Santa Clara University School of Law

Santa Clara Journal of International Law

Volume 15 | Issue 1 Article 4

2-4-2017

The Digital Underworld: Combating Crime on the Dark Web in the Modern Era

Sophia Dastagir Vogt

15 *SANTA CLARA JOURNAL OF INTERNATIONAL LAW* 104 (2017)

The Digital Underworld: Combating Crime on the Dark Web in the Modern Era

Sophia Dastagir Vogt*

Abstract:

* Sophia Dastagir Vogt is a California-licensed attorney currently working for the United States Senate in Washington, D.C. where she specializes in criminal procedure, technology and privacy law. Vogt is originally from Santa Cruz, California and holds a B.A. in International Relations from the University of San Diego (2009), and her J.D from the Santa Clara University School of Law (2016).

More and more individuals are turning toward encrypted methods of Internet communication in order to keep their online activities private. As a result of this trend, the government is facing serious difficulties in combating crimes such as online child trafficking on the dark web due to its highly encrypted design. While it is my conclusion in this paper that under the third party doctrine, an individual has no heightened expectation of privacy when using the dark web, it is my belief that the third party doctrine must be revisited in order to reflect evolving expectations of privacy, conflicts of law, and the realities of modern day Internet usage. It is my goal in this paper to analyze the issue through the increasingly complex and rapidly evolving labyrinth of domestic and international privacy law.

I. INTRODUCTION

In 2013, the dark web gained particular notoriety when the media reported the FBI's takedown of Ross Ulbricht, the kingpin behind the infamous Silk Road black marketplace.[1] Ulbricht's capture sent a chill across the online community, leaving many questioning how law enforcement was able to track Ulbricht's identity on the highly encrypted dark web. Most importantly, Ulbricht's capture served as a reminder that there is no reasonable expectation of privacy online, regardless of how deep one may go on the Internet.

The dark web has been both lauded for its accomplishments in facilitating democratic ideals, and criticized for enabling criminals to conduct illegal activity beyond the reach of the law. Following the Snowden leaks[2] in 2013, many have turned to the dark web to encrypt online identity and defend privacy for both legal and illegal means. With the public advocating for encryption and more robust privacy laws, law enforcement is now facing a serious threat in combating crime.[3]

The purpose of this paper is to analyze the concept of privacy on the dark web, and evaluate whether dark web users have an expectation of privacy in their encrypted activity in light of law enforcement's interest in tracking and identifying criminals involved in cross-border crime. It is my position that an individual who voluntarily shares information on the Internet, whether on the dark or surface web, can only assert a limited expectation of privacy, if at all, in such activity. Dark web users conduct their activity in a public forum. Therefore, strong encryption does little to establish a reasonable expectation of privacy on balance with law enforcement's strong interest in combating crime.

First, this paper will introduce various international approaches to privacy as a human right. Second, it will provide an overview of the differing layers of the Internet. Third, it will examine the U.S. legal framework surrounding online privacy in both the domestic and international arenas, and introduce the methods the U.S. government has adopted to unveil the identity of dark web users. Fourth, it will determine whether individuals have an expectation of privacy in activity on the dark web. Finally, it will analyze the jurisdictional obstacles facing law enforcement's ability to execute criminal investigations while respecting different approaches to data privacy in a globalized world.

II. PRIVACY AS A FUNDAMENTAL RIGHT

1. Vincenzo Ciancaglini et al., *Below the Surface: Exploring the Deep Web*, TREND MICRO (2015), http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_below_the_surface.pdf (last visited Dec. 8, 2016).
2. In 2013, Edward Snowden, a former contractor for the CIA, leaked to the media, details of mass Internet and phone surveillance by the U.S. National Security Agency (NSA). The controversial program, code named PRISM, began in 2007 and involved participation by several technology companies such as Yahoo!, Google, and Microsoft.
3. Natasha Bertrand, *ISIS is Taking Full Advantage of the Darkest Corners of the Internet*, BUSINESS INSIDER (Jul. 11, 2015, 11:26 AM), *available at* http://www.businessinsider.com/isis-is-using-the-dark-web-2015-7.

