CYBER INSECURITY: CONSTITUTIONAL RIGHTS IN THE DIGITAL ERA*

Jennifer M. Paulson**

I. INTRODUCTION

In June 2013, Glenn Greenwald, a columnist for *The Guardian*, boarded a flight to Hong Kong[1] to meet an anonymous source who had been contacting him via encrypted messages for six months.[2] After arriving in Hong Kong, Greenwald stood outside a specified restaurant and waited for a man carrying a Rubik's Cube to walk by.[3] Greenwald, per the source's instructions, asked the man when the restaurant would open.[4] The man replied that the food was bad—a cue for Greenwald to follow him to a hotel room.[5] The man with the Rubik's Cube was Edward Snowden, and the following events materialized into the "most serious compromise of classified information in the history of the U.S. intelligence community."[6]

Snowden turned over thousands of top secret documents to Greenwald that exposed controversial domestic surveillance operations.[7] Over the next month, *The Guardian* published a series of articles detailing the content of the documents, revealing the U.S. government was secretly using private entities to collect mass amounts of data on millions of Americans.[8]

---

* Best Legal Comment (2016), Southern Illinois University Law Journal.

** Jennifer Paulson is a third-year law student at Southern Illinois University who is expecting her JD in May of 2017. She would like to thank her friends and family for all of their support and encouragement, especially Kelly Meredith, who has selflessly devoted herself to the SIU Law Journal as Editor in Chief for the 2016/2017 school year.

1. Roy Greenslade, *How Edward Snowden Led Journalist and Film-maker to Reveal NSA* Secrets, GUARDIAN (Aug. 19, 2013), http://www.theguardian.com/world/2013/aug/19/edward-snowden-nsa-secrets-glenn-greenwald-laura-poitras.
2. Janet Reitman, *Snowden and Greenwald: The Men who Leaked the Secrets*, ROLLING STONE (Dec. 4, 2013), http://www.rollingstone.com/politics/news/snowden-and-greenwald-the-men-who-leaked-the-secrets-20131204.
3. Greenslade, *supra* note 1.
4. *Id.*
5. *Id.*
6. In an interview on the CBS program 60 Minutes, the Central Intelligence Agency deputy director Michael Morell described the Snowden Leaks as such. *60 Minutes: The Deputy Director* (CBS television broadcast Oct. 30, 2013) (transcript available at http://www.cbsnews.com/news/the-deputy-director-mike-morell/).
7. Reitman, *supra* note 2.
8. *See, e.g.*, James Ball et al., *Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security*, GUARDIAN (Sept. 6, 2013), http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security; Glen Greenwald, *NSA Collecting Phone Records of Millions of*

Although the entwinement of the government and private entities naturally occurs to effectuate national security policies and promote public safety, without proper safeguards, this entanglement may threaten fundamental rights as technological advancements enable companies to collect and analyze large amounts of information about their consumers. Because the Constitution is generally a restriction on the government, and not private actors,[9] traditional mechanisms of protecting individual rights such as the Due Process Clause are not applicable in the private sector.[10] Furthermore, a lack of transparency and the inability to articulate a concrete injury from surveillance makes it nearly impossible to challenge government actions, even when Constitutional rights do apply.

Part I of this Comment provides a history of how the government utilizes private entities to acquire data about private persons**.** Part II analyzes how the entwinement of public and private organizations affects fundamental rights. Part III proposes a statute that regulates how the government can use privately collected data, establishes a special court to oversee domestic surveillance, and creates standing by means of a citizen suit.

II. BACKGROUND

As society becomes more dependent on the Internet to facilitate business transactions, social interactions, and tasks associated with everyday living, more data than ever before is being created each second.[11] While it is impossible to tell exactly who stores this data and how it is used,

---

Verizon Customers Daily, GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

9. *See* LEGAL INFORMATION INSTITUTE, *State Action Requirement*, CORNELL U. L. SCH., https://www.law.cornell.edu/wex/state_action_requirement.

> The state action requirement stems from the fact that the constitutional amendment which protect individual rights (especially the Bill of Rights and the 14th Amendment) are mostly phrased as prohibitions against government action . . . Because of this requirement, it is impossible for private parties (citizens or corporations) to violate these amendments, and all lawsuits alleging constitutional violations of this type must show how the government (state or federal) was responsible for the violation of their rights.

Id.

10. *See* Kristen E. Eichensehr, *Public-Private Cybersecurity*, 95 TEX. L. REV. (forthcoming 2017) (observing the "structural differences between the government and private actors" and the absence of "legal obligations, such as requirements of due process and equal protection" in the regulation of private actors).

11. "As of 2012, about 2.5 exabytes of data are created each day, and that number is doubling every 40 months or so. More data cross the Internet every second than were stored in the entire Internet just 20 years ago." Andrew McAfee & Erik Brynjolfsson, *Big Data: The Management Revolution*, 90(10) HARV. BUS. REV. (Oct. 2012), https://hbr.org/2012/10/big-data-the-management-revolution.

big-data is undoubtedly transforming the way private entities communicate with their consumers and increasing the efficiency and effectiveness of business decisions. Big-data, however, is not just used to draw assumptions about our shopping habits or determine business needs: it also provides the national government with new resources to monitor individual behavior. The impalpable nature of cyberspace allows the government to use privately collected data to draw assumptions about its citizens without their knowledge[12] and sometimes without congressional, judicial, or public oversight.[13] Although the rise of big-data presents the government with new intelligence capabilities, enlisting the private sector to assist in surveillance is nothing new in the United States.

A. The Crypto Wars

The Snowden Leak exposed that the government was actively exploiting cybersecurity measures implemented by private organizations in order to maintain surveillance capabilities through clandestine National Security Agency (NSA) operations.[14] Backed by a $250 million a year budget, the Sigint Enabling Project sought to compromise the encryption of everyday Internet communications by working directly with companies to insert backdoors in products and lobbying for encryption standards it could crack.[15] Another program, Operation Bullrun, used supercomputers to decipher encrypted bank communications and medical records.[16] These programs are merely episodes in the saga of the NSA and law enforcement's attempt to control public encryption capabilities, commonly referred to as the "Crypto Wars."[17]

---

12. Margaret Hu, *Big Data Blacklisting*, 67 FLA. L. REV. 1735, 1745-46 (2015) ("[B]ecause of the virtual nature of mass data collection and database screening, and the classified or semi-classified nature of certain programs, the digital mediation of and potential interference with interests can occur without the individual's knowledge or consent.").
13. *See* Am. Civil Liberties Union v. Clapper, 785 F.3d 787, 820 (2d Cir. 2015) ("[O]nly a limited subset of members of Congress had a comprehensive understanding of the [metadata collection] program or its purported legal bases.").
14. *See* Nicole Perlroth, Jeff Larson, & Scott Shane, *N.S.A. Able to Foil Basic Safeguards of Privacy on the Web*, N.Y. TIMES (Sept. 5, 2013), http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html.
15. *Id.*
16. Ball et al., *supra* note 8.
17. *See* Swire & Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416, 417–18 (2012); *see also* Andy Greenberg, *The Father of Online Anonymity Has a Plan to End the Crypto War*, WIRED (Jan. 6, 2016, 7:00 AM), https://www.wired.com/2016/01/david-chaum-father-of-online-anonymity-plan-to-end-the-crypto-wars/ (describing the crypto wars as "the conflict between privacy advocates and governments").

