-cia-worker-says-he-leaked-surveillance-data.html?_r=0; Scott Shane, *Ex-Contractor is Charged in Leaks on N.S.A. Surveillance*, N.Y. TIMES (June 22, 2013), http://www.nytimes.com/2013/06/22/us/snowden-espionage-act.html; Tim Bakken, *The Prosecution of Newspapers, Reporters, and Sources for Disclosing Classified Information: The Government's Softening of the First Amendment*, 45 U. TOL. L. REV. 1, 28 (2013).

44. Mazzetti & Schmidt, *supra* note 43.

45. Kevin Drum, *Edward Snowden Didn't Expose the NSA's Bulk Phone Collection Program. Leslie Cauley Did.*, MOTHER JONES (Jun. 4, 2015), http://www.motherjones.com/kevin-drum/2015/06/edward-snowden-didnt-expose-nsas-bulk-phone-collection-program-leslie-cauley-did.

46. Mark Hosenball, *UK asked N.Y. Times to destroy Snowden material*, REUTERS (Aug 30, 2013, 1:54 PM), http://www.reuters.com/article/us-usa-security-snowden-nytimes-idUSBRE97T0RC20130830.

"forced some needed transparency."[47] Clapper quickly qualified his remarks, explaining that Snowden "exposed so many other things that had nothing to do with so-called domestic surveillance or civil liberties and privacy in this country."[48]

Clapper described only one area of direct harm caused by the leaks.[49] The day after his comments, Guardian journalist Glenn Greenwald wrote a story regarding an important program operating in Afghanistan, "the program was shut down by the government of Afghanistan, which was the single most important source of force protection and warning for our people in Afghanistan."[50] Government officials, both publicly and privately, lament the significant intelligence damage and the lives placed at risk by the Snowden revelations, but few specific incidents will be described on the record.[51] This lack of information fuels belief among Snowden's supporters that officials are overstating the harms.[52]

Snowden's disclosures included documentation suggesting that the United States was spying on European Union officials by obtaining access to their computer networks, audio surveillance equipment, email servers, and internal documents.[53] Another document revealed that as of April 5, 2013, there were 117,675 foreign nationals targeted for ongoing surveillance.[54]

Most surprising for many, was the knowledge that the NSA had the ability to receive live notifications about email and chat activities by these targets.[55] Since the data was coming from the technology company providing the service, this meant that the NSA and the ISPs were coordinating to allow real-time intelligence gathering.[56] This revelation rocked the public trust in the major service providers and may have proved to be one of the most sig-

47. Jamie Crawford, *Top Intel Official: Edward Snowden Forced 'Needed Transparency'*, CNN (Sept. 9, 2015), http://www.cnn.com/2015/09/09/politics/james-clapper-edward-snowden-transparency.

48. *Id.*

49. *Id.*

50. *Id.*

51. Jason Leopold, *Official Reports on the Damages Causes by Edward Snowden's Leaks Are Totally Redacted*, VICE NEWS (Feb. 25, 2015), https://news.vice.com/article/official-reports-on-the-damage-caused-by-edward-snowdens-leaks-are-totally-redacted.

52. *See* Crawford, *supra* note 47.

53. *See* Dana Liebelson, *5 Intriguing New NSA Revelations From Edward Snowden*, MOTHER JONES (Jul. 1, 2013, 1:06 PM), http://www.motherjones.com/politics/2013/06/5-new-revelations-nsa-spying-snowden.

54. *Id.*

55. *Id.*

56. *Id.*

nificant long-term impacts of the revelations.[57] This collaboration was further substantiated by the revelation that the FBI's data interception unit was operating from inside the premises of the private telecommunications companies.[58]

The Snowden disclosures created significant angst between U.S. and EU governments over the allegations of international spying among allies.[59] The European Parliament characterized Snowden as a hero for revealing the spying against Germany.[60]

The Snowden leaks that had the greatest legislative impact, however, are those related to the bulk collection of telephone data authorized by § 215 of the USA PATRIOT Act.[61] Ironically, the bulk data collection was specified in the statute and covered by news reports as early as 2006. *USA Today* correspondent Leslie Cauley had already alerted the public that the NSA's goal is "to create a database of every call ever made." She had already shown that "[w]ith access to records of billions of domestic calls, the NSA has gained a secret window into the communications habits of millions of Americans."[62] But the legislature seemed only to respond years later when Snowden detailed the same information.

Section 215 of the USA PATRIOT Act and its counterpart, § 2703(d) of the Stored Communications Act, both provide the government access to non-

57. Chris Paoli, *One Year Post-Snowden: Shattered Trust Is Hard to Repair*, REDMOND MAG. (Jul. 29, 2014), https://redmondmag.com/articles/2014/08/01/trust-is-hard-to-repair.aspx.

