GOING DARK: SCRATCHING THE SURFACE OF GOVERNMENT SURVEILLANCE

Abdulmajeed Alhogbani*

The Internet is akin to our oceans.[1] While most Internet users are limited to what is on the surface or immediately beneath it,[2] there is a vast wealth of information that can be found if one swims deep enough.[3]

Whistleblowers, such as Edward Snowden and Julian Assange, changed the way people view Internet surveillance.[4] U.S. citizens were forced to face the fact that the government has kept a close eye on its citizens through regulations like the USA PATRIOT Act.[5] Most people believe the PATRIOT ACT only targets individuals suspected of terrorist activity, and do not consider that it could apply to them.[6] A poll conducted in 2004 showed that only 29% of Americans believed that the government had overly restricted civil liberties, while 49% believed that the government had not gone far enough to protect the country.[7] The opinion of the American people changed drastically when Snow-

* J.D. Candidate, The Catholic University of America, Columbus School of Law, 2016.

1 Michael K. Bergman, *White Paper: The Deep Web: Surfacing Hidden Value*, J OF ELECTRONIC PUB., Aug. 2001, at 1, *available at* http://quod.lib.umich.edu/j/jep/3336451.0007.104/—white-paper-the-deep-web-surfacing-hidden-value?rgn=main;view=fulltext.

2 *Id.*

3 *See id.* at 2.

4 Pierluigi Paganini, *How Edward Snowden Protected Information and His Life*, INFOSEC INST. (July 25, 2013), http://resources.infosecinstitute.com/how-edward-snowden-protected-information-and-his-life/.

5 *Id.*; *see generally* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

6 *See Few See Adequate Limits on NSA Surveillance Program*, PEW RES. CENTER (July 26, 2013), http://www.people-press.org/2013/07/26/few-see-adequate-limits-on-nsa-surveillance-program/press.org/2013/07/26/few-see-adequate-limits-on-nsa-surveillance-program/ ("This is the first time a plurality has expressed greater concern about civil liberties than security since the question was first asked in 2004.").

7 *See id.* (providing a graphical representation of the 2004 poll).

den exposed the depth and gravity of the National Security Agency's ("NSA") surveillance on U.S. citizens as well as foreigners.[8] By 2013, 47% of Americans believed the government had impinged upon citizens' civil liberties; only 35% thought the government has not gone far enough to protect the country.[9] As a result, Internet users began to realize the depth of the government's surveillance, and many of them started using proxy servers to protect their privacy.[10] Proxy servers disguise a users' location and allows them to "go dark."[11]

Government spying is not a new phenomenon; it has been an ongoing custom since the earliest forms of government. [12] The NSA's spying program constrains one of humanity's most important inventions, the Internet.[13] The United States government crossed a threshold that grants access to limitless amounts of information.[14] They are overstepping constitutional boundaries,[15] and raising the possibility of a police state.[16] By advocating that surveillance is necessary for national security, the government provides an incentive for citizens to bypass the surveillance.[17] Anonymity is an important virtue of the Internet, and destroying it causes more harm than good.[18] Legislators must reexamine current legislation, redefine what constitutes a reasonable search, and balance national security with an individual's right to privacy. Courts must reconcile

---

8 Paganini, *supra* note 4; Igor Bobic, *NSA Fesses up to Improper Surveillance of U.S. Citizens*, THE HUFFINGTON POST, http://www.huffingtonpost.com/2014/12/26/nsa-spying-report_n_6382572.html (last updated Dec. 26, 2014, 12:59 PM).

9 *Few See Adequate Limits on NSA Surveillance Program*, *supra* note 6.

10 Patrick Howell O'Neill, *Tor and the Rise of Anonymity Networks*, THE DAILY DOT (Oct. 24, 2013), http://www.dailydot.com/technology/tor-freenet-i2p-anonymous-network/.

11 *See id.* (explaining that proxy servers, such as Tor, "are designed to hide their users").

12 *See, e.g.*, Chris Thompson, *The History of Mass Surveillance*, TRUTH OUT (June 21, 2013, 11:45 PM), http://www.truth-out.org/speakout/item/17139-the-history-of-mass-surveillance http://www.truth-out.org/speakout/item/17139-the-history-of-mass-surveillance (explaining "Bentham's Panopticon prison concept" which is identified as "the earliest form of surveillance technology").

13 *See* Kristy Hughes, *Internet Freedoms Under Increasing Attack*, INDEX ON CENSORSHIP (June 19, 2012), http://www.indexoncensorship.org/2012/06/internet-freedom-under-attack/.

14 *See* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1938 (2013).

15 *See id.* at 1950 (discussing the chilling-effect theory on First Amendment rights).

16 *See id.* at 1951.

17 *See* Andrea Peterson, *The NSA is Trying to Crack Tor The State Department is Helping Pay for it*, WASH. POST (Oct. 5, 2013), http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/05/the-nsa-is-trying-to-crack-tor-the-state-department-is-helping-pay-for-it/.

18 Dave Maass, *Online Anonymity Is Not Only for Trolls and Political Dissidents*, ELECTRONIC FRONTIER FOUND. (Oct. 29, 2013), https://www.eff.org/deeplinks/2013/10/online-anonymity-not-only-trolls-and-political-dissidents.

modern technology with the U.S. Constitution. Moreover, the judiciary must fulfill their constitutional function by keeping the executive branch in check.

This Comment proceeds in four parts. Part I discusses the historical development of communication surveillance regulations and case law. Part II examines the infrastructure of the Internet, outlines the six layers that make it function, and discusses the methods that can be used to go dark and bypass the public portion of the Internet. Part III highlights the right to privacy and argues for Internet anonymity by showing its benefits in real life situations. Part IV suggests change to Internet surveillance legislation through a reexamination of the Fourth Amendment and urges the judicial branch to fulfill its governmental function.

I. INTERNET REGULATION AND SURVEILLANCE

A. Pre-9/11

1. Early Forms of Communications Regulation

Internet regulation and surveillance are not a new phenomena in the United States.[19] In 1934, the U.S. government enacted the Communications Act of 1934 ("The Act"),[20] which served to

> [R]egulat[e] interstate and foreign commerce in communication by wire and radio so as to make available, so far as possible, to all the people of the United States a rapid, efficient, nationwide, and worldwide wire and radio communication service with adequate facilities at reasonable charges, for the purpose of the national defense, and for the purpose of securing a more effective execution of this policy by centralizing authority theretofore granted by law to several agencies and by granting additional authority with respect to interstate and foreign commerce in wire and radio communication.[21]

The Communications Act was part of President Franklin D. Roosevelt's New Deal and attempted to centralize the regulatory process of telecommunications and provide affordable access to communication services.[22] Additional-

---

19 *See generally* Everett Ehrlich, *A Brief History of Internet Regulation*, PROGRESSIVE POL'Y INST. (Mar. 13, 2014), http://www.progressivepolicy.org/issues/economy/a-brief-history-of-internet-regulation-2/; *see also* Ray Downs, *A Brief History of the US Government Spying on Its Citizens*, VICE (June 14, 2013), http://www.vice.com/read/a-brief-history-of-the-united-states-governments-warrentless-spying (providing that a forerunner to the NSA, the "Black Chamber" began a surveillance project in the 1920's on communications such as international telegraphs originating and/or being delivered to the United States).

20 47 U.S.C. § 2 (2012).

21 *Id.* § 151.

22 *See id.* § 390; *What is the Communications Act of 1934?*, ROOSEVELT INST., http://www.rooseveltinstitute.org/new-roosevelt/what-communications-act-1934 (last visited

ly, the Act created the Federal Communications Commission (FCC) to oversee and regulate the communication industry.[23] The Act prohibited the disclosure of personally identifiable information without the customer's consent. However, the Act did include some notable exceptions.[24] For example, consent is not required if disclosure is made pursuant to a court order[25] and the individual against whom disclosure is offered may argue against the order in court.[26] Moreover, the Act permits the President to override or amend regulations if there is a national emergency or threat of war .[27]

In theory, the government's ability to intercept information that threatens national security is important.[28] However, this power has been abused.[29] In the 1960s, for example, the U.S. government conducted warrantless surveillance of civil rights activists and citizens who were critical of the Vietnam War.[30] The U.S. government spied on Martin Luther King, Jr., Muhummad Ali, and U.S. Senators Frank Church and Howard Baker, among others.[31] The government continued to abuse its surveillance power until the Supreme Court, in *Katz v. United States*, limited the government's ability to conduct warrantless domestic surveillance.[32] The Court held that using an electronic listening device on a phone booth without a warrant violated the Fourth Amendment and constituted an unreasonable search and seizure.[33] The Court reasoned that "[t]he Fourth

---

Jan. 24, 2015).

23 § 151.

24 *Id.* § 222(c)-(d).

25 *Id.* § 551(h).

26 *Id.* § 551(h)(2).

27 *Id.* § 606(c)

> Upon proclamation by the President that there exists war or a threat of war, or a state of public peril or disaster or other national emergency, or in order to preserve the neutrality of the United States, the President, if he deems it necessary in the interest of national security or defense, may suspend or amend, for such time as he may see fit, the rules and regulations applicable to any or all stations or devices capable of emitting electromagnetic radiations within the jurisdiction of the United States as prescribed by the Commission, and may cause the closing of any station for radio communication.

Id.

28 In re Production of Tangible Things From [redacted], No. BR 08-13, 2009 WL 9150913, at *1 (FISA Ct. 2009).

29 *See id.* at *6 (finding that the NSA conducted an unauthorized use of the alert list and made misrepresentations to the court).

30 Matthew M. Aid & William Burr, *Secret Cold War Documents Reveal NSA Spied on Senators*, FOREIGN POL'Y (Sept. 25, 2013), http://www.foreignpolicy.com/articles/2013/09/25/it_happened_here_NSA_spied_on_senators_19 70s.

31 *Id.*

32 Katz v. United States, 389 U.S. 347, 358 (1967). In *Katz*, the government conducted a warrantless wiretap and listened to a telephone that the defendant, Charles Katz, was using to conduct gambling activities, and used it as evidence against him. *Id.*

33 *Id.* at 353.