Modern encryption emerged in the 1970s and received almost immediate pushback from the federal government.[18] Professors from Stanford developed an encryption method that would give the public access to strong encryption.[19] When a Massachusetts Institute of Technology (MIT) professor planned to present this information at a conference, the NSA warned him that doing so would violate the International Traffic in Arms Act because foreign nationals would be attending.[20]

As computer technology and encryption developed, "[l]aw enforcement and national security agencies became increasingly concerned that the proliferation of private sector encryption would erode their ability to monitor criminal and foreign entities."[21] However, encryption plays a vital role in our technology-based society, and advocates assert that without encryption, "financial records, business secrets, webmail, medical and legal records, cars, and airplanes" are at risk.[22]

In 1994 the Clinton Administration announced an encryption initiative referred to as the Clipper Chip.[23] The Clipper Chip was an encryption device placed in telecommunication devices such as telephones, fax machines, and computers.[24] The Clipper Chip initiative was adopted as the government standard, but the NSA hoped the government's buying power would force the private sector to adopt it as well.[25] The Clipper Chip purportedly encrypted communications, thereby protecting parties from eavesdroppers.[26] However, the government would hold a decryption key in escrow that, with a court order, it could use to decipher communications.[27] Civil liberties groups strongly opposed the program, warning against

---

18. John T. Soma & Charles P. Henderson, *Encryption, Key Recovery, and Commercial Trade Secret Assets: A Proposed Legislative Model*, 25 RUTGERS COMPUTER & TECH. L.J. 97, 103–04 (1999).
19. *Id.* at 103.
20. *Id.* at 104.
21. Swire & Ahmad, *supra* note 17, at 434. In 2014 James B. Comey, the Director of the Federal Bureau of Investigation, stated: "Encryption isn't just a technical feature; it's a marketing pitch. But it will have very serious consequences for law enforcement and national security agencies at all levels. Sophisticated criminals will come to count on these means of evading detection." James B. Comey, Director Federal Bureau of Investigation, Speech at Brookings Institution Washington, D.C. (Oct. 16, 2014) (transcript available at https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course).
22. *The Crypto Wars: Governments Working to Undermine Encryption*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/document/crypto-wars-governments-working-undermine-encryption (last visited Feb. 25, 2017).
23. Aaron Perkins, *Encryption Use: Law and Anarchy on the Digital Frontier*, 41 HOUS. L. REV. 1625, 1638 (2005).
24. Christopher E. Torkelson, *The Clipper Chip: How Key Escrow Threatens to Undermine the Fourth Amendment*, 25 SETON HALL L. REV. 1142, 1165 at n.125 (1995).
25. Perkins, *supra* note 23.
26. Torkelson *supra* note 24, at 1165.
27. *Id.*

government surveillance and the abuse of privacy rights.[28] Members of the computer and software industries were also among the program's biggest adversaries.[29] They feared their overseas competitors who did not utilize the Clipper Chip would erode the domestic market.[30] The program caved under these pressures and was abandoned by 1996.[31]

In the wake of the Snowden Leaks, encrypted Internet communication drastically increased,[32] and technology companies such as Apple and Google developed more sophisticated encryption methods for their products.[33] Apple began encrypting its devices by default, making it virtually impossible for even the company itself to access data running on its operating software.[34] Government officials spoke out against Apple, arguing that encryption places individuals beyond the law.[35] Tensions finally reached a breaking point in 2015 when a San Bernardino judge issued a court order to Apple, mandating the company assist with a terrorist investigation by creating a backdoor to the iPhone.[36] Apple's CEO, Tim Cook, released a public letter on behalf of Apple, refusing to comply.[37] The legal battle was rendered moot when a third party unlocked the phone for the FBI,[38] but the volatile clash implicates complex legal issues and a tense ideological debate surrounding privacy, national security, and the government's authority over private entities.

---

28. Perkins, *supra* note 23, at 1639.
29. *Id.*
30. *Id.*
31. *See* Parker Higgins, *On the Clipper Chip's Birthday, Looking Back on Decades of Key Escrow Failures*, ELEC. FRONTIER FOUND. (Apr. 16, 2015), https://www.eff.org/deeplinks/2015/04/clipper-chips-birthday-looking-back-22-years-key-escrow-failures.
32. A network equipment company, Sandvine, released a study finding Americans used encryption sixty percent more after the Snowden Leaks than before. Lauren C. Williams, *More People are Encrypting Their Web Traffic in the Wake of NSA Spying Revelations*, THINK PROGRESS (May 17, 2014), https://thinkprogress.org/more-people-are-encrypting-their-web-traffic-in-the-wake-of-nsa-spying-revelations-47f92868d97#.og11idvcu.
33. RONALD GOLDFARB ET. AL., AFTER SNOWDEN: PRIVACY, SECRECY, AND SECURITY IN THE INFORMATION AGE 22 (Thomas Dunne Books, 2015).
34. *See* Joe Miller, *Google and Apple to Introduce Default Encryption*, BBC NEWS (Sept. 19, 2014), http://www.bbc.com/news/technology-29276955.
35. *See* Igor Bobic & Ryan J. Reilly, *FBI Director James Comey 'Very Concerned' About New Apple, Google Privacy Features*, HUFFINGTON POST (Sept. 26, 2014), http://www.huffingtonpost.com/2014/09/25/james-comey-apple-encryption_n_5882874.html.
36. *See* Andrew Blankstein, *Judge Forces Apple to Help Unlock San Bernardino Shooter iPhone*, NBC NEWS (Feb. 16, 2016), http://www.nbcnews.com/storyline/san-bernardino-shooting/judge-forces-apple-help-unlock-san-bernardino-shooter-iphone-n519701.
37. *See* Tim Cook, Apple Customer Letter, *A Message to Our Customers* (Feb. 16, 2016) http://www.apple.com/customer-letter/.
38. Alina Selyuk, *The FBI Has Successfully Unlocked the iPhone Without Apple's Help*, NAT'L PUB. RADIO (Mar. 28, 2016), http://www.npr.org/sections/thetwo-way/2016/03/28/472192080/the-fbi-has-successfully-unlocked-the-iphone-without-apples-help.