58. *See* Liebelson, *supra* note 53 (quoting Bill Binney, a former senior NSA official who had attempted to become a whistleblower under the federal statute).

59. Notwithstanding the revelations that the United States systematically spies on its allies, the government continued to refuse any adjustment to the prison sentence of Jonathan Pollard, the only U.S. citizen convicted of spying for a U.S. ally. Pollard was convicted of spying for Israel in 1987. On Nov. 20, 2015, he was released from prison, having served thirty years of his life sentence and becoming eligible for "mandatory" parole. *See* Sonia Moghe, *Convicted Israel Spy Jonathan Pollard Free After 30 Years*, CNN (Nov. 20, 2015, 7:47 PM), http://www.cnn.com/2015/11/20/us/jonathan-pollard-israel-spy-release/.

60. Jay Newton-Small, *U.S. Allies Still Angry at Snowden's Revelations of U.S. Spying*, TIME (Oct. 04, 2013), http://nation.time.com/2013/10/04/u-s-allies-still-angry-at-snowdens-revelations-of-u-s-spying/ ("The European Parliament this week named Edward Snowden a finalist for its prestigious human rights award, the Sakharov Prize for Freedom of Thought . . . . Snowden . . . revealed that the U.S. monitored Germany as closely as it does China or Russia, intercepting some 500 million communications monthly.").

61. Shaun B. Spencer, *Data Aggregation and the Fourth Amendment*, 19 J. INTERNET L. 13, 16 (2015) ("Since 2006, the government has relied on Section 215 of the USA Patriot Act to collect telephone metadata on telephone calls made to or from telephone numbers in the United States.").

62. Drum, *supra* note 45.

content records related to telephone activities.[63] Section 215, however, was applied in a vastly broader manner. Items subject to the warrants include anything "relevant" to an investigation.[64] The government expanded the definition of relevant in a way that made unrelated telephone metadata relevant to the subject of investigations merely because the size of the database improved the quality of the data.[65] Most actions under § 215 are heard by The United States Foreign Intelligence Surveillance Court (FISC or FISA Court).[66]

63. In upholding the constitutionality of Section 215, a U.S. Foreign Intelligence Surveillance Court (FISC or FISA Court) reviewed the difference between the two provisions:

> For non-content records production requests, such as the type sought here, Section 2703(c) provides a variety of mechanisms, including acquisition through a court order under Section 2703(d). Under this section, which is comparable to Section 215, the government must offer to the court "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation." *Id.* § 2703(d) (emphasis added). Section 215, the comparable provision for foreign intelligence purposes, requires neither "specific and articulable facts" nor does it require that the information be "material." Rather, it merely requires a statement of facts showing that there are reasonable grounds to believe that the records sought are relevant to the investigation.

In re F.B.I. for an Order Requiring Prod. of Tangible Things from [Redacted], No. BR 13-109, 2013 WL 5741573, at *4 (FISA Ct. . Aug. 29, 2013). Despite the lower privacy protection afforded by Section 215, the decision found the other provisions of the law sufficient to be consistent with Smith v. Maryland, 442 U.S. 735 (1979), which established a very low bar for public protection of intrusion into non-call information. *Id.*

64. *See* Am. Civil Liberties Union v. Clapper, 785 F.3d 787, 812 (2d Cir. 2015).

> [T]he government takes the position that the metadata collected—a vast amount of which does not contain directly "relevant" information, as the government concedes—are nevertheless "relevant" because they may allow the NSA, at some unknown time in the future, utilizing its ability to sift through the trove of irrelevant data it has collected up to that point, to identify information that is relevant. We agree with appellants that such an expansive concept of "relevance" is unprecedented and unwarranted.

65. *Id.*

66. *See About the Foreign Intelligence Surveillance Court*, U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT, http://www.fisc.uscourts.gov/about-foreign-intelligence-surveillance-court, (last visited Nov. 10, 2016) ("The Foreign Intelligence Surveillance Court was established by Congress in 1978. The Court entertains applications made by the United States Government for approval of electronic surveillance, physical search, and certain other forms of investigative actions for foreign intelligence purposes."). The FISA Court was

Section 215 decisions by the FISA Court are made after *ex parte* hearings, and both the proceedings and the notifications are generally not published.[67] Still, a number of federal district and appellate circuit courts differ sharply on the constitutionality of § 215 under traditional Fourth Amendment jurisprudence.[68]

Prior to the Snowden revelations, most debate over the constitutionality of § 215 was held within courtrooms. Afterwards, however, questioning its propriety became a mainstream topic. President Obama addressed the issue and Snowden's role:

> [T]he combination of increased digital information and powerful supercomputers offers intelligence agencies the possibility of sifting through massive amounts of bulk data to identify patterns or pursue leads that may thwart impending threats. It's a powerful tool. But the government collection and storage of such bulk data also creates a potential for abuse . . . . America's capabilities are unique, and the power of new technologies means that there are fewer and fewer technical constraints on what we can do . . . .
>
> And for these reasons, I indicated in a speech at the National Defense University last May that we needed a more robust public discussion about the balance between security and liberty. Of course, what I did not know at the time is that within weeks of my speech an avalanche of unauthorized disclosures would spark controversies at home and abroad that have continued to this day.
>
> Given the fact of an open investigation, I'm not going to dwell on Mr. Snowden's actions or his motivations . . . . [T]he sensational way in which these disclosures have come out has often shed more heat than light, while revealing methods to our adversaries that could impact our operations in ways that we might not fully understand for years to come.[69]

---

established under the Foreign Intelligence Surveillance Act (FISA). 50 U.S.C. §§ 1801–1885c (2015).

67. *See id.* ("Pursuant to FISA, the Court entertains applications submitted by the United States Government for approval of electronic surveillance, physical search, and other investigative actions for foreign intelligence purposes. Most of the Court's work is conducted ex parte as required by statute, and due to the need to protect classified national security information.").

68. *See* U.S. v. Jones, 132 S. Ct. 945 (2012); Smith v. Maryland, 442 U.S. 735 (1979); Spencer, *supra* note 61, at 16–17.

69. Barack Obama, Speech on NSA Reforms at The Justice Department (Jan. 17, 2014) (transcript available at https://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html).

The effort to reform § 215 culminated in the passage of the USA FREEDOM Act.[70] In terms of direct legislative change triggered by the Snowden revelations, this modification is likely the only tangible result of his efforts. Under the new law, bulk collection is no longer permitted.[71] But the government has the ability to utilize the data, which continues to be available from the telephone companies.[72]

In practice, very few changes may result of the new law. "It addresses . . . the domestic phone records collection. But it does nothing to affect . . . the NSA's collection of foreign Internet content from U.S. tech companies, a program that sweeps up lots of American communications."[73] The USA FREEDOM Act addresses some of the problems surrounding the FISA Court secrecy but only modestly.[74] And it does nothing to change foreign intelligence gathering or efforts by the NSA to thwart encryption and to discourage corporations from providing effective encryption tools to the public.[75]

Snowden faces serious criminal charges and has already been indicted on three charges brought by the United States.[76] The first charge is that of theft of government property.[77] The other two charges are forms of espionage, specifically unauthorized communication of national defense information[78] and willful communication of classified communications intelligence information to an unauthorized person.[79] Notably, neither of the espionage charges require that the information be made available to an enemy state.[80] As a result of the nature of the charges and the scope of the theft, which was

70. *See* Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, Pub. L. No. 114-23, 129 Stat. 268; *In re* Application of the F.B.I. for an Order Requiring the Production of Tangible Things, No. BR 15-75 & Misc. 15-01 (FISA Ct. June 29, 2015), http://www.fisc.U.S.C.ourts.gov/sites/default/files/BR%2015-75%20Misc%2015-01%20Opinion%C20and%20Order_0.pdf.; Spencer, *supra* note 61, at 17.

71. Ken Dilanian, *6 Things to Know About the Newly Approved USA Freedom Act*, PBS NEWSHOUR (June 3, 2015 at 11:19, AM EST), http://www.pbs.org/newshour/rundown/questions-answers-newly-approved-usa-freedom-act/.

72. *See id.*

73. *See id.*

74. *See id.*

75. *See id.*

76. Peter Finn & Sari Horwitz, *U.S. Charges Snowden with Espionage*, WASH. POST (Jun. 21, 2013), https://www.washingtonpost.com/world/national-security/us-charges-snowden-with-espionage/2013/06/21/507497d8-dab1-11e2-a016-92547bf094cc_story.html.

77. 18 U.S.C. § 641 (2015).

78. *Id.* § 793(d).

79. *Id.* § 798(a)(3).

80. *Id.*; *id.* § 793(d).

significantly broader than that necessary to alert the public regarding illegal governmental activities, Snowden will likely find it difficult to mount a compelling legal defense.[81]

Although the Snowden revelations made a great deal of difference to the public perception of privacy in 2013, they seem quaint in light of the 2015 focus on terrorism and the efforts by the United States and foreign governments to use these tools in an effort to anticipate terrorist activities. For better or worse, the focus on privacy protection has been largely dropped from the current agenda.