The concept of privacy is rooted in some of the world's oldest texts and cultures.[4] Its definition, however, can vary dramatically from culture to culture.[5] Societies made up of large communities living in close contact with one another often assume a lower expectation of privacy, whereas more separated, individualized cultures assume a higher expectation of privacy that values autonomy and space.[6] World bodies, organizations, and individuals have grappled with the concept and definition of privacy, associating it with an individual's ability to choose the manner and circumstances under which one may expose his feelings and behavior to others, to the essence of human personality.[7] Such ideals are meant to guard individuality, autonomy, dignity, emotional release, self-evaluation, and interpersonal relationships.[8]

In several parts of the world, privacy has developed within the context of human rights.[9] In 1948, the General Assembly of the United Nations adopted the Universal Declaration of Human Rights.[10] Article 12 of the Universal Declaration of Human Rights explicitly announced: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks."[11] Similarly set forth in 1948, the Organization of American States adopted the American Declaration of the Rights and Duties of Man, providing that, "[e]very person has the right to the protection of the law against abusive attacks upon . . . his private and family life."[12] In 1950, the Council of Europe introduced the European Convention for the Protection of Human Rights and Fundamental Freedoms, which sought to formalize the goals of the Universal Declaration of Human Rights by rule of law.[13] The Convention states that, "[e]veryone has the right to respect for his private and family life, his home and his correspondence."[14]

4. PETER SWIRE & KENESA AHMAD, FOUNDATIONS OF INFORMATION PRIVACY AND DATA PRIVACY: A SURVEY OF GLOBAL CONCEPTS, LAWS AND PRACTICES 1, 2 (2012) [hereinafter SWIRE & AHMAD, FOUNDATIONS] ("Privacy is referenced numerous times in the laws of classical Greece and in the Bible. The concept of the freedom from being watched has historically been recognized by Jewish law. Privacy is similarly recognized in the Qur'an and in the sayings of Mohammed where there is discussion of the privacy of prayer as well as in the avoidance of spying or taking ill of something behind their back.").
5. Jeremy Fogel, *From the Bench: A Reasonable Expectation of Privacy*, THE AMERICAN BAR ASSOCIATION LITIGATION JOURNAL (Spring 2014), http://www.americanbar.org/publications/litigation_journal/2013-14/spring/a_reasonable_expectation_privacy.html (last visited Dec. 8, 2016). (Legal recognition of privacy has existed in England since 1361).
6. *Id.*
7. SWIRE & AHMAD, FOUNDATIONS, *supra* note 4, at 1.
8. *Id.*
9. *Id.* at 3.
10. *Id.*
11. Universal Declaration of Human Rights, G.A. Res. 217 (III) A, U.N. Doc. A/RES/217(III) (Dec. 10, 1948).
12. SWIRE & AHMAD, FOUNDATIONS, *supra* note 4, at 3.
13. *Id.*
14. *Id.*

In the United States, privacy has focused on the right to privacy of one's person.[15] Unlike the E.U., the U.S. Constitution does not provide a "right" to privacy, whereas European legal texts define privacy as a human right.[16] Furthermore, the U.S. has no single, overarching privacy law.[17] Instead, it follows a sectoral approach that imposes federal regulations on specific industries, such as healthcare and consumer credit reporting, while leaving others unprotected.[18] Beyond these limited federal privacy restrictions, Congress has left stricter privacy legislation to the states.[19]

In contrast with the U.S., the European Union employs a comprehensive model to privacy regulation, setting forth an overarching legal structure to protect the fundamental rights and freedoms of E.U. citizens.[20] Data privacy laws in the E.U. are far stricter than those in the U.S., producing both benefits and drawbacks. For example, in March 2015, Germany suffered the blowback of a strict privacy regime when Germanwings co-pilot Andreas Lubitz crashed a commercial airplane into the French Alps, killing everyone on board.[21] Germany's vigorous approach to privacy protection enabled Lubitz to hide a serious mental illness from his employer and commit mass murder.[22] This event, among other recent attacks, has raised concerns that European privacy laws are too strict and has ignited a debate regarding whether European privacy laws are too robust on balance with protecting public safety.[23]

In Australia, which uses a co-regulatory model, individuals do not have absolute rights under Australian law, but rather the focus is on "reasonableness" to reflect adequate privacy protection while also facilitating business.[24] At the other end of the spectrum, the People's Republic of China does not have a comprehensive privacy law.[25]

III. THE DIVIDED INTERNET

15. Fogel, *supra* note 5 ("When he famously described "the right to be let alone" as "the most comprehensive of rights and the right most valued by civilized men," . . . Justice Brandeis was channeling a sentiment that is embedded deeply in both our common law and our society.").
16. SWIRE & AHMAD, FOUNDATIONS, *supra* note 4, at 41.
17. Daniel Dimov, *Differences Between the Privacy Laws in the EU and the US*, INFOSEC INSTITUTE (Jan. 10, 2013), http://resources.infosecinstitute.com/differences-privacy-laws-in-eu-and-us/.
18. *Id.*
19. *Id.*
20. SWIRE & AHMAD, FOUNDATIONS, *supra* note 4, at 34.
21. Simon Shuster, *German Privacy Laws Let Pilot 'Hide' His Illness From Employers*, TIME (Mar. 27, 2015), *available at* http://time.com/3761895/germanwings-privacy-law/.
22. *Id.*
23. *See id.* ("[A]s a rule, when the German legal system is compared to those in the U.S. and other European states, Germany gives more weight to personal privacy than to public safety . . . [e]mployers are even restricted in checking the criminal records of the people they are seeking to hire, as under German law, the employer must usually rely on the applicants themselves to provide such information voluntarily.").
24. SWIRE & AHMAD, FOUNDATIONS, *supra* note 4, at 45. *See also* ALBERT J, MARCELLA JR. & CAROL STUCKI, PRIVACY HANDBOOK: GUIDELINES, EXPOSURES, POLICY IMPLEMENTATION, AND INTERNATIONAL ISSUES 72 (2003) (under the co-regulatory approach, "industry develops rules for the protection of privacy, which are enforced by the industry and overseen by the privacy agency.").
25. SWIRE & AHMAD, FOUNDATIONS, *supra* note 4, at 45.