B. Commercial Databases

The definition of "big data" is elusive and there are multiple ways to define the term.[39] However, big-data are virtually always high volume, derived from several sources, arrive in various formats at a high speed, and require analysis to be useful.[40] Throughout the past decade, companies have capitalized on big-data through big-data analytics, "the process of examining large data sets to uncover hidden patterns, unknown correlations, market trends, customer preferences and other useful business information."[41] For instance, credit-card companies determined people who bought anti-scuff pads for furniture were more likely to make their payments on time; and Target discovered customers who bought large purses were more likely to be pregnant.[42] Big-data analytics is also useful in the public realm, for example, for "allocating police resources by predicting where and when crimes are most likely to occur; finding associations between air quality and health; or using genomic analysis to speed the breeding of crops like rice for drought resistance."[43]

While big-data analytics can lead to more efficient and effective business decisions while also positively impacting the public domain, big-data has evolved into a largely unregulated and controversial industry.[44] Data-brokers collect, analyze, and package consumer information and sell it to third parties, including the government.[45] "Because the companies involved in the practice are not state actors, Fourth Amendment doctrine does not bar [them] from searching and seizing information about private matters."[46]

---

39. Anne Marie Smith, *Seven Best Practices to Boost Big Data Governance*, TECH TARGET (May 2014), http://searchdatamanagement.techtarget.com/answer/Seven-best-practices-to-boost-big-data-governance-efforts.
40. *Id*.
41 Margaret Rouse, *Big Data Analytics*, TECH TARGET (last updated Oct. 2014), http://searchbusinessanalytics.techtarget.com/definition/big-data-analytics.
42. JEFFREY F. BEATTY & SUSAN S. SAMUELSON, BUSINESS LAW AND THE LEGAL ENVIRONMENT 263 (South-Western College/West, 6th ed. 2012).
43. Jonathan Shaw, *Why "Big Data" Is a Big Deal*, HARV. MAG. (Mar.-Apr. 2014), http://harvardmagazine.com/2014/03/why-big-data-is-a-big-deal.
44. *See* Alexander Tsesis, *The Right to Erasure: Privacy, Data Brokers, and the Indefinite Retention of Data*, 49 WAKE FOREST L. REV. 433, 440 (2014).

> Consumers, students, and others on the Internet benefit from [data collection] by getting more accurate and personalized returns on searches and advertisements that are integrated into third party websites or that they receive by email. But the benefits of personalized market analysis come with little consumer control over what information is being manipulated . . . .

Id.
45. *60 Minutes: The Data Brokers* (CBS television broadcast March 9, 2014).
46. *See* Tsesis, *supra* note 44.

"The US federal government uses commercial data brokers extensively for a wide variety of government activities."[47] A "reasonable and conservative estimate" states the government provides billions of dollars in revenue to commercial data brokers.[48] Some of these brokers specialize in collecting and interpreting big-data to compile lists of individuals who fit into a specific classification. For example, Thomson Reuters' World-Check analyzes online data from public and private sources to identify "heightened risk individuals."[49] World Check is utilized by over 300 government and intelligence agencies worldwide[50] despite being criticized for allegedly using wikpedia.org as a source of information,[51] and listing "major charities, activists, and mainstream religious institutions under its category of 'terrorism.'"[52] Another commercial data broker, ChoicePoint, which is now part of LexisNexis, states on its website that it is used by "70 percent of local agencies and almost 80 percent of the Federal government."[53]

The Privacy Act of 1974[54] imposes restrictions and transparency requirements on federal agencies in their collection and maintenance of databases, including notice, access, and correction rights.[55] However, the Privacy Act imposes virtually no restrictions on information federal agencies obtain from commercial data brokers if the information remains outsourced and is not maintained in a government system.[56] Furthermore, while sector-specific privacy laws exist for certain categories of data such as credit, medical, and financial, these laws "are riddled with exceptions of varying breadth, which allow access to and sharing of data for law enforcement or intelligence purposes."[57]

---

47. Robert Gellman & Pam Dixon, *Data Brokers and the Federal Government: A New Front in the Battle for Privacy Opens*, WORLD PRIVACY F. 10 (Oct. 30, 2013), http://www.worldprivacyforum.org/wp-content/uploads/2013/10/WPF_DataBrokersPart3_fs.pdf.
48. *Id*.
49. *Id*.
50. THOMSON REUTERS, *Thomson Reuters World-Check* 3, http://financial.thomsonreuters.com/content/dam/openweb/documents/pdf/governance-risk-compliance/fact-sheet/world-check-risk-screening-fact-sheet.pdf.
51. *See* Joseph Cox, *Thomson Reuters' Terrorism Database Cites Wikipedia as a Source*, MOTHERBOARD (July 1, 2016), http://motherboard.vice.com/read/thomson-reuters-world-check-terrorism-database-cites-wikipedia-as-a-source.
52. Namir Shabibi & Ben Bryant, *VICE News Reveals the Terrorism Blacklist Secretly Wielding Power Over the Lives of Millions*, VICE NEWS (Feb. 4, 2016), https://news.vice.com/article/vice-news-reveals-the-terrorism-blacklist-secretly-wielding-power-over-the-lives-of-millions.
53. Gellman & Dixon, *supra* note 47, at 8.
54. Formally cited as 5 U.S.C. § 552a (1974).
55. Chris Jay Hoofnagle, *Big Brother's Little Helpers*, 29 N.C. J. INT'L L. COM. REG. 595, 622 (2004).
56. Gellman & Dixon, *supra* note 47, at 4.
57. James X. Dempsey & Lara M. Flint, *Commercial Data and National Security*, 72 GEO. WASH. L. REV. 1459, 1472 (2004).

C. Cybersecurity Information Sharing Act

Through monitoring consumer activities and providing technology-based services, the private sector controls an immeasurable amount of consumer data. Consequentially, private entities are enticing targets to cyber-criminals. When criminals gain access to consumer information, individuals are exposed to potentially devastating repercussions associated with identity theft, extortion, and various other fraudulent schemes.[58] Private companies also bear the cost of cybercrime in the form of intellectual property and confidential business information loss, opportunity costs derived from service and employment disruptions, the additional cost of securing networks, and reputational damages.[59] A study conducted by IBM and the Ponemon Institute examined the costs of data breaches incurred by sixty-two different U.S. companies, spanning across sixteen industries.[60] These companies spent an average of $6.53 million in recuperation.[61]

Cybercrime is "increasing in frequency, scale, sophistication, and severity of impact" and "impose[s] cumulative costs on U.S. economic competitiveness and national security."[62] In turn, cybersecurity has become an integral aspect of American infrastructure. The Obama Administration described cybersecurity as "one of the most important challenges we face as a Nation."[63]

In response to the increasing importance of cybersecurity, President Obama outlined a national action plan aimed at protecting America's digital infrastructure.[64] The plan includes $3 billion in funding to revamp federal computer systems, creating the federal position of Chief Information Security Officer, encouraging the growth of cyber professionals via student loan forgiveness, scholarships, and recruitment, and the creation of a

58. *See generally Internet Crime Schemes*, FED. BUREAU INVESTIGATION INTERNET CRIME COMPLAINT CTR. (IC3) (last visited Sept. 30, 2016), https://www.ic3.gov/crimeschemes.aspx (providing information on "current and ongoing Internet trends and schemes . . .").