B. Undermining International Commerce: The Other Impact of Edward Snowden

Although the impact of Edward Snowden's revelations had little effect beyond minor changes to § 215, his disclosures have had a much greater resonance internationally.[82] In part, this may be because the European Union has long had greater individual protection from unauthorized disclosure of private information for its citizens than that afforded to the citizens of the United States.[83]

Privacy protection is best characterized as having two separate components: protection from the government's unauthorized intrusion into its citizens and protection from corporate or private individuals' intruding into the lives of others.[84] One of the ironies of the Snowden revelations is that his focus was on improper government behavior, but the effect of the disclosures will more directly impact corporate policies and access for U.S. companies to operate in European markets.[85]

The European Union has long had greater individual protection from unauthorized disclosure of private information for its citizens than that afforded to the citizens of the United States.[86] In 1995, the European Union adopted a comprehensive data directive to protect the privacy and informa-

81. Crawford, *supra* note 47.

82. *See* Richard J. Peltz-Steele, *The Pond Betwixt: Differences in the US-EU Data Protection/Safe Harbor Negotiation*, 19 J. INTERNET L. 1 (2015).

83. *Id.* at 15 ("Both privacy and data protection are today part of the fundamental rights system of Europe, a component of the amalgamated constitution of the European Union. Both are part of the legislative and regulatory state at the national and federal levels. This remarkable ubiquity of privacy and data protection in European law has come into being substantially in just the last half century.").

84. Larry Magid, *Protecting Your Privacy From Corporations, The Government and You*, FORBES (Dec. 31, 2013), http://www.forbes.com/sites/larrymagid/2013/12/31/protecting-your-privacy-from-corporations-the-government-and-you/.

85. *Id.*

86. *See id.*

tion of the residents of all member states.[87] Numerous additional directives expanded and clarified the regime of data and privacy protection in Europe while the U.S. legal system only added sectoral privacy for health records, financial records, and various types of information.[88]

While these systems have dramatically diverged, they are both structured around the common concepts of notice and choice.[89] Notice relates to the transparency of data practices while choice provides consumers the ability to give or withhold consent to the collection or use of data.[90] Notice and choice became the common ground that enabled the European Union to ignore these significantly different data practices.[91] The agreement was formalized through the adoption of the FTC Safe Harbor provisions and EU Commission Directive (2000/520).[92]

In actuality, the agreement was likely illusory. The "notice" given to consumers is often done so in turgid, hard-to-read, difficult-to-access end user license agreements which remain subject to change at the whim of the data collector.[93] Because opt-out schemes make it cumbersome and difficult to actually opt-out, consent is often artificial.[94] Moreover, opt-out schemes often condition the use of company services on data disclosures and data resale, which turns disclosure into a consumer-cost rather than a necessary

87. DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA, 1995 O.J. (L 281) 31.

88. *See generally* Peltz-Steele, *supra* note 82, at 16–20; Joel R. Reidenberg et al., *Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding*, 30 BERKELEY TECH. L.J. 39, 44–49 (2015).

89. Reidenberg, *supra* note 88, at 43–44.

90. *Id.*; BUREAU OF CONSUMER PROT., FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS 7 (1998), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

91. *See* FED. TRADE COMM'N, FEDERAL TRADE COMMISSION 2013 PRIVACY AND DATA SECURITY UPDATE (2014) ("The U.S.-E.U. Safe Harbor Framework provides a way for businesses to transfer personal data from the EU to the U.S. in a manner consistent with EU law. The U.S. Department of Commerce administers the voluntary framework, and the FTC provides an enforcement backstop. To participate, a company must self-certify annually to the Department of Commerce that it complies with the seven privacy principles required to meet the EU's adequacy standard: notice, choice, onward transfer, security, data integrity, access, and enforcement.").

92. *See* Commission Decision (EC) No. 520/2000 of 26 July 2000, pursuant to Directive 95/46/EC of the European Parliament and of the Council, 2000 O.J. (L 215) 1 [hereinafter Commission Decision (EC) No. 520/2000].

93. *See* Reidenberg, *supra* note 88, at 46–49.

94. *See generally id.* at 48–49.

part of the customer transaction.[95] Despite the privacy protections purportedly provided by the Safe Harbor provisions, multinational corporations could still transfer information between the United States and the EU without violating European data privacy directives.[96]

Shortly after Snowden made his disclosures about U.S. surveillance in *The Guardian*,[97] Austrian citizen Maximilian Scherms brought a complaint to the Irish Data Protection Commissioner related to the transfer of data by Facebook Ireland, Ltd. to Facebook, Inc. in the United States.[98] Although the Irish Data Protection Commission did not address the case, it triggered a review by the Court of Justice of the European Union.[99] There, the EU Court specifically addressed the intrusion by the NSA under the PRISM program revealed by Snowden.[100]

Following his success in the Court of Justice, Max Schrems began extending his complaint against Facebook to more data protection agencies.[101] He has filed actions in Ireland, Germany, and Belgium.[102] Schrems is personally focused on companies in the United States identified as facilitating NSA

95. *See supra* text accompanying note 88.