Amendment protects people, not places" and therefore, that individuals must have a reasonable expectation of privacy in the area being searched in order to claim constitutional protection.[34]

The Court's analysis of the Fourth Amendment is outdated in regards to new technologies.[35] The Court has held that an individual has no reasonable expectation of privacy in what they disclose to third parties.[36] In *U.S. v. Jones*, as Justice Alito opined, "[s]ome people may find the 'tradeoff' of privacy for convenience 'worthwhile,' or come to accept this 'diminution of privacy' as 'inevitable.'"[37] Justice Scalia, on the other hand, noted that, "this approach is ill-suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[38] The two differing opinions exemplify the public's standing on surveillance in the 21st century.

2. Foreign Intelligence Surveillance Act (FISA)

Shortly after the decision in *Katz*, courts continuously held that warrantless surveillance is constitutional as long as it was for foreign intelligence, while warrantless domestic surveillance is unconstitutional.[39] The difficulty is determining what constitutes foreign surveillance versus domestic surveillance, as this distinction is often ambiguous.[40] Intelligence surveillance also became a major area of concern, which led to the enactment of Foreign Intelligence Surveillance Act (FISA) in 1978.[41] FISA allows the U.S. government to conduct warrantless searches if the agency has reasonable grounds to believe the targeted individual is an agent of a foreign power.[42] It defines foreign intelligence as:

---

34 *Id.* at 351.

35 *See* Timothy Casey, *Electronic Surveillance and the Right To Be Secure*, 41 U.C. DAVIS L. REV. 977, 979 (2008) ("Recent controversies involving the government's expanded use of technological capabilities highlight the difficulties modern courts face when navigating issues in the field of electronic surveillance.").

36 United States v. Jones, 132 S. Ct. 945, 957 (2012).

37 *Id.* at 962.

38 *Id.* at 957.

39 *See, e.g.*, United States v. Brown, 484 F.2d 418, 426-27 (1973) (ruling that the government did not violate the Telecommunications Act of 1934, when they wiretapped firearms trafficker, Hubert Brown's, communications without a warrant because it was a matter of national security).

40 *See id.* at 425-26.

41 *See generally* 50 U.S.C. §§ 1801-85(c).

42 *See id.* § 1802; *see also id.* § 1802(b)

> (1) any person other than a United States person, who—(A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section; (B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—

(A) the national defense or the security of the United States; or

(B) the conduct of the foreign affairs of the United States.[43]

Along with the definition of a foreign power, FISA grants the government broad power to conduct surveillance on foreign agents.[44] Moreover, FISA establishes a separate court, the FISA court, to process warrants for the surveillance of foreign and domestic intelligence.[45] The FISA court has been dubbed

---

presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; (C) engages in international terrorism or activities in preparation therefore; (D) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor; or (E) engages in the international proliferation of weapons of mass destruction, or activities in preparation therefor for or on behalf of a foreign power; or (2) any person who (A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States; (B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States; (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power; (D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power.

Id.

[43] *Id.* § 1801(e).

[44] *See id.* § 1801(a)

(1) [A] foreign government or any component thereof, whether or not recognized by the United States; (2) a faction of a foreign nation or nations, not substantially composed of United States persons; (3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments; (4) a group engaged in international terrorism or activities in preparation therefor; (5) a foreign-based political organization, not substantially composed of United States persons; (6) an entity that is directed and controlled by a foreign government or governments; or (7) an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction.

Id.

[45] *See id.* § 1803(a)(1).

"the most secret court in America."[46] This Comment will discuss the FISA court in a later section.

3. The National Security Agency (NSA)

The earliest form of the NSA was created during World War II with the aim of decoding enemy transmissions. President Harry Truman officially created the NSA in 1952 to continue code-breaking post-World War II.[47] The agency evolved over time and the crux of their mission today is twofold: 1) information assurance, which prevents foreign agents from obtaining classified information,[48] and 2) signals intelligence, which collects and analyzes foreign intelligence.[49] Because their mission, to safeguard national security, is extremely sensitive, the NSA's operations and budget are classified information.[50] James Clapper, the director of the NSA, notes that the "budgets are classified as they could provide insight for foreign intelligence services to discern top national priorities, capabilities and sources and methods that allow us to obtain information to counter threats."[51] While the exact dollar amount of the NSA's budget is classified, it is obvious that the NSA spends an enormous amount of money and manpower to achieve their goals.[52]

---

[46] John Shiffman & Kristina Cooke, *The judges who preside over America's secret* court, REUTERS, (June 21, 2013, 1:11 AM), http://www.reuters.com/article/2013/06/21/us-usa-security-fisa-judges-idUSBRE95K06H20130621.

[47] Tom Murse, *What is the National Security Agency?*, ABOUT NEWS, http://uspolitics.about.com/od/agencies/a/What-Is-The-National-Security-Agency.htm (last visited Jan. 31, 2015).

[48] *Mission*, NSA/CSS, https://www.nsa.gov/about/mission/index.shtml (last visited Jan. 31, 2015).

[49] *Id.*

[50] *See* Exec. Order No. 13,526, 3 C.F.R. 298, 300 (2010); *see also* Max Ehrenfreund, *'Black Budget' leaked by Edward Snowden describes NSA team that hacks foreign targets*, WASH. POST (Aug. 30, 2013), http://www.washingtonpost.com/world/national-security/black-budget-leaked-by-edward-snowden-describes-nsa-team-that-hacks-foreign-targets/2013/08/30/8b7e684c-119b-11e3-bdf6-e4fc677d94a1_story.html (identifying the budget as "Top Secret").

[51] Wash. Post Staff, *DNI James Clapper's statement to The Post*, WASH. POST (Aug. 29, 2013), http://www.washingtonpost.com/world/national-security/dni-james-clappers-statement-to-the-post/2013/08/29/52d52090-10e1-11e3-85b6-d27422650fd5_story.html.

[52] *See* Wilson Andrews & Todd Lindeman, *'THE BLACK BUDGET': How Intelligence Agencies Spend $52 Billion*, WASH. POST (Aug. 29, 2013), http://www.washingtonpost.com/wp-srv/special/national/black-budget/project-files/black-budget-doubletruck-web.pdf/ (noting the NSA's $10.8 billion budget for 2013).

B. Post-9/11

Following the attacks of 9/11, the United Nations Security Council unanimously adopted a broad, anti-terrorism resolution.[53] One of the provisions calls upon all states to "[f]ind ways of intensifying and accelerating the exchange of operational information, especially regarding use of communications technologies by terrorist groups."[54] The United States took its own measures to counteract terrorism by enacting the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act").[55]

1. USA PATRIOT Act

Congress passed the USA PATRIOT Act in October 2001 as a preemptive tool for preventing terrorist attacks.[56] Title II of the Act relaxed the requirements for securing a court order to conduct surveillance and expanded the government's authority to monitor nearly all areas of electronic communication.[57] In essence, the Act granted the authority to intercept all wire, oral, and electronic communications relating to terrorism or national security.[58] Title VII called for enhanced cooperation and information sharing among federal, state, and local agencies.[59] The PATRTIOT Act also redesigned the structure of FISA by superseding its authority and changing its purpose into a law enforcement body.[60] Similar acts and amendments were passed post-9/11.[61]

---

53 S.C. Res. 1373, U.N. Doc. S/RES/1373 (Sept. 28, 2001); Security Counsel, *Security Counsel Unanimously Adopts Wide Ranging Anti-Terrorism Resolution; Calls for Suppressing Financing, Improving, International Cooperation*, UNITED NATIONS (Sept. 28, 2001), http://www.un.org/press/en/2001/sc7158.doc.htm.

54 S.C. Res. 1373, ¶ 3.

55 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

56 *Id.*

57 *Id.* at 278, 283-96 (codified as amended at 18 U.S.C. §§ 2516(1), 2517 (2006)).

58 *Id.* at 278 (codified as amended at 18 U.S.C. § 2516(1) (2006)).

59 *Id.* at 374 (codified as amended at 42 U.S.C. § 3796(h) (2006)).

60 Casey, *supra* note 35, at 1003, n. 147.

61 *See, e.g.*, FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (2008); FISA Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238, 126 Stat. 1631 (2012).

2. The 2007 Protect America Act

In 2007, President George W. Bush was granted considerable authority under the Protect America Act,[62] which was passed because the Bush Administration asserted that FISA was outdated and significantly burdened counterterrorism efforts.[63] The Act amended FISA to allow the president to conduct warrantless surveillance on any communication that is made to an individual outside of the U.S., effectively removing the requirement of a "foreign agent" under the old FISA statute.[64] More importantly, the amendment allowed the president to conduct surveillance with minimal oversight from the FISA court.[65]

II. HOW THE INTERNET WORKS

Section II examines the infrastructure of the Internet and the rules of technology that govern it. This analysis is twofold. The first part examines the layers of the Internet; the second part explains the immensity of the web and the trend to go dark in order to circumvent the reaches of Internet surveillance. One common misconception about the Internet is that it is something intangible and unidentifiable.[66] Although that may be the case for certain information that travels through the Internet, the Internet itself is fixed and clearly identifiable.[67]

A. The Layers of the Internet

The modern Internet originated from the Advanced Research Projects Agency's (ARPA) goal to create a network connecting four computers (ARPANET) using existing phone lines.[68] The ARPANET was connected to the packet radio

---

62 Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552, 552-54 (codified at 50 U.S.C. § 1805(a) et seq.).

63 George W. Bush, *President's Radio Address*, WHITE HOUSE RADIO (July 28, 2007), http://georgewbush-whitehouse.archives.gov/news/releases/2007/07/print/20070728.html.

64 *ACLU Fact Sheet on the "Police America Act,"* ACLU (Aug. 7, 2007), https://www.aclu.org/national-security/aclu-fact-sheet-%E2%80%9Cpolice-america-act.

65 50 U.S.C. § 1802(a)(1) (2012).