59. CTR. FOR STRATEGIC & INT'L STUD., THE ECONOMIC IMPACT OF CYBERCRIME AND CYBER ESPIONAGE 8 (July 2013), http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf.

60. PONEMON INST., 2015 COST OF DATA BREACH STUDY: UNITED STATES 1 (May 2015), http://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03055usen/SEW03055USEN.PDF?.

61. *Id.*

62. James Clapper, Dir. of Nat'l Intelligence, Statement for the Record: Worldwide Cyber Threats, House Permanent Select Committee on Intelligence 2 (Sept. 10, 2015), https://fas.org/irp/congress/2015_hr/091015clapper.pdf.

63. Press Release, Office of the Press Sec'y, White House, FACT SHEET: Cybersecurity National Action Plan (Feb. 9, 2016), https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

64. *Id.*

bipartisan Commission on Enhancing National Cybersecurity.[65] President Obama also signed into law a controversial bill that purports to "detect, prevent, or mitigate cybersecurity threats."[66]

The Cybersecurity Information Sharing Act of 2015 (CISA) is based on information-sharing that seeks to eliminate cyber incidents.[67] CISA encourages businesses to share information they collect on consumers with one another and the federal government without legal barriers (such as warrants), and without the risk of liability.[68] According to CISA, the government can only use collected data for cybersecurity purposes or to respond to serious federal offenses such as terrorism and sexual exploitation of a minor.[69]

Naturally, CISA has attracted a strong resistance from staunch proponents of civil liberties and privacy rights.[70] More surprising, however, is the backlash from major tech companies who have long-advocated for enhanced cybersecurity.[71] The Computer and Communications Industry, the trade group representing Google, Facebook, and Yahoo,[72] stated that it could not support CISA because of insufficient protection of users' privacy and inadequate restrictions on the government.[73] Apple, Yelp, Twitter, Wikimedia, Dropbox, and Reddit have all independently voiced opposition to CISA as well, on the grounds that security should not compromise personal privacy rights.[74]

The information collected on individuals under CISA is exempt from public disclosure under the Freedom of Information Act (FOIA) and "from disclosure under any State, tribal, or local law requiring disclosure of information or records."[75] CISA's disclosure exemptions purportedly serve

---

65. *Id.*
66. *See* Cybersecurity Information Sharing Act of 2015, 6 U.S.C. § 1501 (2015).
67. *See id.*
68. 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.
69. *See* 6 U.S.C. § 1501.
70. *See* Rachel Nusbaum, *CISA Isn't About Cybersecurity, It's About Surveillance*, ACLU (Mar. 13, 2015), https://www.aclu.org/blog/cisa-isnt-about-cybersecurity-its-about-surveillance.
71. Catherine Ho, *Lobbying on Data, Cybersecurity Has Tripled*, WASH. POST (May 11, 2014), https://www.washingtonpost.com/business/capitalbusiness/lobbying-on-data-cybersecurity-has-tripled/2014/05/11/fad0fe12-d6e9-11e3-8a78-8fe50322a72c_story.html.
72. Brian Fung, *Apple and Dropbox Say They Don't Support a Key Cybersecurity Bill, Days Before Crucial Vote*, WASH. POST (Oct. 20, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/10/20/apple-says-its-against-a-key-cybersecurity-bill-days-before-a-crucial-vote/.
73. Bijan Madhani, *CCIA Urges Senate to Improve Cybersecurity Information Sharing Act*, COMPUTER & COMM. INDUSTRY ASS'N (Oct. 15, 2015), http://www.ccianet.org/2015/10/ccia-urges-senate-to-improve-cybersecurity-information-sharing-act/.
74. Fung, *supra* note 72.
75. *See* Cybersecurity Information Sharing Act of 2015, 6 U.S.C. § 1503(d)(3)(B) (2015).

the interests of companies that are concerned about exposing trade secrets and sensitive business information.[76]

D. Domestic Surveillance

Many opponents of CISA are concerned with unwarranted and uncontrolled government surveillance. Our nation's history of domestic surveillance has fostered distrust among many individuals who fear an abuse of power and lack of accountability by the government. Conversely, proponents of surveillance legislation advocate that surveillance is necessary for matters of national security and is not concerning unless you have something to hide. These arguments are often difficult to evaluate because the exact scope and breadth of government surveillance is difficult to grasp, given the naturally secretive nature in which surveillance laws are implemented. There are, however, important parts of our nation's history that reveal how the government has utilized domestic surveillance.

1. Foreign Intelligence Surveillance Act

In 1975, in light of the Watergate Scandal,[77] a special congressional committee ("the Church Committee") conducted an investigation probing "intelligence abuses by the FBI, CIA, IRS, and NSA."[78] The Church Committee found that these agencies implemented domestic surveillance programs under the Kennedy, Johnson, and Nixon Administrations, often for political gain.[79] NSA's project "Shamrock" enlisted major private communication companies to turn over international message traffic for nearly three decades.[80] "From 1949 until 1975 the project continued . . .

76. *See* Brad S. Karp et al., *Federal Guidance on the Cybersecurity Information Sharing Act of 2015*, HARV. L. SCH. F. ON CORP. GOVERNANCE & FIN. REG. (Mar. 3, 2016), https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/ (stating that certain CISA provisions, such as protections from FOIA disclosure, were meant to encourage more information sharing by corporations).

77. In 1972, five men were arrested for burglarizing the offices of the Democratic National Committee located at the Watergate hotel. *See generally The Watergate Story*, WASH. POST, http://www.washingtonpost.com/wp-srv/politics/special/watergate/#chapters (last visited Sept. 20, 2016). It was later revealed that the men were acting under the direction of President Richard Nixon and were attempting to place warrantless wiretaps in the office as a part of the President's reelection efforts. *Id.* The events led to conspiracy, burglary, and wiretapping convictions of former Nixon aides as well as the first resignation of a United States President. *Id.*

78. Katelyn Epsley-Jones & Christina Frenzel, *The Church Committee Hearings & the FISA Court*, PBS FRONTLINE (May 15, 2007), http://www.pbs.org/wgbh/pages/frontline/homefront/preemption/churchfisa.html.