96. *See* Jaap Kronenberg, *EU Court Blocks Transfer of Personal Data to the US via 'Safe Harbor' Arrangement*, LEGAL KNOWLEDGE PORTAL (Oct. 22, 2015), http://legalknowledgeportal.com/2015/10/22/eu-court-blocks-transfer-of-personal-data-to-the-us-via-safe-harbor-arrangement/.

97. Glenn Greenwald et al., *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, THE GUARDIAN (June 11, 2013), https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

98. Kronenberg, *supra* note 96.

99. Case C-362/14, Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:627, http://curia.europa.eu/juris/liste.jsf?language=EN&jur=C,T,F&num=C-362/14&td=ALL.

100. *Id.* (The case notes that "all companies involved in the PRISM programme [a large-scale intelligence collection programme], and which grant access to U.S. authorities to data stored and processed in the [United States], appear to be Safe Harbour certified . . . ." The effect is that PRISM and the USA PATRIOT Act create "a number of legal bases under U.S. law allow[ing] large-scale collection and processing of personal data" from EU residents. The data may be "accessed and further processed by U.S. authorities beyond what is strictly necessary and proportionate to the protection of national security as foreseen under the exception provided in (Decision 2000/520).").

101. Glyn Moody, *After Safe Harbor Ruling, Legal Moves to Stop Facebook from Sending Data to US*, ARS TECHNICA (Dec. 2, 2015), http://arstechnica.com/tech-policy/2015/12/after-safe-harbour-ruling-legal-moves-to-force-facebook-to-stop-sending-data-to-us/.

102. *Id.*

surveillance, such as Apple, Google, Microsoft and Yahoo.[103] But the court decision affects all U.S. companies relying on the Safe Harbor provisions and the Safe Harbor decision of the EU Commission (2000/520).[104]

According to the Federal Trade Commission (FTC), "U.S. and EU officials are currently discussing the development of an enhanced mechanism that protects privacy and provides an alternative method for transatlantic data transfers."[105] The remainder of the FTC's advice focuses on robust data privacy protections by the companies certifying data transfers within the European Union.[106] The advice simply ignores that it is the U.S. government's access to the private data, not the actions of the data holders, that has triggered the invalidation of the Safe Harbor provisions.

The result of this work is the EU-U.S. Privacy Shield Framework, which serves to replace the Safe Harbor.[107] The European Union has certified that the changes to the data protection are sufficient to meet the requirements of the European Court of Justice based on U.S. commitments to enhance privacy protections.[108] In particular, the United States included assurances

103. *Id.*

104. *See* COMMISSION DECISION (EC) No. 520/2000, *supra* note 92, at 1.

105. *Federal Trade Commission Update on the U.S.-EU Safe Harbor Framework, Safe Harbor Related News & Events*, EXPORT.GOV, https://build.export.gov/main/safeharbor/eg_main_018244 (last updated Nov. 6, 2015).

106. *Id.*

107. *See U.S.-EU & U.S.-Swiss Safe Harbor Frameworks Advisory*, http://2016.export.gov/SAFEHARBOR/ ("On July 12, [2016] U.S. Secretary of Commerce Penny Pritzker joined European Union Commissioner Věra Jourová to announce the approval of the EU-U.S. Privacy Shield Framework, which will replace the U.S.-EU Safe Harbor. Secretary Pritzker announced that the Department will start accepting certifications on August 1st [2016].").

108. Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield (notified under document C(2016) 4176) (Text with EEA relevance), 2016 O.J. (L 207) 1, 3 at ¶ 13, http://eur-lex.europa.eu/eli/dec_impl/2016/1250/oj [hereinafter Commission Implementing Decision 2016/1250] ("The Commission . . . concludes that the United States ensures an adequate level of protection for personal data transferred under the EU-U.S. Privacy Shield from the Union to self-certified organisations in the United States."). *See also The EU-U.S. Privacy Shield*, EUROPEAN COMMISSION, http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm ("This new framework protects the fundamental rights of anyone in the EU whose personal data is transferred to the United States as well as bringing legal clarity for businesses relying on transatlantic data transfers. The new arrangement includes: strong data protection obligations on companies receiving personal data from the EU; safeguards on U.S. government access to data; effective protection and redress for individuals; [and] annual joint review to monitor the implementation.).

that it would provide oversight of self-certifying organizations and enforcement of the Privacy Shield provisions.[109] The United States also promised the government intrusion into privacy rights for "national security, law enforcement or other public interest purposes . . . will be limited to what is strictly necessary to achieve the legitimate objective in question . . . ."[110] Nonetheless, the new Privacy Shield Framework retains the self-certification that was deeply criticized under the safe harbor provisions.[111]

Schrems suggests that companies could overcome the concerns of NSA spying by adopting comprehensive encryption, a technique that would thwart easy access by the government.[112] Given the high level of anti-terrorist collaboration between the nations, it is understandable that a new form of cooperation emerged that adjusts both U.S. and EU expectations of privacy from the government. The concessions made by the United States are rather trivial, so the concessions by the EU were essentially a repudiation of the *Schrems* decision.