66 *See Internet of Things*, TECH CRUNCH, http://techcrunch.com/topic/subject/internet-of-things/ (last visited Jan. 30, 2015).

67 Forest Time, *What is an Example of an Intangible Good?*, CHRON, http://smallbusiness.chron.com/example-intangible-good-35031.html (last visited Jan. 16, 2015).

68 *See* Robert Hobbes Zakon, *Hobbes Internet Timeline 12*, ZAKON.ORG, http://www.zakon.org/robert/internet/timeline/ (last visited Jan. 31, 2015); *see also How Did the Internet Get Started*, MUSEUM OF SCI. AND INDUSTRY, http://www.msichicago.org/scrapbook/scrapbook_exhibits/commex/history.html (last visit-

network (PRNET) that links computers through radio waves.[69] Subsequently, the two networks were connected to a third network, the satellite network (SATNET), and these three networks were later joined to other networks.[70] This concept of connecting networks together, inter-networking, became known as the Internet.[71]

Information travels through the Internet by going through multiple layers.[72] The first layer is the content layer, which is comprised of the information being communicated.[73] This may be a file, email, or picture.[74] In the second layer, the content must pass through an application that uses the Internet, such as Firefox or Safari, which is referred to as the application layer.[75] In the next layer, the content is broken into data packets and travels through the transport layer.[76] In the fourth layer, data packets flow through the Internet protocol layer, which is a set of rules that determine how data flows through the network.[77] In the fifth layer, the link layer connects the computer to the physical layer through an Internet Service Provider (ISP) or a server.[78] In the last layer, the data packets flow through the physical layer, which consists of the hardware needed to send and receive information; this hardware may be an optical cable, satellite, or copper wire.[79] At its core, the structure of the Internet is similar to the way our roads are organized.

There are several rules, called protocols, which determine how information is passed through the Internet.[80] The most common protocols are the Transmission Control Protocol (TCP) and the Internet Protocol (IP).[81] TCP, which is vital to the transport layer, is responsible for taking information from a com-

---

ed Jan. 16, 2015) ("The grandfather of today's Internet was called the "ARPANET," named after the Department of Defense's Advanced Research Projects Agency that developed it in the late 1970s and early 1980s.").

69 Zakon, *supra* note 68.

70 *Id.*

71 *See* Mark Harrison, *What is the Origin of the Word "Internet"?*, QUORA (Sept. 2, 2011), http://www.quora.com/What-is-the-origin-of-the-word-internet.

72 Lawrence B. Solum & Chung Minn, *The Layers Principle: Internet Architecture and the Law*, 79 NOTRE DAME L. REV. 815, 816 (2004).

73 *Id.*

74 *See id.* at 816, 829-30.

75 *Id.* at 816, 841.

76 *Id.* at 816, 840 (stating that a "data packet" is a smaller portion of the original digital request from the application layer to be sent to the network layer).

77 *Id.*

78 *Id.* at 816, 839-40.

79 *Id.* at 816, 839.

80 *Id.* at 838-39.

81 Lee Copeland, *How-To: TCP/IP*, COMPUTERWORLD (Jan. 17, 2000, 12:00 AM), http://www.computerworld.com/article/2593612/networking/tcp-ip.html.

puter and sending it as a complete packet.[82] IP, which is vital to the Internet layer, is primarily responsible for addressing, fragmenting, and reassembling the complete packets to accommodate the network.[83] These protocols require every network device to have a unique address, referred to as an IP address, to designate origin and destination.[84] Without the equivalent of a device's "electronic return address," requested information will not arrive at the proper destination.[85] IP addresses ensure that the fragmented information is reconstructed by IP into a complete packet, which eventually produces a picture or file.[86] The process of sending and receiving information through the Internet has a fixed starting and ending point;[87] each point has an identifiable address that can be easily traced.[88]

B. The World Wide Web

The Internet, also known as "a global network of networks,"[89] evolved into a behemoth that was difficult to navigate. The World Wide Web (Web) was created to streamline navigation.[90] All websites are connected through the Web,[91] and "if the Internet is the ocean, then the World Wide Web is a massive fleet of ships and submarines, taking people through that ocean."[92] The Web swiftly transformed the way people communicate and share information, and it happened on a global scale.[93] It became flooded with information from an array of

---

82 *See How TCP/IP Works*, TECHNET, http://technet.microsoft.com/en-us/library/cc786128(v=ws.10).aspx (last updated Mar. 28, 2003).

83 *Id.* (explaining that while IP does attempt to deliver packets between hosts, delivery is not guaranteed due to potential loss, improper sequence, duplication, or delay).

84 *See id.*

85 Every device that is connected to the Internet has an address, which is called an IP address. An IP address is needed so the information can be delivered to its destination. *IP 101: The Basics of IP Addresses*, WHATISMYIPADDRESS.COM, http://whatismyipaddress.com/ip-basics (last visited Sept. 8, 2014).

86 *How TCP/IP Works*, *supra* note 82.

87 *Id.*

88 *Id.*

89 Solum & Minn, *supra* note 72.

90 *Happy Birthday to the World Wide Web!*, THE PARISH GROUP (Mar. 14, 2014), http://www.parishgroup.com/2014/03/happy-birthday-to-the-world-wide-web/.

91 Vangie Beal, *The Difference between the Internet and the World Wide Web*, WEBOPEDIA (June 24, 2010), http://www.webopedia.com/DidYouKnow/Internet/Web_vs_Internet.asp (explaining that Internet is the infrastructure that connects computers, whereas the World Wide Web is an information-sharing protocol that links websites).

92 Abraham Riesman, *The Web Is Not the Internet (You're Probably Getting That Wrong)*, MOTHERBOARD (July 17, 2012), http://motherboard.vice.com/en_uk/blog/the-web-is-not-the-internet-you-re-probably-getting-that-wrong.

93 Shortly after Tim Berners-Lee invented the World Wide Web, Internet usage skyrocketed. Internet usage in 1995 was reported at 16 million and that number doubled nearly

Internet users and it had to be organized in a manner that makes it easier to retrieve.[94] Today, the Web is organized in two major components and a minor, hidden, subsection.[95] The surface web is at the top, which brings up results of a standard search on any search engine,[96] while the deep web contains search results on a library database.[97]

1. Surface Web v. Deep Web

Search engines such as Google, Bing, and Yahoo allow Internet users to access information on the surface web.[98] They are the vessels that take users to static and fixed documents or web pages on the Internet.[99] These pages already exist as files on web servers and are readily accessible via a hyperlink.[100] Most search engines work in a similar way.[101] For example, when a user enters a search in Google for "flights," Google sends "spiders" to index hyperlinks to static web pages that sell flight tickets.[102] The result of that search takes the user into the surface web, however, "it is estimated that even the best search engines can access only 16 percent of information available on the Web."[103] In order to go deeper into the Web, the user must click one of the hyperlinks and use the website to create a dynamic search for a specific flight.[104]

---

every year, for the following four years. It reached 36 million in 1996, 70 million in 1997, 147 million in 1998, 248 million in 1999, and today that number has reached 937 million. See *Internet World Stats*, http://www.internetworldstats.com/emarketi-ng.htm (last visited Sept. 7, 2014); *Internet Growth Statistics: Today's Road to e-Commerce and Global Trade Internet Technology Reports*, INTERNET WORLD STATS: USAGE AND POPULATION STATISTICS, http://www.internetworldstats.com/emarketing.htm (last visited May, 12, 2015).

94 *See* Bergman, *supra* note 1, at 8-9 (explaining the evolution of more sophisticated search engine methods).

95 *See* Jeff Stone & Charles Poladian, *Meet the Deep Web: Inside the Hidden Internet That Lies beyond Google*, INT'L BUS. TIMES (Nov. 19, 2014, 9:51 AM), http://www.ibtimes.com/meet-deep-web-inside-hidden-internet-lies-beyond-google-1725784.

96 *See* Brad Yale, *How the Internet Works: The Deep Web*, INFORMIT (Oct. 21, 2014), http://www.informit.com/blogs/blog.aspx?uk=How-the-Internet-Works-The-Deep-Web.

97 *See* Bergman, *supra* note 1.

98 *Id.*

99 *Id.*

100 *Id.* at 3.

101 *Id.* at 9-10.

102 A spider is an Internet bot that searches websites and indexes the websites based on the executed search. *See Spider*, TECHTERMS.COM, http://techterms.com/definition/spider (last visited Jan. 31, 2015) ("A spider is a software program that travels the Web (hence the name "spider"), locating and indexing websites for search engines.").

103 Rabia Iffat & Lalitha K. Sami, *Understanding the Deep Web*, LIB. PHIL. AND PRAC., May 21, 2010, at 2.

104 *Id.*

Since most of the content on the Internet is located in the deep web and search engines cannot find it, this part of the Web is only accessible through a specific web server.[105] The Deep Web includes websites with password protection; these databases cannot be indexed by search engines.[106] The search engine's software cannot gain access because "when an indexing spider comes across a database, it's as if it has run smack into the entrance of a massive library with securely bolted doors. Spiders can record the library's address, but can tell you nothing about the books, magazines or other documents it contains."[107] Books, magazines and other documents are a small portion of what makes up the deep web.[108]

Understanding what the deep web is and how to navigate it is a critical part of the analysis. But one must also understand the vastness of the deep web. According to a study conducted in 2000, information on the deep web is approximately 400 to 550 times larger than the content on the World Wide Web.[109] The study indicates that "[t]he deep web contains 7,500 terabytes of information compared to nineteen terabytes of information in the surface web."[110] When considering the number of documents available, the study provides that "[t]he deep web contains nearly 550 billion individual documents compared to the one billion of the surface web."[111] To put the enormity of the deep web into further perspective, "[m]ore than 200,000 deep web sites presently exist."[112] The study also shows that "[s]ixty of the largest deep web sites collectively contain about 750 terabytes of information — sufficient by themselves to exceed the size of the surface web forty times."[113]

Due to its size, "[t]he deep Web is the largest growing category of new information on the Internet."[114] Unlike websites on the surface web, "[d]eep web sites tend to be narrower, with deeper content, than conventional surface sites."[115] Furthermore, "[t]otal quality content of the deep web is 1,000 to 2,000 times greater than that of the surface web."[116] When it comes to organization,

---

105 *Id.*

106 *See id.*

107 Chris Sherman, *The Invisible Web*, FREEPINT.CO.UK, http://www.d.umn.edu/~fsimmons/invisible.htm (last visited Jan. 25, 2015).