79. *Id.*

80. *Id.* The chief counsel of the Church Committee, Frederick Schwarz, stated in an interview with PBS that the most "fundamental lessons learned" from his participation in the Committee was that

without the knowledge of subsequent Presidents. To keep the project under the radar, NSA deliberately refrained from formalizing the relationship in any sort of (traceable) document."[81] Meanwhile, Shamrock's sister project, Minaret, "placed particular individuals or organizations involved in civil disturbances, anti-war movements, [or] demonstrations under surveillance."[82] Amongst the organizations and individuals targeted were senators, a congressman, singer Joan Baez, Martin Luther King, Jr., the American Civil Liberties Union (ACLU), Americans for Democratic Action, the NAACP, and other civil liberties organizations.[83] "Operation Shamrock put the government in the position of asking private industry to break the law, not execute it."[84]

The Foreign Intelligence Surveillance Act (FISA) was enacted in 1978 in response to these revelations.[85] FISA regulates government surveillance operations conducted for foreign intelligence purposes via judicial oversight.[86] FISA established the Foreign Intelligence Surveillance Court (FISC)[87] which has exclusive jurisdiction to review and authorize government surveillance efforts.[88] FISA set out to ensure the protection of civil liberties while "accommodating the flexibility, secrecy, and executive discretion" necessary in foreign affairs.[89]

Under the original provisions of FISA, the government could not prospectively collect information on suspected terrorists and could not target an American citizen.[90] Generally, surveillance efforts occurred only in the end-stages of an investigation—after probable cause was shown by "less intrusive techniques."[91]

"when you start small, you go big . . . When you start in a way that seems legitimate, it inevitably goes too far." *The Church Committee and FISA*, BILL MOYERS JOURNAL (Oct. 26, 2007), http://www.pbs.org/moyers/journal/10262007/profile2.html (ellipsis in original).

81. Laura K. Donohue, *Anglo-American Privacy and Surveillance*, 96 J. CRIM. L & CRIMINOLOGY 1059, 1080 (2006).
82. *Id.* at 1081.
83. *Id.* at 1083.
84. *Id.* at 1081.
85. Epsley-Jones & Frenzel, *supra* note 78.
86. Nola K. Breglio, *Leaving FISA Behind: The Need to Return to Warrantless Foreign Intelligence Surveillance*, 113 Yale L.J. 179, 187 (2003).
87. Nicholas J. Whilt, *The Foreign Intelligence Surveillance Act: Protecting the Civil Liberties that Make Defense of Our Nation Worthwhile*, 35 SW. U. L. REV. 361, 372 (2006).
88. *Id.*
89. Breglio, *supra* note 86, at 186.
90. 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, 50 (2005).
91. *Id.* at 41.

2. The 2001 USA PATRIOT Act

Amidst the chaos of September 11, 2001, the Bush Administration developed a legislative proposal to boost counter-intelligence operations.[92] The final version of the USA PATRIOT[93] Act was introduced to Congress on October 23, 2001 and passed just three days later.[94] Before the PATRIOT Act, the government was required to show that the "primary purpose" of its surveillance was to collect information on foreign intelligence.[95] The PATRIOT ACT amended FISA to replace the "primary purpose" test with a less demanding "significant purpose" test and also permitted "pen registers and trap and trace devices to be used against U.S. citizens" which was previously restricted.[96] Furthermore, Section 505 of the PATRIOT Act further enlarged the scope of domestic surveillance by permitting the FBI to circumvent warrant requirements under FISA using national security letters (NSLs) to collect information or conduct surveillance as long as the target was "relevant to any authorized [antiterrorism or clandestine intelligence activities] investigation." [97] This standard is more relaxed compared to previous requirements of "articulable facts" connecting the target to a foreign power.[98] NSLs are "formal demands to surrender certain records and refrain from disclosing the fact of the request."[99]

The PATRIOT Act marked a drastic change in oversight and surveillance methods. The government was no longer collecting data on proposed terrorists, but rather, collecting data of millions of American in the hopes of finding a terrorist.[100]

3. American Civil Liberties Union v. Clapper

In 2013 the ACLU, the New York Civil Liberties Union Foundation, and current and former Verizon customers sued the government officials

92. *Id.* at 53.
93. USA PATRIOT is an acronym for Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, formally cited as Pub. L. No. 107-56, 115 Stat. 272 (2001).
94. *Id.*
95. John J. Dvorske, *Validity, Construction, and Application of Foreign Intelligence Surveillance Act of 1978 (50 U.S.C.A. §§ 1801 et seq.) Authorizing Electronic Surveillance of Foreign Powers and Their Agents*, 190 A.L.R. Fed. 385, 385 (2003).
96. *Id.*
97. Andrew E. Nieland, *National Security Letters and the Amended Patriot Act*, 92 CORNELL L. REV. 1201, 1211 (2007).
98. *Id.*
99. *Id.* at 1201.
100. *See* Am. Civil Liberties Union v. Clapper, 785 F.3d 787, 787 (2d Cir. 2015).

who oversaw the telephone metadata collection program revealed in the Snowden Leaks.[101] The court described the program as follows:

> The metadata concerning *every* telephone call made or received in the United States using the services of the recipient service provider are demanded, for an indefinite period extending into the future. The records demanded are not those of suspects under investigation, or of people or businesses that have contact with such subject, or of people or businesses that have contact with others who are in contact with the subject—they extend to every record that exists, and indeed to records that do not *yet* exist, as they impose a continuing obligation on the recipient of the subpoena to provide such records on an ongoing basis as they are created.[102]

The program collected metadata from virtually all telephone communications within the United States.[103] A FISC order revealed, for example, that Verizon was ordered to produce to the NSA "all call detail records or telephony metadata created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls."[104]

Metadata includes such information as the length of a phone call, the phone number making the call, the phone number to which the call was made, and a general location of the call.[105] While metadata does not reveal the direct content of telephone calls, metadata is "often a proxy for content."[106] For instance, the court explained that a call to certain hotlines "might reveal that an individual is: a victim of domestic violence or rape; a veteran; suffering from an addiction of one type or another; contemplating suicide; or reporting a crime. Metadata can reveal civil, political, or religious affiliations; they can also reveal and individual's social status, or whether and when he or she is involved in intimate relationships."[107]

The court found that the metadata collection program exceeded the scope of the PATRIOT Act.[108] The court also noted that the majority of Congress lacked a "comprehensive understanding of the program or of its purported legal bases."[109] Because of the secrecy associated with national

---

101. *Id.* at 799.
102. *Id.* at 813.
103. *See id.* at 796.
104. *Id.* at 795–96.
105. *Id.* at 793–94.
106. *Id.* at 794.
107. *Id.*
108. *Id.* at 826.
109. *Id.* at 820.

security there was no opportunity for congressional debates or public oversight of the government's interpretation of the PATRIOT Act.[110]

E. Fourth Amendment

ACLU v. Clapper suggested that the government's metadata collection was a violation of the Fourth Amendment, but ultimately avoided a resolution based on constitutional grounds.[111] Under the Fourth Amendment "[t]he right of the people to be secure in their persons, houses, paper, and effects, against unreasonable searches and seizures, shall not be violated . . . ."[112]

The meaning of "searches" as it appears in the Fourth Amendment was originally interpreted to extend protection to only the actual, physical intrusion of "constitutionally protected area[s]."[113] However, the Court adopted a new standard in *Katz v. United States*, when it held that physical intrusion is not determinative of protection under the Fourth Amendment.[114] Rather, *Katz* dictated that the Fourth Amendment protects an individual when (1) she has an "actual (subjective) expectation of privacy" and (2) "society is prepared to recognize [that expectation] as reasonable."[115]