II. DOES PRIVACY REGULATION EVEN MATTER? DATA VULNERABILITY CONTINUES TO EXPAND

There has been a corollary with the types of cyber-attacks committed based on 2015's growth of terrorist activities. Data breaches are an ongoing problem for both the private and public sector. Symantec reported that in 2014, "more than 317 million new pieces of malware" were released.[113] Another report noted that in 2014, "the total number of security incidents detected by respondents grew to 42.8 million around the world, up 48 percent from 2013."[114]

2014 was a notable year in cybersecurity for its security breaches, so any review of 2015 must consider the context of the previous year's record-setting quantity and severity of breaches.[115] "Major enterprises like Target, Home Depot, and Sony Entertainment experienced breaches that required the companies to pay hundreds of millions of U.S. dollars to cover costs of the

109. Commission Implementing Decision 2016/1250, *supra* note 108, 32 ¶ 139.

110. *Id.* 32 ¶ 140.

111. *See* Moody, *supra* note 101; Commission Decision (EC) No. 520/2000, *supra* note 92, at 1.

112. *See* Moody, *supra* note 101.

113. Virginia Harrison & Jose Pagliery, *Nearly 1 Million New Malware Threats Released Every Day*, CNN MONEY (April 14, 2015), http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/.

114. ISACA, STATE OF CYBERSECURITY: IMPLICATIONS FOR 2015, AN ISACA AND RSA CONFERENCE SURVEY, CYBERSECURITY NEXUS 2 (2015), http://www.isaca.org/cyber/pages/state-of-cybersecurity-implications-for-2015.aspx.

115. *See id.*

attacks. JP Morgan Chase and other financial institutions were affected even more severely."[116]

The Sony Entertainment attack, though occurring in late 2014, is the most notable because it may have been a state-sponsored form of cyber-warfare, and it reflected a new level of anti-corporate "hacktivism." This attack began after a spokesperson for the foreign ministry of North Korea declared the Sony movie, "The Interview," an "act of terrorism" and promised "merciless" retaliation as a response to the release of the film.[117] Despite this warning in June, Sony elected to continue with the distribution of the film.[118] In November, as the movie release date approached, "skulls appeared on employees' screens with a message threatening to expose 'secrets' from data obtained in a sophisticated hack."[119]

The attack, however, was far more than a mere denial of service attack. A series of interconnected viruses and malware stole emails and documents, published confidential materials including movie scripts, and erased computer drives to cripple the company.[120] A previously unknown group, Guardians of Peace, claimed responsibility and threatened physical attacks against any movie theaters that planned to show the film.[121]

The scale of the attack and the resulting financial harm, combined with terrorist threats, make this a uniquely dangerous attack. Revelations made in January 2015, however, add yet another dimension.[122] The NSA acknowledged that it has concrete information of North Korea's direct involvement with the attack because of U.S. surveillance technology implanted on the North Korean military's systems.[123] The pattern of probing and intrusions took nine months, which suggests that the cyber-efforts began shortly before the North Korean foreign minister made the threatening comments against Sony.[124]

---

116. *Id.*

117. *The Interview: A Guide to the Cyber Attack on Hollywood*, BBC NEWS (Dec. 29 2014), http://www.bbc.com/news/entertainment-arts-30512032.

118. *See id.*

119. *Id.*

120. Kim Zetter, *Sony Got Hacked Hard: What We Know and Don't Know So Far*, WIRED (Dec. 3, 2014, 4:02 PM), https://www.wired.com/2014/12/sony-hack-what-we-know/.

121. *See The Interview: A Guide to the Cyber Attack on Hollywood*, *supra* note 117.

122. *See* David Sanger & Martin Fackler, *N.S.A. Breached North Korean Networks Before Sony Attack, Officials Say*, N.Y. TIMES (Jan. 19, 2015), http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html?_r=1.