108 Bergman, *supra* note 1, at 4, 10-11 (demonstrating the diversity of Deep Web content; classified 17,000 Deep Web sites into twelve categories: 1. Topic Databases, 2. Internal Sites, 3. Publications, 4. Shopping/Auction, 5. Classifieds, 6. Portals, 7. Library, 8. Yellow and White Pages, 9. Calculators, 10. Jobs, 11. Message or Chat, and 12. General Search).

109 *Id.* at 1.

110 *Id.*

111 *Id.*

112 *Id.*

113 *Id.*

114 *Id.* at 2.

115 *Id.*

116 *Id.*

compared to the surface web "[m]ore than half of the deep web content resides in topic-specific databases."[117] When it comes to access " [a] full ninety-five per cent of the deep web is publicly accessible information — not subject to fees or subscriptions."[118] Hidden underneath the deep web is a dark web, which is comprised of "websites that are outdated, broken, abandoned, or inaccessible using standard web browsing techniques."[119]

2. Dark Web, Darknets and Going Dark

The dark web consists of underground websites and databases.[120] This part of the web can be used for host malware, sale of illicit drugs, child pornography, hit men, terrorists, and money laundering services.[121] Websites like the "Silk Road," "Pandora Market," and "Hydra Marketplace" offer such services.[122] These underground websites use "bitcoins" as the main form of currency for the illicit transactions.[123] "Bitcoins" are online currency with no central authority or banks, which are exchanged online.[124] Alternatively, political activists, the military, corporate whistleblowers, and victims of abuse use the dark web to maintain confidentiality while exercising their freedom of speech.[125] The dark web is only accessible through special web browsers called darknets. A darknet is "any closed, private network that operates on top of the more conventional Internet Protocols."[126] Darknets bypass TCP/IP to ensure "anonymous, virtually untraceable global networks . . . ."[127] Programs like The Onion Router, Freenet, and I2P allows users to join these darknets and "go dark."[128]

---

117 *Id.*

118 *Id.* at 4.

119 *The Dark Web*, DARK SIDE OF THE WEB, https://davidenewmedia.wordpress.com/workingterms/darkweb/ (referencing LEAH A. LIEVROUW, ALTERNATIVE AND ACTIVIST NEW MEDIA (2011)).

120 GARY PRICE & CHRIS SHERMAN, THE INVISIBLE WEB: UNCOVERING INFORMATION SOURCES SEARCH ENGINES CAN'T SEE 57 (2001).

121 Stuart Andrews, *The Dark Side of the Web*, PC PRO (Mar. 9, 2010), http://www.pcpro.co.uk/features/356254/the-dark-side-of-the-web.

122 *See* Jan Dekadent, *How the Dark Web's New Favorite Drug Market is Profiting from Silk Road 2's Demise*, MAINSTREAMLOS BLOG, http://mainstreamlos.blogspot.com/2014/12/how-dark-web-new-favorite-drug-market.html (identifying Evolution as the new online drug market in the wake of seizures of Silk Road, Pandora Market, and Hydra Marketplace).

123 *Id.*

124 BITCOIN, https://bitcoin.org/en/ (last visited Nov. 2, 2014).

125 Andrews, *supra* note 121.

126 *Id.*

127 Adrian Goldberg, *The Dark Web: Guns and Drugs for Sale on the Internet's Secret Black Market*, BBC NEWS (Feb. 3, 2012), http://www.bbc.com/news/business-16801382.

128 Andrews, *supra* note 121.

3. The Onion Router

The Onion Router ("Tor") started as a project by the U.S. Navy for ensuring secure government communications,[129] and then became a free program that helps Internet users defend against network surveillance.[130] As indicated by the name, Tor's software is an onion routing network, which consists of many layers of relay nodes.[131] When data is sent and received through the Tor network, it is encrypted in multiple layers and passes to a random server on the network, called a node.[132] The first node removes a layer of encryption, and then sends it to another random node, which repeats the same process and "each relay along the way knows only which relay gave it data and which relay it is giving data to…," which adds to the secretive nature.[133] Eventually, the data reaches an exit node that unencrypts the data and sends it to its destination.[134] Once the data reaches its final destination, it is then sent back through another randomized path as encrypted data.[135] There are over 5,000 nodes all over the world, making it nearly impossible to trace the original destination.[136]

4. Efforts to Thwart Tor

Tor's mission to allow its users to be anonymous on the Internet has been opposed by the NSA,[137] while "other branches of the federal government are

---

129 *Tor: Overview*, TORPROJECT.ORG, https://www.torproject.org/about/overview.html.en (last visited Jan. 31, 2015).

130 *Tor: Anonymity*, TORPROJECT.ORG, https://www.torproject.org/ (last visited Jan. 31, 2015).

131 Jan Camenisch & Anna Lysyanskaya, *A Formal Treatment of Onion Routing*, *in* ADVANCES IN CRYPTOLOGY – CRYPTO2005: 25TH ANNUAL CRYPTOLOGY CONFERENCE, SANTA BARBARA, USA, AUG. 14-18, 2005 PROCEEDINGS, 169-87 (V. Shoup. Ed., 2005), *available at* http://cs.brown.edu/people/anna/papers/cl05-full.pdf.

132 Margaret Rouse, *Encryption*, WHATIS.COM, http://searchsecurity.techtarget.com/definition/encryption (last visited Sept. 7, 2014) ("Encryption is the conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people.").

133 *Tor: Overview*, *supra* note 129.

134 *Questions*, Answer to *Why can a Tor exit node decrypt data, but not the entry node?*, STACKEXCHANGE.COM, http://security.stackexchange.com/questions/36571/why-can-a-tor-exit-node-decrypt-data-but-not-the-entry-node (last updated May 28, 2013, 4:08 PM).

135 *Tor: Overview*, *supra* note 129.

136 *Tor Metrics-Servers*, TORPROJECT.ORG, https://metrics.torproject.org/network.html (last visited Jan. 31, 2015); *see, e.g.*, *Tor Metrics-Relays with Exit, Fast, Guard, Stable, and HSDir flags*, TORPROJECT.ORG, https://metrics.torproject.org/relayflags.html (last visited Jan. 31, 2015) (displaying a graph illustrating over 5,000 running relays within the Tor network); *see generally Tor Metrics -About*, TORPROJECT.ORG, https://metrics.torproject.org/about.html#relay (last visited Jan. 31, 2015) (defining a relay as "publicly listed node in the Tor network that forwards traffic on behalf of clients, and that registers itself with the directory authorities").

137 Peterson, *supra* note 17.

helping fund [Tor's] service."[138] The NSA "has been reportedly waging an ever-evolving stealth campaign against the service for years."[139] James Clapper, director of the NSA, asserts that online anonymity should be eliminated "based on the undeniable fact that these are the tools our adversaries use to communicate and coordinate attacks against the United States and our allies."[140]

The complexity and depth of Tor's software has made it difficult for the NSA to find weaknesses or bugs.[141] They began a program codenamed "EgotisticalGiraffe" that attacks users downloading Tor on outdated browsers.[142] EgotisticalGiraffe recognizes the Tor download, infects the user's computer or phone with malware, which allows the NSA to monitor the downloader's activity.[143] According to Roger Dingledine, president of the Tor Project, this method does not allow them to do mass surveillance because "[t]here's no indication they can break the Tor protocol or do traffic analysis on the Tor network."[144] It only allows them to identify specific users who downloaded Tor on an outdated browser.[145]

III. REMAINING ANONYMOUS AND THE RIGHT TO PRIVACY

The Framers of the Constitution recognized that the right to privacy and protection from unreasonable searches and seizures are both fundamental liberty interests.[146] These beliefs sparked the American Revolution against Great Britain after King George III repeatedly encroached upon these rights when he issued broad warrants that allowed agents to search any property.[147] Benjamin Franklin famously said, "Those who would give up essential Liberty, to pur-

---

138 *Id.*

139 *Id.*

140 *Id.*

141 James Ball et al., *NSA and GCHQ Target Tor Network That Protects Anonymity of Web Users*, THE GUARDIAN (Oct. 4, 2013), http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption.

142 *See id.* (identifying the specific vulnerability of older versions of the browser Firefox).

143 *Id.*

144 *Id.*

145 *Id.*

146 U.S. CONST. amend. IV

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Id.

147 *What are The Writs of Assistance?*, THE FOUNDERS CONST., http://press-pubs.uchicago.edu/founders/documents/amendIVs2.html (last visited Jan. 31, 2015).

chase a little temporary Safety, deserve neither Liberty nor Safety."[148] Franklin's quote became the rallying cry during the Revolution.[149] The fear of giving a government an unchecked power over its citizens' right to security and privacy underlies the Fourth Amendment.[150]

A. Political Activists

Freedom of speech is both a universal human right and a crucial element of a democratic society.[151] This right, however, is not recognized in many parts of the world.[152] North Korea, Iran, Cuba, and Saudi Arabia restrict speech and control the dissemination of domestic and international media.[153] The Internet is a powerful method for communication, and offers a vital tool for people to communicate, cooperate, and collaborate.[154] Revolutions that are spurred online capture the opinions, events, and experiences of a people over a period of time.[155] For example, social media played a significant role in the "Arab Spring" revolutions that occurred throughout the Middle East in 2010.[156]

A political activist's ability to go dark and garner support against an oppressive government may be risky.[157] For example, Malala Yousafzai, a 14-year-old Pakistani girl, started a blog at the age of 11, documenting her terror of the Taliban and ambitions of becoming a doctor.[158] Taliban members were angered

---

148 Independence Hall Ass'n, *The Electric Ben Franklin: Quotable Franklin*, USHISTORY.ORG, http://www.ushistory.org/franklin/quotable/quote04.htm (last visited Sept. 11, 2014).