Several years later, the Court reexamined its holding in *Katz* in *United States v. Miller*, where a criminal defendant sought to suppress financial records law enforcement obtained from the defendant's bank, alleging a violation of his Fourth Amendment rights.[116] The Court held that

> the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[117]

The Court subsequently held in *Smith v. Maryland*,[118], that "a single criminal defendant did not retain a reasonable expectation of privacy in

110. *Id.* at 821.
111. *Id.* at 792.
112. U.S. CONST. amend. IV.
113. Silverman v. United States, 365 U.S. 505, 512 (1961).
114. Katz v. United States, 389 U.S. 347, 354 (1967).
115. *Id.*at 361 (Harlan, J., concurring).
116. United States v. Miller, 425 U.S. 435, 436 (1976).
117. *Id.* at 443.
118. *See generally* Smith v. Maryland, 442 U.S. 735 (1979).

twenty-four hours of telephone dialing information, which he voluntarily transmitted to the telephone company to complete his calls."[119]

The holdings in *Miller* and *Smith* have been the focus of much scholarly debate, centered around whether individuals automatically forfeit any expectation of privacy upon disclosure of information to a third party.[120] This is referred to as the "third party doctrine."[121] The Court has not recognized such a sweeping interpretation of *Miller* and *Smith*, and doing so would be particularly consequential to privacy rights in the digital context.[122] "Under an aggressive reading of the third-party doctrine, the Fourth Amendment would not guarantee privacy of any personal data held by any private company" which "would include virtually all records of electronic communications, web browsing activity, and cloud data . . . ."[123]

Because federal courts are generally "reluctant to delve into the business of regulating electronic surveillance" and "[e]xisting Fourth Amendment tests are not fit for the digital long haul[,]"[124] online privacy rights are largely derived from state and federal statutes.[125]

F. Electronic Communications Privacy Act of 1986 (ECPA)

The Electronic Communications Privacy Act of 1986 (ECPA) amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III") "to prohibit not only the interception of wire and oral communications but also the interception of electronic communications."[126] The ECPA also sets forth privacy protections and rules for government access of stored communication and data.[127] However, the ECPA has been widely criticized for being outdated and inapplicable to modern technology practices.[128] For instance, "email older than six months is presumed to be

119. Alexander Galicki, *The End of* Smith v. Maryland?: *The NSA's Bulk Telephony Metadata Program and the Fourth Amendment in the Cyber Age*, 52 AM. CRIM. L. REV. 375, 376 (2015)
120. *See* Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1391 (2004); Henderson, *infra* note 122, at 39–46.
121. *See* Galicki, *supra* note 119, at 390.
122. Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39, 41 (2011).
123. Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. NAT'L SECURITY L. & POL'Y 247, 265 (2016).
124. *Id*.at 248.
125. John P. Collins, *The Third Party Doctrine in the Digital Age*, JUST. ACTION CTR. 7 (2012), http://www.nyls.edu/documents/justice-action-center/student_capstone_journal/cap12collins.pdf.
126. Bellia, *supra* note 120, at 1391.
127. *Id.* at 1391
128. Price, *supra* note 123, at 265; Charles H. Kennedy, *An ECPA for the 21st Century: The Present Reform Efforts and Beyond*, 20 COMM. LAW CONSPECTUS 129 (2011).

abandoned and therefore accessible to law enforcement without a warrant."[129]

III. ANALYSIS

In *Griswold v. Connecticut* the Court held a Connecticut law criminalizing the use of contraceptives unconstitutional.[130] Justice Douglas delivered the opinion of the Court[131] and stated that "specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance. Various guarantees create zones of privacy."[132] For the first time, the Court recognized an un-enumerated right to privacy and expressed that privacy plays a vital role in preserving constitutional rights from unwarranted government intrusion.[133]

The dissenting opinion criticized the majority for finding a constitutional right without any textual basis.[134] But regardless of whether a constitutional right to privacy does or should exist, Justice Douglas's conviction that privacy is essential to maintaining and exercising constitutional rights has become evident in our increasingly technology-dependent society.

The Snowden Leaks revealed that the federal government was collecting and storing meta-data from millions of Americans on a daily basis by forcing Verizon to hand over seemingly private information.[135] Furthermore, the government can potentially access data controlled by private actors via information sharing, buying the information, or compromising technology that protects and facilitates personal communications. The entwinement between the government and private actors distorts individuals' expectations of privacy on the Internet—a forum that has become essential to effectuating First Amendment rights. Modern society relies on Internet connections to communicate, read, write, explore new ideas, and create new things. The Internet has even proved instrumental in sparking political revolution.[136] Privacy in online

129. Price, *supra* note 123, at 265 n.139.
130. Griswold v. Connecticut, 381 U.S. 479, 485 (1965).
131. *Id.* at 480.
132. *Id.* at 484.
133. *Id.*
134. *Id.* at 508–09.
135. Greenwald, *supra* note 8.
136. In 2010, a picture posted on Facebook depicting police brutality in Egypt sparked protests that eventually led to the resignation and murder prosecution of President Hosni Mubarak—the country's longstanding president of 30 years. Jose Antonio Vargas, *Spring Awakening: How an Egyptian Revolution Began on Facebook*, N.Y. TIMES (Feb. 17, 2012), http://www.nytimes.com/2012/02/19/books/review/how-an-egyptian-revolution-began-on-facebook.html?_r=0; Yasmine Saleh & Dina Zayed, *Mubarak to be Tried for Murder of*

communications is essential to preserving the free flow of information in our society and protecting fundamental rights.

A. First Amendment Implications

The lack of privacy on the Internet chills First Amendment rights. The First Amendment and its constitutional guarantees of freedom of speech, freedom of association, and freedom of expression are "inextricably entwined" with privacy.[137] The Court has held that laws compelling disclosure of membership in groups "engaged in advocacy of particular beliefs" impermissibly violate First Amendment rights.[138] The Court recognizes the importance of privacy in protecting the free flow of information, especially "dissident beliefs."[139] The Court has explained:

> The right of freedom of speech and press includes not only the right to utter or to print, but the right to distribute, the right to receive, the right to read and freedom of inquiry, freedom of thought, and freedom to teach . . . Without those peripheral rights the specific rights would be less secure . . . In *NAACP v. State of Alabama* we protected the "freedom to associate and privacy in one's associations," noting that freedom of association was a peripheral First Amendment right. Disclosure of membership lists of a constitutionally valid association, we held, was invalid "as entailing the likelihood of a substantial restraint upon the exercise by petitioner's members of their right to freedom of association." In other words, the First Amendment has a penumbra where privacy is protected from governmental intrusion.[140]

However, because the Court is cautious to effectively regulate electronic surveillance, and statutory protections are largely inadequate, dwindling expectations of online privacy chills First Amendment rights and fosters self-censorship.[141] "Self-censorship refers to a decision by an individual or group to refrain from speaking" that is often induced by fear.[142]

Protesters, REUTERS (May 24, 2011), http://www.reuters.com/article/us-egypt-mubarak-idUSTRE74N3LG20110524.