123. *See id.*

124. *See id.*

The major North Korean attack on a U.S. corporation (albeit one with strong Asian roots) was followed in 2015 by a direct attack on key U.S. government resources. An ongoing series of attacks breached the records of the United States Office of Personnel Management (OPM).[125] OPM is an independent agency of the United States that recruits, screens, and vets potential employees for U.S. government positions that require any form of governmental clearance.[126] In one of the two reported incidents, personnel data of 4.2 million current and former Federal government employees had been stolen.[127] In the other, "19.7 million individuals that applied for a background investigation, and 1.8 million non-applicants, primarily spouses or co-habitants of applicants" had application information stolen.[128]

The stolen data included Social Security numbers, employment history, residency and educational history, criminal and financial history, fingerprints, information about health, and personal and business acquaintances.[129] On a categorical basis, this includes (almost)[130] the most sensitive personal information stored in any record keeping system.

Like the attack on Sony, government officials believe the OPM attack was directed at the United States by a foreign government.[131] "U.S. investigators believe Chinese hackers are responsible for the massive security breach at nearly every federal government agency, a law enforcement source and another U.S. official told CNN on Thursday."[132] This matters because, unlike other attacks, the OPM attack was designed merely to collect information. "The national security community is now working under the assumption that the Chinese have hundreds of thousands of security clearance forms."[133]

Testifying before the Senate Armed Services Committee, Director of National Intelligence James R. Clapper Jr., characterized the OPM breach as one of "theft or espionage" rather than an "attack" that would presumably

125. *Cybersecurity Incidents*, OFFICE OF PERSONNEL MANAGEMENT, CYBERSECURITY RESOURCE CENTER, https://www.opm.gov/cybersecurity/cybersecurity-incidents/ (last visited Nov. 10, 2016).

126. .*See About OPM*, OFFICE OF PERSONNEL MANAGEMENT, https://www.opm.gov/about-us/ (last visited Nov. 10, 2016).

127. *Cybersecurity Incidents*, *supra* note 125.

128. *Id.*

129. *Id.*

130. *See* discussion of Ashley Madison hack, *infra* notes 139–147 and accompanying text (suggesting that correspondence regarding planned infidelity is perhaps more sensitive than even social security and fingerprint data).

131. Theodore Schleifer, *How China Could Have Hacked the U.S. Government in 10 Steps*, CNN (June 5, 2015, 4:38 PM), http://www.cnn.com/2015/06/05/politics/chinese-data-hack-ten-steps/.

132. *Id.*

133. *Id.*

require a military or cyber-military response.[134] He chose this frame because of the information about U.S. activities revealed by Snowden and others and also to keep tensions between the United States and China from escalating as a result of this successful intrusion into the heart of U.S. information systems.[135]

Nonetheless, by September 2015, the threat had resulted in real-world consequences. *CNN* reported, "[e]mployees of the Central Intelligence Agency, National Security Agency and Defense Intelligence Agency assigned to China are at risk of being exposed . . . ."[136] *The Washington Post* further explained that the comprehensive scope of the OPM attack could enable China to cross-reference the employees in a government facility.[137] Anyone who did not have his or her name in the OPM database could be presumed to have been hired by the CIA rather than through the State Department.[138]

Both the scale of the attack and the lack of a meaningful response have increased the U.S. government's vulnerability. In an age of increased cyber-espionage and terrorism, the loss of control of cyber-security has created a fundamental foreign policy crisis. In the year of cyber-terrorism, the inability to respond may highlight the problems we face for the future.

Despite the governmental vulnerabilities highlighted by the OPM attack, one private company attack has potentially proven even more embarrassing and intrusive. In July 2015, a hacker group identifying itself as "the Impact Team" attempted extortion when it threatened to expose up to ten gigabytes of customer data if the Avid Life Media (ALM) site, Ashley Madison was not removed from the Internet.[139] Ashley Madison is among the most well-known Internet adultery sites. It uses the trademarked slogan, "Life is short. Have an affair."[140]

---

134. Ellen Nakashima & Adam Goldman, *CIA Pulled Officers from Beijing After Breach of Federal Personnel Records*, WASH POST (Sept. 29, 2015), https://www.washingtonpost.com/world/national-security/cia-pulled-officers-from-beijing-after-breach-of-federal-personnel-records/2015/09/29/1f78943c-66d1-11e5-9ef3-fde182507eac_story.html.

135. *Id.*

136. Evan Perez, *U.S. Pulls Spies From China After Hack*, CNN MONEY (Sept. 30, 2015, 9:50 AM), http://money.cnn.com/2015/09/30/technology/china-opm-hack-us-spies/.

137. *See* Nakashima & Goldman, *supra* note 134.

138. *Id.*

139. *See* Kim Zetter, *Hackers Finally Post Stolen Ashley Madison Data*, WIRED (Aug. 18, 2015, 5:55 PM), http://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/.