149 *Id.*

150 U.S. CONST. amend. IV.

151 *The Universal Declaration of Human Rights*, UNITED NATIONS, http://www.un.org/en/documents/udhr/ (last visited Jan. 30, 2015).

152 *10 Most Censored Countries*, COMMITTEE TO PROTECT JOURNALISTS (May 2, 2012), http://cpj.org/reports/2012/05/10-most-censored-countries.php.

153 Frederick Reese, *Journalism's Future Could Depend on Tor's Security*, MINT PRESS NEWS (Dec. 27, 2013), http://www.mintpressnews.com/journalisms-future-depend-tors-security/175683.

154 *See, e.g.*, Jose Antonio Vargas, *Spring Awakening*, N.Y. TIMES, Feb. 19, 2012, at 12.

155 *See, e.g.*, *id.*

156 *See, e.g.*, *id.*

157 Chris Green, *British woman Roya Nobakht could be executed in Iran after insulting Islam on Facebook*, THE INDEPENDENT (Apr. 2, 2014), http://www.independent.co.uk/news/world/middle-east/british-woman-jailed-in-tehran-for-insulting-islam-and-iranian-government-on-facebook-fears-execution-9233732.html (explaining that a woman was arrested for posting comments online attacking the Iranian government).

158 Declan Walsh, *Taliban Gun Down Girl Who Spoke Up for Rights*, N.Y. TIMES, Oct. 10, 2012, at 1. Malala Yousafzai won the Nobel Peace Prize for motivating the "struggle against the suppression of children and young people and for the right of all children to education." Her achievements would not have been possible without the ability to use the Internet. *See Malala Yousafazai*,

by Yousafzai's values and her notoriety she attained through her online blog. [159] The Taliban claimed she was becoming a symbol for the West and attempted to kill her.[160] Similarly, other journalists and political dissidents need to remain anonymous if they wish to use the Internet to discredit repressive regimes.[161]

B. The Internet's role in Propaganda

Propaganda is a powerful tool for uniting a group of people or nation behind a single goal.[162] For example, Germany used propaganda in the 1930s to gain the public support needed to wage war and kill over six million Jews.[163] The Nazis limited the information available to the German people and the international community.[164] As a result, the international community did not know the extent of the atrocities that occurred in concentration camps until the end of the War.[165] The Nazis had intended to keep the extermination of Jews a secret.[166]

More recently, civil unrest broke out following the shooting of Michael Brown in Ferguson, Missouri, and officials attempted to suppress the spread of information.[167] Police fired rubber bullets and tear gas at journalists who were attempting to document the scene and arrested others.[168] The police's efforts

---

NOBELPRIZE.ORG, http://www.nobelprize.org/nobel_prizes/peace/laureates/2014/yousafzai-facts.html (last visited Jan. 30, 2015).

159 Walsh, *supra* note 158.

160 *Id.*

161 *See, e.g.*, Joe Bendel, *The Dangers of Blogging in Oppressive Regimes: Film*, THE EPOCH TIMES (June 11, 2013), http://www.theepochtimes.com/n3/101790-the-dangers-of-blogging-in-oppressive-regimes/print.php (discussing Zeng Jinyan, a human rights blogger that the Chinese Communist Party blocked from leaving her apartment, placing her on house arrest).

162 *Nazi Propaganda*, U.S. HOLOCAUST MEMORIAL MUSEUM, http://www.ushmm.org/wlc/en/article.php?ModuleId=10005202 (last updated June 20, 2014) (citing Adolf Hitler's use of propaganda as an effective tool to build the Nazi state in Germany).

163 *How did the Nazis use Propaganda?*, THE HOLOCAUST EXPLAINED, http://www.theholocaustexplained.org/ks4/the-nazification-of-germany/impact-of-the-nazi-state/how-did-the-nazis-use-propaganda/#.VGvo6mYo670 (last visited Jan. 30, 2015).

164 *Id.*

165 The world was made aware of the extent of Nazi atrocities especially through the Nuremberg Trials, a public prosecution of Nazi party members, soldiers, and scientists. *The Nuremberg Trials*, U.S. HOLOCAUST MEMORIAL MUSEUM, http://www.ushmm.org/outreach/en/article.php?ModuleId=10007722 (last visited Mar. 28, 2015).

166 *American Response to the Holocaust*, HISTORY, http://www.history.com/topics/world-war-ii/american-response-to-the-holocaust (last visited Jan. 30, 2015).

167 Christopher Zara, *Ferguson Media Blackout: Mike Brown Shooter Hidden, Journalists Arrested, Secrecy Backfires*, INTES BUS. TIMES (Aug. 14, 2014), http://www.ibtimes.com/ferguson-media-blackout-mike-brown-shooter-hidden-journalists-arrested-secrecy-backfires-1658836.

168 *Id.*

backfired as journalists uploaded the police's actions to the Internet.[169] Without the Internet, the rest of the country may have never known the seriousness of the events in Ferguson.[170] By controlling access to news via the Internet, a government can portray itself in a more favorable light and greatly influence public opinion.[171] If journalists cannot go dark to bypass government censorship, corrupt regimes, such as that of Bashar Al-Assad in Syria, may continue indefinitely.[172]

IV. PROPOSITION

A. Reapplying the Fourth Amendment

The application of the Fourth Amendment to Internet surveillance has expanded the government's ability to conduct unreasonable searches. The government's power is currently unchecked and must be recalibrated.[173] The Court's interpretation in *Katz,* that the Fourth Amendment protects people, not places, and that people have a "reasonable expectation of privacy" has become irrelevant due to the advances in technology.[174] Understanding that the Internet is, in theory, a place where content flows, and renders nearly everything on the Internet incapable of protection under the Fourth Amendment.[175] Instead of adopting a narrow interpretation, legislatures need to apply the broader rationale behind the Fourth Amendment, which reasons, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[176] The Court must better protect what a person seeks to preserve as private.[177]

---

169 *Id.*

170 *What Happens to #Ferguson Affects Ferguson*, MEDIUM.COM (Aug. 14, 2014), https://medium.com/message/ferguson-is-also-a-net-neutrality-issue-6d2f3db51eb0.

171 *10 Most Censored Countries*, *supra* note 152 (explaining that North Korea controls all media within its borders, and most news are skewed in the government's favor).

172 *See, e.g.*, Walsh, *supra* note 158 (stating that Malala Yousafzai was targeted because of her powerful voice as a woman for the rights of children).

173 Katz v. United States, 389 U.S. 347, 347 (1967).

174 *See* United States v. Jones, 132 S. Ct. 945, 957 (2012); Bond v. United States, 529 U.S. 334, 339 (2000) (holding that the Fourth Amendment protects an individual that exhibits and expectation of privacy if it is "one that society is prepared to recognize as reasonable").

175 Hatcher v. State, 726 S.E.2d 117, 119 (Ga. App. 2012) (citing Rehberg v. Paulk, 611 F.3d 828, 842-47 (11th Cir. 2010)).

176 *Katz*, 389 U.S. at 351.

177 *Id.* at 331.

The reasonable expectation of privacy is a two-pronged test. First, the person must have an actual subjective expectation of privacy.[178] Second, society must recognize that that subjective expectation is "reasonable."[179] Following the *Katz* decision, Fourth Amendment jurisprudence held that there is no reasonable expectation of privacy regarding information voluntarily given to a third party.[180] Thus, the use of a pen register, a device that records phone numbers dialed from a phone, pursuant to a court order, does not constitute a search for Fourth Amendment purposes.[181] There is no reasonable expectation of privacy because the person dialing the phone number is sending this information to the telephone company, a third party, and requesting a connection through the company's equipment.[182]

The Snowden revelations show that an extremely broad legal certification permits the NSA to obtain this data.[183] The NSA and FBI have acquired "telephone metadata in bulk" pursuant to Section 215 of the USA PATRIOT Act.[184] A Section 215 order compels a company to produce any "tangible things" required "for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution."[185] The court order requires approval by the FISA court and must be supported by "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation."[186] The court orders were approved and used to compel Verizon to give daily records of all calls, "telephony metadata" between the United States and foreign nations, and local calls within the United States.[187] The NSA has admitted to collecting records of millions of U.S. citizens indiscriminately, regardless of misconduct.[188] This data collected is stored for at least five years on separate NSA servers.[189]

---

178 *Id.* at 361.

179 *Id.*

180 Smith v. Maryland, 442 U.S. 735, 743-44 (1979).

181 *Id.* at 744-46.

182 *Id.* at 742-44.

183 *See* Ellen Nakashima & Barton Gellman, *For NSA*, *Broad Leeway to Intercept Data,* WASH. POST, July 1, 2014, at A14 (noting the breadth of locations from which the NSA is permitted to collect data).

184 David S. Kris, *On the Bulk Collection of Tangible Things*, 7 J. OF NAT'L SECURITY L. & POL'Y 209, 209-10 (2014).

185 50 U.S.C. § 1861 (2012).

186 *Id.*

187 Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 6, 2013, 6:05 PM), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

188 *See* Klayman v. Obama, 957 F. Supp. 2d 1, 10 (D.D.C 2013) (noting that the NSA

The NSA gains complete control over the data once it is placed on their servers, with statutory limitations.[190] After which, NSA intelligence analysts have the discretion to access the information on the servers through "queries" that use "identifiers," like phone numbers.[191] However, one of twenty-two designated NSA officials must approve that the "identifiers" used to search the database gives rise to a "reasonable, articulable suspicion," and the search term "is associated with one or more of the specified foreign terrorist organizations approved for targeting by the [Foreign Intelligence Surveillance Court ("FISC")]."[192] Requiring such approval is moot. Once the warrant is approved by the FISC, there is no legal authority to ensure the approving NSA official has a "reasonable, articulable suspicion."[193] Executive officers may have a reasonable, articulable suspicion with respect to a small portion of the surveillance they approve, but the vast majority of the surveillance approved is unlikely to be reasonable and more likely to be intrusive.[194] Regardless, the Supreme Court "has never sustained a search upon the sole ground that officers reasonably expected to find evidence of a particular crime and voluntarily confined their activities to the least intrusive means consistent with that end."[195] Traditional Fourth Amendment analysis requires a neutral and detached magistrate, "not the risk that executive discretion may be reasonably exercised."[196]

The NSA asserts that the identifiers are limited to identifying persons associated with foreign terrorist organizations and should be allowed because it is vital to NSA's counterterrorism mission.[197] However, evidence has pointed to the contrary.[198] A report to the government in 2009 showed that as of January 15, 2009, a staggering 1,935 of the 17,835 identifiers approved by the designated NSA officers were based on a reasonable, articulable suspicion.[199] Although this appears to be a clear abuse of discretionary authority under § 1861,

---

confirmed the authenticity of the Edward Snowden leaks).