137. *See* Vill. of Belle Terre v. Boraas, 416 U.S. 1, 15 (1974) (Marshall, J., dissenting) ("The freedom of association is often inextricably entwined with the constitutionally guaranteed right of privacy.").

138. NAACP v. Alabama, 357 U.S. 449, 462 (1958).

139. *Id.*

140. Griswold v. Connecticut, 381 U.S. 479, 482–83 (1965).

141. *Global Chilling: The Impact of Mass Surveillance on International Writers*, PEN AMERICA 5 (Jan. 5, 2015), http://www.pen.org/sites/default/files/globalchilling_2015.pdf.

142. Robert A. Sedler, *Self-Censorship and the First Amendment*, 25 NOTRE DAME J.L. ETHICS & PUB. POL'Y 13, 13 (2011).

PEN American Center conducted an international survey of writers that accumulated 772 responses from writers in 50 different countries.[143] The report summarized that "[w]riters living in liberal democratic countries have begun to engage in self-censorship at levels approaching those seen in non-democratic countries."[144] Writers reported avoiding certain topics or at least seriously considered avoiding certain topics due to concerns of government surveillance.[145]

In 2013, the First Unitarian Church of Los Angeles, along with twenty-one other advocacy groups, filed a lawsuit against the National Security Agency. The Complaint alleged the bulk acquisition of telephone communications information revealed in the Snowden leaks unconstitutionally chilled plaintiffs' freedom of association guaranteed under the First Amendment.[146] The Complaint further alleged that each plaintiff experienced a decrease in communications from members since the existence of the program became publicly known.[147] Plaintiffs who operate hotlines experienced a decrease in calls and an increase in callers expressing concerns about the confidentiality of their communications.[148]

The lack of privacy expectations on the Internet squashes progressive thought and undermines First Amendment rights. Our nation has experienced tremendous political and civil revolutions that were birthed from ideas once viewed as radical, like women's suffrage and civil rights. However, the fear of being labeled a threat or becoming a target of domestic surveillance chills the exploration of unpopular beliefs. The government used unwarranted surveillance of civil rights leaders in the 1970's before the Internet gave rise to more far-reaching spying techniques.[149] It is disturbing to imagine whether such efforts would have been successful in stifling political adversity with modern Internet capabilities.

B. Due Process Implications

The Due Process Clauses of the Fifth and Fourteenth Amendments provide that neither the federal government nor state governments shall deprive a person of "life, liberty, or property, without due process of

143. *Global Chilling*, *supra* note 141, at 4.
144. *Id.* at 5.
145. *Id.*
146. *See* Second Amended Complaint for Constitutional and Statutory Violations, First Unitarian Church of Los Angeles v. NSA, Case No. 4:13-cv-03287 JSW, https://www.eff.org/files/2014/08/20/first_uni_2ac_filed.pdf.
147. *Id.* at 16.
148. *Id.*
149. *See generally* Epsley-Jones & Frenzel, *supra* note 78.

law."[150] CISA allows private actors to identify and share information regarding cyber threats with the government without consideration of due process guarantees. Although the government uses information shared by private entities to conduct further investigations and prosecute crimes, there are no constitutional limits or other protections that require procedures for how private actors determine what amounts to a threat. Furthermore, CISA provides immunity to private actors against potential claims associated with sharing personal information with the government.[151]

Commercial databases also raise similar due process concerns. "There are few legal or regulatory constraints on the government's use of commercial data sources about individuals. Commercial database owners are largely unregulated for privacy, and they are generally free to sell information as they please with little regard for accuracy, currency, completeness, or fairness."[152] Furthermore, there are inherent flaws in using even accurate data. For instance, data often fails to account for an individual's motive.[153] Take the following anecdote, for example:

> An algorithm, designed to probe a database containing all personal data available to the government, sees that you have recently bought some fertilizer and a large truck, and that you have emailed someone with a .lb (Lebanon) email address. Seeing this red flag pop up on his computer, a government agent pulls your bank records, your Amazon and iTunes purchases, the domain names that you've recently visited, and a list of everyone you have recently phoned or emailed. Inspecting all of these records, the agent determines that you were merely asking your Lebanese uncle for advice on expanding your farm and makes a notation in his database.[154]

But what would have happened if this agent had not delved into the individual's motives? Many similarly situated people are often "categorized by the government as administratively 'guilty until proven innocent' by virtue of digitally generated suspicion"[155] and placed on lists determining who can work, fly, or vote.[156] Commercial databases are often used by federal agencies and in government initiatives to determine eligibility for benefits, mitigate crime, and identify national security threats.

---

150. U.S. CONST. amends. V, XIV; Daniels v. Williams, 474 U.S. 327, 331 (1986) (refusing to recognize negligent conduct as a deprivation under the Due Process Clause because it is intended to prevent intentional, arbitrary exercises of government power).
151. 6 U.S.C. § 1505 (2015).
152. Gellman & Dixon, *supra* note 47, at 10.
153. Dempsey & Flint, *supra* note 57, at 1470.
154. *Data Mining, Dog Sniffs, and the Fourth Amendment*, 128 HARV. L. REV. 691, 691 (2014).
155. Hu, *supra* note 12, at 1737.
156. *See id.* at 1735.

For example, the U.S. Treasury's Do Not Pay portal is used to verify "the eligibility of individuals to receive government benefits, such as those receiving food stamps, housing assistance, and survivor benefits."[157] The portal utilizes a commercial database that is not subject to the same privacy laws that regulate government databases.[158] In recognition of the potential harm from inaccurate data, the Office of Management and Budget established privacy standards for commercial databases used by the Do Not Pay portal.[159] However, these standards do not exist in the context of other government initiatives while the same potential for harm does.[160]

The dangers of inaccurate and unverified data are far reaching when used to determine who is eligible for government assistance programs, afforded the freedom to travel, or barred from exercising civil liberties. In the specific context of counterterrorism, consequences of using data include "arrest, deportation, loss of a job, greater scrutiny at various screening gates, investigation or surveillance, or being added to a watch list."[161]

However, because of a lack of transparency and regulation of commercial databases, it is difficult to tell how the government utilizes the data and whether it follows constitutional procedures according to the Due Process Clause.

C. Article III Standing Requirements Bar Judicial Inquiry into Government Surveillance

Like all other constitutional rights, the First Amendment guarantees are only applicable to state actors. However, the courts recognize a justiciable constitutional challenge under the First Amendment when government actions indirectly deter an individual's First Amendment rights.[162] This doctrine is known as the "chilling effect."[163]

The national government's increasing control over and cooperation with private entities that facilitate online communications undoubtedly has a chilling effect on First Amendment rights and intrudes on individuals' privacy. However, alleging that a chill effect is induced by mere knowledge of government surveillance activity is generally not sufficient to satisfy the injury facet of Article III standing.[164] In *Clapper v. Amnesty*

157. Gellman & Dixon, *supra* note 47, at 4.
158. *Id.*
159. *Id.*at 5.
160. *Id.*
161. *Id.* at 1471.
162. Laird v. Tatum, 408 U.S. 1, 12–13 (1972).
163. Monica Youn, *The Chilling Effect and the Problem of Private Action*, 66 VAND. L. REV. 1473, 1474 (2013).
164. *Laird*, 408 U.S. at 11.