140. *Id.*

Avid Life Media refused to close down and the Impact Team posted a notice attacking the company for both its morals and its business practices.[141] "We have explained the fraud, deceit, and stupidity of ALM and their members. Now everyone gets to see their data."[142]

The posting by the Impact Team also suggested that the attack was focused on corporate management, not merely the potential adulterers on the site. "Keep in mind the site is a scam with thousands of fake female profiles . . . . 90–95% of actual users are male."[143]

The resulting breach was quite severe. The data breach affected a reported thirty million accounts, "including those of 10,000 American government officials, a handful of celebrities, a few clergymen and, apparently, very few real female profiles.[144] Leaked emails also showed that the company may have hacked into the computer networks of its competitors."[145]

The breach did result in some serious damage to Ashley Madison and its leadership. Approximately one month after the data breach, the company's chief executive, Noel Biderman, stepped down from his leadership role in the company.[146]

Biederman was not alone in leaving his post following a data breach. Amy Pascal left her position at Sony Pictures Entertainment as co-chairwoman following its February 2015 intrusion, and Target chairman and CEO, Gregg Steinhafel, resigned from his position after both the dramatic retail data breach and other missteps that badly tarnished the once-popular retailer.[147]

One additional 2015 data breach is also important to note in the context of long-term consequences of data theft and intrusion. The controversial spyware company known primarily to cybersecurity insiders, Hacking Team, was itself the subject of a major intrusion. The attack exposed over 400 gigabytes of its internal sensitive data on the Internet.[148] "The breached trove includes executive emails, customer invoices and even source code; the com-

141. *Id.*

142. *Id.*

143. *Id.*

144. Nicole Perlrothaug, *Ashley Madison Chief Steps Down After Data Breach*, N.Y. TIMES (Aug. 28, 2015), http://www.nytimes.com/2015/08/29/technology/ashley-madison-ceo-steps-down-after-data-hack.html?_r=0.

145. *Id.*

146. *Id.*

147. *Id.*

148. Andy Greenberg, *Hacking Team Breach Shows A Global Spying Firm Run Amok*, WIRED (July 6, 2015, 10:26 AM), http://www.wired.com/2015/07/hacking-team-breach-shows-global-spying-firm-run-amok/ ("One document pulled from the breached files, for instance, appears to be a list of Hacking Team customers . . . [which] include Azerbaijan, Bahrain, Egypt, Ethiopia, Kazakh-

pany's twitter feed was hacked, controlled by the intruders for nearly 12 hours, and used to distribute samples of the company's hacked files."[149]

The data dump exposed "what appear to be new confirmations that Hacking Team sold digital intrusion tools to authoritarian regimes. Those revelations may be well timed to influence an ongoing U.S. policy debate over how to control spying software . . . ."[150] As with any intrusion of this sort, the information both helps shed light on the activities of the affected company and provides those hoping to gain from such illegal intrusions new insights and tools on how best to proceed.

The latter aspect of this attack should create a new level of concern. Security expert Lior Div notes that the disclosed information "is the equivalent of offering free copies of 'nation-state hacking for dummies' to anyone remotely interested in the topic. Now, novice and/or minimally talented hackers have the capacity to pull off extremely sophisticated hacking operations, a shift that is sure to level the cyber crime playing field."[151]

While this illustration of hacktivism may help take a significant tool away from some authoritarian regimes, it is more likely that it exposed a toolkit to an even greater set of cyber-criminals and terrorists.

III. CONCLUSION

While the Internet may bring the world closer, in 2015 it may have contributed to making the world a more dangerous and existentially more threatening place. Instead of a year defined by increasing individual privacy and holding governments accountable for their spying on their citizens, the increased focus on global terror and significant state-sponsored cyber-attacks placed the focus squarely on security.

The impact of Edward Snowden was lost amidst the physical attacks in London and San Bernardino. China's alleged attack on the OPM and North Korea's attacks on Sony highlighted the difficulty of defining the nature of cyberwarfare and responding when it occurs. The applications of the Cybersecurity Act of 2015 will expand to change the relationship of corporate America with the federal agencies regulating it.

The loss of the US/EU Safe Harbor Agreement further erodes the ease with which lawful information can travel across the globe, but the attack on Ashley Madison reminds us that unauthorized disclosures can occur at a moment's notice. In short, 2015 was a difficult year for cybersecurity, one that

---

stan, Morocco, Nigeria, Oman, Saudi Arabia, Sudan, and several United States agencies including the DEA, FBI and Department of Defense.").

149. *Id.*

150. *Id.*

151. Lior Div, *Why The Hacking Team Breach Further Tips The Scales Against Businesses*, FORBES (Aug. 4, 2015, 12:53 PM), http://www.forbes.com/sites/frontline/2015/08/04/why-the-hacking-team-breach-further-tips-the-scales-against-businesses/.

undermined many of the hopes that a robust online community adds to our global understanding. Hopefully, however, the challenges of the past year will bring a renewed energy to solving the problems facing the global community and build a more transparent and resilient system for the coming years.