189 *Id.* at 26.

190 *See id.* at 15-16 (explaining the processes for accessing the data and noting that all approvals within this process are completed within the NSA).

191 *Id.* at 16.

192 *Id.*

193 *See* Decl. of Acting Assistant Dir. Robert J. Holley FBI at 7, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (No. 13 Civ. 3994(WHP)) (explaining the approval process in its entirety).

194 *See* 957 F. Supp. 2d at 18-19 (noting specific violations that have occurred).

195 United States v. United States Dist. Ct., E. D. Of Mich., 407 U.S. 297, 317 (1972) (quoting Katz v. United States, 389 U.S. 347, 357 (1967)).

196 *Id.*

197 *Klayman*, 957 F. Supp. 2d at 16; Decl. of Acting Assistant Dir. Robert J Holley FBI at 11, *Clapper*, 959 F. Supp. 2d 724 (No. 13 Civ. 3994(WHP)).

198 In re Production of Tangible Things From [redacted], No. BR 08-13, 2009 WL 9150913, at *2 (FISA Ct. 2009).

199 *Id.* at n.2.

the NSA argues that the bulk collection of Internet metadata is similar to a pen register and does not constitute a search within the meaning of the Fourth Amendment.[200]

The government relies on outdated court decisions to say that the nature of the data collected from providers (phone numbers, time of call, and date of call) under section 215 is similar to what pen registers permit.[201] The current mantra is to treat NSA's surveillance as it was treated in *Smith v. Maryland*.[202] There is a stark difference between how much data can be collected via a pen register in the 20th century and how much data the NSA is able to collect today.[203] A pen register in the 20th century allowed government officials to view a suspected individual's incoming and outgoing calls for a specified length of time.[204] The NSA equivalent of a "pen register" works in this fashion:

> [A] search starts with telephone number (123) 456–7890 as the "seed," the first hop will include all the phone numbers that (123) 456–7890 has called or received calls from in the last five years (say, 100 numbers), the second hop will include all the phone numbers that each of *those* 100 numbers has called or received calls from in the last five years (say, 100 numbers for each one of the 100 "first hop" numbers, or 10,000 total), and the third hop will include all the phone numbers that each of *those* 10,000 numbers has called or received calls from in the last five years (say, 100 numbers for each one of the 10,000 "second hop" numbers, or 1,000,000 total).[205]

This type of surveillance is grossly different from a simple pen register. Judge Richard Leon asserts, "I am convinced that the surveillance program now before me is different from a simple pen register and that *Smith* is of little value in assessing whether the Bulk Telephony Metadata Program constitutes a Fourth Amendment search."[206] The warrant is not limited to the collection of data on a single individual; it is mass surveillance that is capable of gathering data on every U.S. citizen.[207] An individual certainly has a subjective expectation of privacy against this type of intrusion, because they would not have to dial the number of the target in question to be captured in NSA search results.[208] If the U.S. population knew how detailed and intrusive the searches were, then societal norms would certainly recognize the collection and analysis of metadata as unreasonable.[209]

---

200 *See* 957 F. Supp. 2d at 37 (detailing that the NSA's argument that their metadata collection did not constitute a search under the Fourth Amendment did not prevail).

201 ACLU v. Clapper, 959 F. Supp. 2d 724, 752 (S.D.N.Y. 2013).

202 *Id.*

203 957 F. Supp. 2d at 35-36.

204 Smith v. Maryland, 442 U.S. 735, 736 (1979).

205 *Klayman*, 957 F. Supp. 2d at 16.

206 *Id.* at 32.

207 *See id.* at 16 (detailing the amount of individuals that can be included in a single query).

208 *Id.*

209 Remarks as Prepared for Delivery at Brookings Institution, Robert S. Litt, Gen. Counsel Office of the Dir. Of Nat'l Intelligence, Privacy, Technology, and National Securi-

It should not be said that U.S. citizens assume the risk of government surveillance through the use of third party channels.[210] Yet, for citizens to assume the risk, there must be some notion of choice and unless citizens are willing to go back to outdated ways of communication, they have to accept the risk of surveillance.[211] It is evident that most people in the 21st century rely heavily on cellphones and the Internet in their daily lives.[212] Citizens should not have to give up their privacy when they have no other option. The Fourth Amendment should protect American citizens against NSA practices under section 215 because it violates the reasonable expectation of privacy, and "[i]t is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative."[213]

B. Fourth Amendment Protection for Darknets

By nature, the Internet is a public network.[214] Therefore, anytime someone uses it, they are knowingly exposing information to the public.[215] Courts have consistently held that senders and recipients of standard mail have no reasonable expectation of privacy with respect to information "put on the outside of mail, because that information is voluntarily transmitted to third parties."[216] Similarly, "e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit."[217] A Verizon customer has no reasonable expectation of privacy because they are giving their IP address voluntarily to Verizon.[218]

---

ty: An Overview of Intelligence Collection (July 19, 2013), http://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/896-privacy,-technology-and-national-security-an-overview-of-intelligence-collection.

210 *E.g.* Smith v. Maryland, 442 U.S. 735, 748 (1979).

211 *Id.* at 749-50.

212 *See* Kristen Purcell & Lee Rainie, *Americans Feel Better Informed Thanks to the Internet*, PEW RESEARCH CTR. 2, n.1 (2014), http://www.pewinternet.org/files/2014/12/PI_InformedWeb_120814_02.pdf (stating that 87% of online adults believe cell phones and the Internet have improved their ability to learn new things).

213 *Smith*, 442 U.S. at 750.

214 *See* ACLU v. Reno, 929 F. Supp. 824, 831 (E.D. Pa. 1996), *aff'd*, 521 U.S. 844 (1997).

215 *Id.* at 832.

216 United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2008); *see* United States v. Hernandez, 313 F.3d 1206, 1209-10 (9th Cir. 2002) ("[A]lthough a person has a legitimate interest that a mailed package will not be opened and searched en route, there can be no reasonable expectation that postal service employees will not handle the package or that they will not view its exterior.").

217 512 F.3d at 510.

218 *See id.* at 510-11.

But what if someone is using a closed network, or a darknet such as Tor, to conceal his or her IP address? If a sender places an envelope within a box, then traditional analysis yields that content on the outside of the box is public information, while content on the outside of the envelope, which is inside the box, is not public information. Only the outside layer is voluntarily transmitted to third parties. Analogously, Tor users disguise their IP addresses using the same layering technique.[219] A Verizon customer using Tor does not voluntarily give the company their IP address because Verizon cannot see it. Instead, Verizon receives a multi-layered request.[220] The customer's actual IP address is not public information, because it is hidden beneath a layer that contains a different IP address, which is what Verizon can see.[221]

This analysis follows *Katz*, insofar as "what a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[222] Although the Internet is a public network and requests sent to an ISP provider are public information,[223] people use Tor's software in order to preserve their privacy[224] and they must be constitutionally protected. Accordingly, the NSA should be required to obtain a search warrant in order to unencrypt the onion routing system and trace IP addresses.[225]

C. National Security and Counter-terrorism

The NSA asserts that the current government surveillance scheme is a special case because national security is at stake and the program is part of a counter-terrorism effort.[226] Therefore, the NSA must provide a compelling case and "[i]t is obvious and unarguable that no governmental interest is more compelling than the security of the nation."[227] The government must balance individual rights against the immediacy of the threat and the efficacy of the NSA's sur-

---

219 *Overview of Tor*, TOR, https://www.torproject.org/about/overview.html.en (last visited Jan. 17, 2015).

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

221 *Id.*

222 Katz v. United States, 389 U.S. 347, 351-52 (1967).

223 United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008).

224 Lee, *supra* note 220.

225 *See generally* 389 U.S. at 351-52; *see also* Peterson, *supra* note 17.

226 Sean Sullivan, *NSA head: Surveillance helped thwart more than 50 terror plots,* WASH. POST (June 18, 2013), http://www.washingtonpost.com/blogs/post-politics/wp/2013/06/18/nsa-head-surveillance-helped-thwart-more-than-50-terror-attempts/.

227 Haig v. Agee, 453 U.S. 280, 307 (1981).

veillance program.[228] The current level of surveillance constitutes a significant intrusion on privacy rights.

The legislation in question was enacted in response to 9/11.[229] Section 215 "enables the Government to quickly analyze past connections and chains of communication, and increases the NSA's ability to rapidly detect persons affiliated with the identified foreign terrorist organizations."[230] The government acknowledges that other methods are available, but claim that they are complex and time-consuming, and might jeopardize the NSA's counter-terrorism efforts.[231] According to General Keith Alexander, the former NSA director, surveillance gathered pursuant to section 215 has thwarted fifty potential terrorist attacks since September 11, 2001, including at least ten on American soil.[232] Yet the government has not offered a single case "in which NSA's bulk metadata collection actually stopped an imminent attack, or otherwise aided the Government in achieving any objective that was time-sensitive in nature."[233]

It is difficult to accept the NSA's assertion that the time-sensitive nature of the counterterrorism program is a compelling enough reason to intrude on the citizenry's privacy rights. Less intrusive methods that require a heightened level of scrutiny, which may be slightly more time-consuming, must be set in place. The first step is transparency, so the American people and elected officials know the extent of the NSA's surveillance practices. The second step is for legislators and courts to recognize that the NSA's rationale is unreasonable. Finally, legislators need to amend the regulations governing NSA surveillance.