Int'l USA,[165] the Court held that "plaintiffs who assert that their activities are 'chilled' by covert surveillance, but who cannot show that it has caused them actual or impending injury, do not have standing . . . ."[166] Furthermore, the lack of transparency makes it extremely challenging to show how the government has used your data and the exact depth of private-public relationships, and thus it is difficult to prove a concrete injury.

Standing requirements are rooted in concerns over the separation of power.[167] The Court stated that judging the "wisdom and soundness of Executive action" is within Congress's authority and not the judiciary's.[168] However, most government data collection programs operate under the veil of national security and either evade congressional scrutiny or are facilitated by collusion between the executive and legislative branches.[169] For instance, the Church Committee uncovered NSA programs that operated for almost three decades, unbeknownst even to the presidents, because of purposeful concealment.[170] Furthermore, Congress was apparently blind to the scope and application of government surveillance programs revealed in the Snowden Leaks due in part to alleged misrepresentations from the NSA during congressional hearings.[171]

The legal theories behind the Article III standing requirements assume that congressional oversight and the political process provide a remedy for individuals who believe the law inadequately protects their rights. However, the political process fails individuals in that sense because of a lack of transparency. The government's national security efforts naturally require a need for secrecy that makes it nearly impossible to monitor how the government's efforts are affecting our individual rights.

IV. PROPOSAL

The government's entwinement with private entities that facilitate and control online activities jeopardizes constitutional and fundamental rights.

---

165. *See generally* 133 S. Ct. 1138 (2013).
166. Christopher Slobogin, *Standing and Covert Surveillance*, 42 PEPP. L. REV. 517, 533 (2015).
167. *Id.* at 531.
168. *Laird*, 408 U.S. at 15.
169. Slobogin, *supra* note 166, at 545.
170. Donohue *supra* note 81.
171. Prior to the leak, the Director of National Intelligence, James Clapper, appeared before Congress during a hearing on surveillance. He was asked "whether the NSA collected any type of data at all on millions or hundreds of millions of Americans." Clapper responded, "No sir." The Snowden Leaks proved otherwise and ultimately revealed that Congress was unable to control the NSA and protect public interests. Ewen Macaskill & Gabriel Dance, *The NSA Files, Part Five: Who's Watching*, GUARDIAN (Nov. 1, 2013), http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.

However, the issues fall short of standing requirements necessary in legal actions against both the public and private sectors. Additionally, private entities are not liable for constitutional violations because the Constitution does not apply to private actors.[172]

I propose a statute that enhances government transparency, regulates how it uses privately acquired data, and includes a statutorily created cause of action that will give courts the ability to clearly define how and to what extent the government can rely on private organizations to provide data collection services. Section I determines what information falls under this act. Section II establishes a court, similar to the FISC, that will maintain the necessary secrecy of national security surveillance operations while protecting civil liberties. Section III outlines the procedures for using data gathered by private organizations. Finally, Section IV creates standing by means of a citizen suit.

THE DATA INTELLIGENCE ACT

Section I. Definitions

This act applies to personal data related to a living individual who is an American citizen located within the United States' jurisdiction after such data has been gathered by a private entity and acquired by a government entity.

(a) "Personal Data"[173] means data consisting of information regarding an individual's (1) racial or ethnic origin; (2) political beliefs; (3) physical or mental health; (4) sexual life; or (5) criminal or alleged criminal history.

(b) "Gathered" means acquiring voluntarily from a non-governmental entity as part of a transaction, contract, or other scheme. This does not include data gathered as part of an existing surveillance operation acting pursuant to a warrant or other judicial authorization.

(c) "Private Entity" means any individual or firm not acting on behalf of the United States, a state or local government within the United States, or a government agency.

(d) "Government Entity" means the United States government, a state or local government within the United States, or a government agency.

Section II. Domestic Intelligence Surveillance Court (DISC)

(a) Composition: The Chief Justice shall appoint five District Court judges to reside over DISC Court.

---

172. LEGAL INFORMATION INSTITUTE, *supra* note 9.

173. The definition of "personal data" is modeled after the United Kingdom's Data Protection Act 1998. Data Protection Act of 1998, c. 29, § 2, http://www.legislation.gov.uk/ukpga/1998/29/section/2.

(b) Authority: DISC shall have authority to authorize and deny petitions under Section III of this Act and require the petitioners to provide any additional, necessary information other than that laid out in Section III (b)(1)-(5).

Section III. Use of Intelligence

(a) A government entity may not use data covered under this act for the following purposes, unless authorized by DISC: (1) pursue criminal charges; (2) place an individual identified by the data in a database, or on a list, or otherwise label the individual in a manner that may interfere with that individual's civil liberties including, but not limited to, traveling, voting, working, associating with a group, receiving government benefits, or maintaining citizenship;

(b) Before engaging in any conduct covered by subsection (a) of this section, the government entity must submit a request to DISC, setting forth the following information[174]: (1) the data gathered; (2) the means by which it was gathered; (3) the reason for pursuing one of the actions set forth in subsection (a)(1)-(2) of this section; (4) the predicted effect on the targeted individual's civil liberties; (5) description of why less intrusive means cannot achieve the government's purpose; and (6) the measures taken, if any, to verify the integrity of the data.

Section IV. Authority to Bring Civil Action

Any persons may commence a civil action on his behalf and against any government entity who is alleged to have violated or be in violation of this act.[175]

V. CONCLUSION

As computer technology becomes increasingly sophisticated, government agencies and criminals alike are provided with more efficient ways of carrying out their goals. Consequentially, there is a conflict between protecting individual privacy while simultaneously giving the government the adequate means to promote national security and public safety. Privacy rights and other individual freedoms are especially at risk when the government utilizes private organizations to provide it with information about individuals' online activity. The government skirts constitutionally afforded protections by enlisting private entities to provide information about individuals. Furthermore, a lack of transparency makes

174. These factors are based on the Data Privacy & Integrity Advisory Committee's report to the Secretary and Chief Privacy Officer of the Department of Homeland Security. DATA PRIVACY & INTEGRITY ADVISORY COMMITTEE, *The Use of Commercial Data* 10-13 (Dec. 6, 2006), https://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_commdata.pdf.

175. This section is modeled after 42 U.S.C. § 7604(a).

it virtually impossible to monitor whether the government is abusing its powers. Corporations who provide the data act under generally outdated electronic privacy laws. By requiring transparency and providing a statutorily created right of action against the government, the courts will finally be able to interpret the expectations of privacy in the digital era.