B. Checks and Balances

The efficiency of bulk data collection under section 215 and the immediacy of the threat to national security are insufficient to override the Fourth

---

228 Klayman v. Obama, 957 F. Supp. 2d 1, 38 (D.D.C. 2013).

229 John T. Soma et al., *Balance of Privacy vs. Security: A Historical Perspective of the USA PATRIOT Act*, 31 RUTGERS COMPUTER & TECH. L.J. 285 (2005).

230 957 F. Supp. 2d at 40.

231 *Id.* at 39-40.

232 Sullivan, *supra* note 226.

233 957 F. Supp. 2d at 40

> In the first example, the FBI learned of a terrorist plot still 'in its early stages' and investigated that plot before turning to the metadata 'to ensure that all potential connections were identified.' In the second example, it appears that the metadata analysis was used only after the terrorist was arrested 'to establish [his] foreign ties and put them in context with his U.S. based planning efforts.' And in the third, the metadata analysis 'revealed a previously unknown number for [a] co-conspirator . . . and corroborated his connection to [the target of the investigation] as well as to other U.S.-based extremists.'

Id.

Amendment.[234] The judiciary's role in government surveillance jurisprudence extends beyond a reapplication of the Fourth Amendment.[235] The judicial branch must reclaim the power they transferred to FISC under FISA.[236]

One of the core principles of the United States Constitution is the system of checks and balances.[237] The judicial branch has been extremely hesitant to oppose the government with regard to intelligence surveillance.[238] In *In re Application of F.B.I.*, the FISA Court approved the collection of telephony metadata on U.S. citizens and interpreted the NSA's surveillance practices as indistinguishable from a pen register.[239] In similar fashion, an Idaho court held, in *Smith v. Obama,* that a citizen seeking an injunction against NSA telephony metadata collection has no reasonable expectation of privacy with respect to her cellphone data.[240] Other courts dismissed similar actions on the basis that plaintiffs lack standing.[241] For example, a District Court in Washington, D.C. held that the plaintiff lacked standing, because "[h]is generalized fear that his communications are being intercepted 'is insufficient to create standing.'"[242]

Opponents of current wiretapping and surveillance legislation have garnered little support from the courts because national security concerns have prevented revisions to surveillance regulations.[243] At the same time, the executive branch's authority in this area has been greatly expanded following 9/11.[244] The 9/11 attacks resulted in "the single largest loss of life from a foreign attack on American soil," and left the nation in a state of terror.[245] The government has

---

234 *See id.* at 39, 41.

235 RONALD WEICH, AM. CIVIL LIBERTIES UNION, UPSETTING CHECKS AND BALANCES: CONGRESSIONAL HOSTILITY TOWARD THE COURTS IN TIME OF CRISIS 4 (Norma Fritz ed., Dep't of Pub. Educ. 2001), *available at* https://www.aclu.org/national-security/report-upsetting-checks-and-balances-congressional-hostility-toward-courts-times-c.

236 *See* Nakashima & Gellman, *supra* note 182.

237 *See, e.g.*, David Stedman & La Vaughn G. Lewis, *Separation of Powers – the genius of America's Constitution*, NAT'L CENTER FOR CONT. STUD. (2015), http://www.nccs.net/separation-of-powers-the-genius-of-americas-constitution.php.

238 957 F. Supp. 2d at 43-44.

239 *See In re* Application of F.B.I., No. BR 14-01, 2014 WL 5463097, at *4 (FISA Ct. 2014); *see also id.* at *7 (noting there is no justification for deviating from *Smith* because of the nature of telephony metadata); *see also id.* at *11 (concluding *Smith* remains the precedent where non-content call records exist).

240 Smith v. Obama, 24 F. Supp. 3d 1005, 1009 (D. Idaho 2014).

241 Clapper v. Amnesty International USA et al, 133 S. Ct. 1138, 1143 (2013).

242 Robinson v. Obama, 2014 WL 1389020, at *1 (D.D.C 2014) (citing Clapper v. Amnesty Intern. USA, 133 S. Ct. 1138, 1152 (2013)).

243 Joshua Kopstein, *Denied in the Supreme Court, Warrantless Wiretap Opponents are Losing Ground Fast*, THE VERGE (Mar. 1, 2013, 3:32 PM), http://www.theverge.com/201313/1/4043944/denied-in-the-supreme-court-warrantless-wiretap-opponents-are-losing.

244 *Id.*

245 *11 Facts About 9/11,* DOSOMETHING.ORG, https://www.dosomething.org/facts/11-facts-about-911 (last visited Jan. 30, 2015).

an obligation to protect citizens from another attack.[246] Nonetheless, there must be a balance between the constitutional rights of the individual and the government's surveillance practices.[247]

The judicial branch must fulfill its constitutional function by serving as a check on the authority of the executive and legislative branches.[248] The FISA court has failed to restrain the power of intelligence agencies over the past two decades. For example, the FISA court approved 20,909 warrants, approximately thirty-three surveillance warrants per week, from 2001 to 2012.[249] During that span, FISA court judges denied only ten applications and approved over 500 business record warrants, which also include bulk metadata from phone and Internet providers under section 215.[250] Most notably, the FISA court "substantially modified" 376 of the 417 business record warrants for 2011 and 2012.[251] It can be reasonably inferred that the modifications by the court show that the FISA court is doing everything it can to approve warrants for the NSA, because the court does not reject them completely.

The FISA court is classified and works in complete secrecy.[252] The judges who preside over this court are appointed to a term of one to seven years by the Chief Justice of the United States.[253] Judges meet with prosecutors and federal agents in a secure room to hear application requests for warrants.[254] According to Reggie Walton, former senior judge at the FISA court, the meetings consist of

> a rigorous review process of applications submitted by the executive branch, spearheaded initially by five judicial branch lawyers who are national security experts, and then by the judges, to ensure that the court's authorizations comport with what the applicable statutes authorize.[255]

Walton's statements are difficult to believe given that FISA judges granted 99.9% of warrant requests in the twelve years following 9/11.[256]

The FISA court's warrant approval rate has led many to believe they are a rubber stamp for the executive branch and are failing to perform their judicial duty.[257] Furthermore, FISA court proceedings are *ex parte*, which means they

---

246 THE 9/11 COMM., THE 9/11 COMMISSION REPORT INCLUDING EXECUTIVE SUMMARY xvi (2004).

247 United States v. United States Dist. Ct., E. D. Of Mich., S. D., 407 U.S. 297, 317-318 (1972).

248 *Id.* at 317.

249 Shiffman & Cooke, *supra* note 46.

250 *Id.*

251 *Id.*

252 *Id.*

253 50 U.S.C. §§ 1803(a)(1), (d) (2012).

254 Shiffman & Cooke, *supra* note 46.

255 *Id.*

256 *Id.*

257 Carol D. Leonnig, Ellen Nakashima & Barton Gellman, *Judge Defends Role in Spy-*

only hear from one party.[258] The government justifies an *ex parte* proceeding because adversarial proceedings are time-consuming, costly, and can obstruct investigations.[259] However, there is a reasonable concern that without someone to argue the other side, the FISA court is turning into "an administrative, rather than a judicial, body."[260] James Robertson, a former FISA judge, explains, a judge must hear both sides of a case to remain unbiased and impartial.[261]

Provisions mandate that the denial of any application before the FISA court is reviewed by three judges from the U.S. District Courts.[262] Additionally, if the application is denied a second time, the Supreme Court has jurisdiction to review the application and approve it.[263] The current system allows the NSA three opportunities to petition the courts for approval of vague, broad, and continuing warrants, all of which are *ex parte*.[264] Furthermore, § 1861 does not include an express right for third parties to challenge the legality of the NSA's production orders approved under § 1803.[265] The party that may challenge the NSA in court is the person or entity receiving a production order, which is limited by a one year statute of limitations.[266] Litigation is further limited because § 1861 requires:

> A judge considering a petition to modify or set aside a nondisclosure order may grant such petition only if the judge finds that there is no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person.[267]

Moreover, if the judge's discretion finds that disclosure will not endanger the national security of the United States, that decision may be overturned:

> If, upon filing of such a petition, the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of the Federal Bureau of Investigation cer-

---

ing, WASH. POST, June 30, 2013, at A1.

258 § 1805(a).

259 Klayman v. Obama, 957 F. Supp. 2d 1, 40 (D.D.C 2013).

260 Shiffman & Cooke, *supra* note 46.

261 *Former judge admits flaws with secret FISA court*, CBS NEWS (July 9, 2013), http://www.cbsnews.com/news/former-judge-admits-flaws-with-secret-fisa-court/.

262 § 1803(b).

263 *Id.*

264 *Id.*

265 Klayman v. Obama, 957 F. Supp. 2d 1, 24 (D.D.C 2013); *see* § 1861(f)(2)(A)(i)

> A person receiving a production order may challenge the legality of that order by filing a petition with the pool established by section 1803(e)(1) of this title. Not less than 1 year after the date of the issuance of the production order, the recipient of a production order may challenge the nondisclosure order imposed in connection with such production order by filing a petition to modify or set aside such nondisclosure order, consistent with the requirements of subparagraph (C), with the pool established by section 1803(e)(1) of this title.

Id.

266 *Id.*

267 *Id.* § 1861(f)(2)(C)(i).

> tifies that disclosure may endanger the national security of the United States or interfere with diplomatic relations, such certification shall be treated as conclusive, unless the judge finds that the certification was made in bad faith.[268]

As previously discussed, national security is the overarching goal of the NSA's surveillance program.[269] Due to that, no one has been afforded a viable opportunity to challenge the NSA's actions in court, which is why a neutral party must be allowed to participate in the proceedings.

Given that the NSA and the FISA court operate under a shroud of secrecy, it does not seem that Congress anticipated that ordinary citizens would know about the existence of these production orders.[270] This conclusion is evident because the statutes governing such programs do not allow third party plaintiffs.[271] A neutral lawyer must be granted in the statute to question the government's actions and argue for the rights of the people. Furthermore, a neutral lawyer will counteract the flaws inherent in the statutes. As stalwart as the NSA's mission to protect national security may be, they have made misrepresentations to the FISA court; a neutral lawyer will help keep the NSA in check.[272]

C. Dissuading the Naysayers

There are many who believe that the NSA's surveillance program is beneficial to the nation and who are not concerned about the agency's practices.[273] Differing opinions are important to a healthy democracy.[274] Supporters of the surveillance programs may be persuaded to change their opinion once they realize how the program has been abused.[275] For example, the NSA has admitted that at least a dozen of its employees have abused the surveillance program to spy on their significant others.[276] The broad warrants issued by the FISA court for production of telephony metadata has given the NSA and its employ-

---

268 *Id.* § 1861(f)(2)(C)(ii).

269 *Klayman*, 957 F. Supp. 2d at 40.

270 *Id.* at 21.

271 § 1861(f)(2)(A)(i).

272 In re Production of Tangible Things From [redacted], BR 08-13, 2009 WL 9150913, at * 4 (FISA Ct. 2009).

273 *Government and corporate surveillance draw wide concern*, WASH. POST (Dec. 22, 2013), http://www.washingtonpost.com/page/2010-2019/WashingtonPost/2013/12/21/National-Politics/Polling/release_282.xml.

274 S.W.R. DE A. SAMARASINGHE, SERIES ON DEMOCRACY AND HEALTH: DEMOCRACY AND DEMOCRATIZATION IN DEVELOPING COUNTRIES 22 (1994), *available at* https://www.hsph.harvard.edu/ihsg/publications/pdf/No-7-1.PDF.

275 Alina Selyukh, *NSA Admits Workers Used Spying Tools To Snoop On Exes*, THE HUFFINGTON POST (Sept. 27, 2013, 10:01 AM), http://www.huffingtonpost.com/2013/09/27/nsa-spying-exes_n_4002834.html.

276 *Id.*

ees access to information about virtually any person in the United States.[277] What should be more alarming is what NSA employees do behind closed doors.[278]

Adrienne Kinne, a former analyst at the NSA, exposed the fact that she and her co-workers had been spying on U.S. soldiers' phone calls.[279] During her tenure at NSA, she was listening in on "everyday, average, ordinary Americans who happened to be in the Middle East, in our area of intercept and happened to be making these phone calls on satellite phones."[280] The phone calls were intimate and NSA employees "routinely shared salacious or tantalizing phone calls that had been intercepted, alerting office mates to certain time codes of 'cuts' that were available on each operator's computer."[281] These are but a few of the known abuses that have occurred and should serve as a warning to supporters of the NSA's surveillance practices.

The bulk collection program is doing more harm than good, because "[b]y casting the net so wide and continuing to collect on Americans and aid organizations, it's almost like they're making the haystack bigger and it's harder to find that piece of information that might actually be useful to somebody."[282] Kinne admits that she wasted a significant amount of time listening to innocent Americans, instead of looking for terrorists in the huge net cast by the NSA's surveillance program.[283]

Governments spy on other governments and on their own citizens.[284] As a result, the market for surveillance software has greatly expanded, and the fear that ordinary citizens will have the ability to spy on each other has become a reality.[285] For only ninety dollars, an individual can install software on any phone that is capable of giving them real time images of what the phone user is doing, as well as access to text messages, email, pictures, contacts, and virtually anything on the phone itself.[286] The NSA plays a huge role in the market, because they give scholarships to computer science students that require a "four-year working stint with the NSA, and then [students] left to go out to

---

277 *Id.*

278 *Id.*

279 Brian Ross, *Inside Account of U.S. Eavesdropping on Americans*, ABC NEWS (Oct. 9, 2008), http://abcnews.go.com/Blotter/story?id=5987804&page=1#.UbCL_vaDSlg.

280 *Id.*

281 *Id.*

282 *Id.*

283 *Id.*

284 Morton Halperin, *I Spy, You Spy: Limiting Government Surveillance of Private Citizens*, THE HUFFINGTON POST (May 7, 2014), http://www.huffingtonpost.com/morton-h-halperin/i-spy-you-spy-limiting-government-surveillance_b_5269132.html.

285 *PhoneSheriff*, TOP TEN REVIEWS, http://cell-phone-monitoring-software-review.toptenreviews.com/phonesheriff-review.html (last visited Nov. 17, 2014).

286 *Id.*

California and start private cybersecurity companies in Silicon Valley."[287] Keith Alexander, former NSA director, owns and operates his own private cybersecurity consulting firm, which advises private companies about network security.[288] Although people may have nothing to hide with respect to their government, they should be weary of the NSA's surveillance and the far-reaching consequences of the legislation that supports the agency.[289]

CONCLUSION

The U.S. government is not on a mission to abolish American's privacy rights and turn into a repressive regime.[290] Yet, the fear that they might should not be understated. The executive branch's power has been expanded greatly and "all men having power ought to be distrusted to a certain degree."[291] As the legislative and judicial branches reconcile privacy expectations with modern technology, they should be wary of sacrificing liberty for the sake of a fleeting sense of security.[292] Terrorists are already operating under the assumption that the NSA is doing everything in its power to thwart potential attacks, and they are responding by going dark.[293]

Modern courts seek a proper application of the Fourth Amendment adapted to modern technology.[294] The next step is for the courts to understand that technology is rapidly evolving, and that they must be flexible to find a proper solution. This is about accountability. The Constitution is something 'we the people' placed on the government.[295] On November 18, 2014, legislators had the ability to curtail the NSA's surveillance program.[296] Senator Patrick Leahy's

---

287 Terry Gross, *An In-Depth Look at the U.S. Cyber War, the Military Alliance and its Pitfalls*, WUNC 91.5 (Nov. 17, 2014, 1:25 PM), http://wunc.org/post/depth-look-us-cyber-war-military-alliance-and-its-pitfalls.

288 *Id.*

289 *Id.*

290 *See* Ross, *supra* note 279 ("It's not for the heck of it. We are narrowly focused and drilled on protecting the nation against al Qaeda and those organizations affiliated with it.").

291 James Madison, Debate at the Constitutional Convention (July 11, 1787) (transcript available at Yale Law School Lillian Goldman Law Library).

292 *See* Pa. Assembly, Reply to the Governor of Pennsylvania (Nov. 11, 1755), *in* THE PAPERS OF BENJAMIN FRANKLIN APRIL 1, 1755, THROUGH SEPTEMBER 30, 1756, at 238-43 (Leonard W. Labaree ed., Yale Univ. Press, 1963), *available at* http://founders.archives.gov/documents/Franklin/01%C2%AD06%C2%AD02%C2%AD0107 ("Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety.").

293 Richard Clarke, *Why You Should Worry About the NSA*, N.Y. DAILY NEWS (June 12, 2013, 4:15 AM), http://www.nydailynews.com/opinion/worry-nsa-article-1.1369705.

294 Klayman v. Obama, 957 F. Supp. 2d 1, 43 (D.D.C 2013).

295 U.S. CONST. pmbl.

296 Ben Kamisar, *Leahy Blasts Criticism of NSA Reform Bill*, THE HILL (Nov. 18, 2014,

bill to limit the NSA's telephony metadata collection program was up for a vote, which needed sixty votes to pass.[297] It was the hope of the American people that our government will respond to the encroachment it has allowed thus far. Unfortunately, Leahy's USA FREEDOM Act of 2014 fell short of the sixty votes needed to pass.[298] The votes were divided among party lines, with the exception of a few votes on each side.[299] Most view the outcome as a major loss for privacy advocates, because the Patriot Act has not been curtailed in any way.[300] However, the rejection of the USA FREEDOM Act has the potential of being a major win for privacy advocates.

Leahy's proposed Act, among other things, would have limited the breadth of the Patriot Act by changing definitions, time limits, targets, and requiring an appointment of special advocates to question any certification or application for an order.[301] For the proposal to gain support in the Senate from proponents of intelligence gathering, the proposed Act would have amended the Patriot Act's sunset provisions for section 215, which are set to expire on June 1, 2015, and extended that date to December 31, 2017.[302] The good news for privacy advocates is that section 215 will, unless Congress votes otherwise, expire in the summer of 2015.[303] Moreover, Leahy's proposed Act would have been a patch on legislation that has tremendous amounts of faults, which can only be solved by tearing it apart and starting from scratch. The bad news for privacy advocates is that the majority of the newly elected Congress supports the Patriot Act and section 215.[304]

The months leading up to the summer of 2015 will be a crucial time for privacy advocates and policy makers. Having the power and capability to intercept mass amounts of data for intelligence gathering purposes, does not give our government the right to impinge on our civil liberties. That is not to say that intelligence gathering is unimportant. Simply that it should coincide with the fundamental rights we have as American citizens. If our government fails to do so, then more people will begin to operate in the dark and open the

---

1:48 PM), http://thehill.com/policy/technology/224540-leahy-blasts-late-criticism-of-nsa-reform-bill.

297 *Id.*

298 Burgess Evertt, *Republican Wall Crushes NSA Bill*, POLITICO (Nov. 19, 2014, 12:06 AM), http://www.politico.com/story/2014/11/mitch-mcconnell-rand-paul-nsa-bill-112984.html.

299 *Id.*

300 *Id.*

301 USA FREEDOM Act, S. 2685, 113th Cong. § 401.

302 *Id.* § 701.

303 *Id.*

304 Julian Hattem, *McConnell: NSA reform would help ISIS*, THE HILL, (Nov. 18, 2014, 10:41 AM), http://thehill.com/policy/technology/224505-mcconnell-nsa-reform-would-help-isis.

floodgates to unforeseen and unprecedented problems.[305] As was the case with Tor, this is not the first time that a government sponsored program backfires.[306]

[305] Clarke, *supra* note 293.
[306] Peterson, *supra* note 17.