The Internet is a network that links websites through the World Wide Web (Web).[26] The Web is divided into different components.[27]

The surface web, which most are familiar with, enables users to access indexed pages through a web browser. Through typing words into a browser's search box, the browser, "sends 'spiders' to index[ed] hyperlinks to static web pages," thereby returning the desired results.[28] While this method of searching is most convenient for the majority of Internet users, "[i]t is estimated that even the best search engines can access only 16 percent of information available on the web."[29]

In contrast to the surface web, the deep web refers to the portion of the Internet that cannot be, or is not indexed through traditional search engines.[30] Most of the content on the Internet is located on the deep web, outside the reach of traditional web browsers.[31] Because material on the deep web is not indexed, one must have the precise URL to access the desired page. Although the deep web may be difficult to navigate, roughly 95 percent of it consists of publicly accessible information.[32]

Within the deep web exists a hidden space called the dark web, which is inaccessible through standard web browsing methods.[33] This hidden space is popularly known as a platform for hosting illicit activity, ranging from terrorist recruitment to drug trading, child pornography, stolen information, and money laundering services.[34] These hidden domains trade in cryptocurrency, or "bitcoins," an unregulated online currency, to maximize anonymity.[35] Most dark web sites use the special anonymity software TOR (The Onion Router), which encrypts user identity by bundling incoming data into encrypted packets, anonymizing information about the sender by stripping away part of its packet header, encrypting the remainder of the address information, and sending the encrypted data packet through several servers, called relays, en route to its final destination.[36] In effect, this prevents others from identifying the user's origin with its destination.[37]

TOR was developed from funding by the Naval Research Laboratory in the 1990s as a tool for evading online detection.[38] It receives roughly 60 percent of its funding through the State Department and

26. Abdulmajeed Alhogbani, *Going Dark: Scratching the Surface of Government Surveillance*, 23 COMMLAW CONSPECTUS 469, 480 (2015).
27. *Id.*
28. *Id.*
29. *Id.* at 480.
30. Ciancaglini et al., *supra* note 1, at 5.
31. Alhogbani, *supra* note 26, at 481.
32. *Id.* at 482.
33. *Id.*
34. *Id.*
35. *Id.*
36. Jill Scharr, *What is Tor? Answers to Frequently Asked Questions*, TOM'S GUIDE (Oct. 23, 2013, 7:00 AM), http://www.tomsguide.com/us/what-is-tor-faq,news-17754.html.
37. Andy Greenberg, *Hacker Lexicon: What is the Dark Web?,* WIRED (Nov. 19, 2014), http://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/.
38. David Perera, *Foundation of 'dark Web' steps into the light*, POLITICO (Oct. 21, 2015, 4:52 PM), http://www.politico.com/story/2015/10/foundation-of-dark-web-steps-into-the-light-215027.

the Department of Defense, both of whom share an interest in developing a secure network for government agencies and promoting an open Internet.[39]

IV. COMBATING INTERNATIONAL CRIME ON THE DARK WEB

International crime rings span across several jurisdictions, all of which offer different degrees of privacy protection. Within the U.S., the Fourth Amendment governs searches and seizures and protects U.S persons from unreasonable government intrusion. Beyond the U.S., law enforcement is held to a more flexible standard, and any international law forbidding sovereigns from infringing on another's data privacy laws may prove ineffective from an enforcement standpoint.[40]

A. U.S. Legal Framework

1. ***The Fourth Amendment***

The Fourth Amendment safeguards against the unreasonable search and seizure, by any government actor, of one's person or one's property by requiring that a warrant based upon probable cause be issued by a neutral magistrate. "A 'search' occurs 'when an expectation of privacy that society . . . consider[s] reasonable is infringed.'"[41] A property-based approach to the Fourth Amendment makes clear that certain areas, such as an individual's home, are awarded the utmost privacy protection.[42] Warrantless intrusion into one's home is fiercely guarded under the Fourth Amendment, while other areas are left less protected.[43] Technology has further complicated the concept of privacy under the Fourth Amendment given the inability of the law to keep up with and protect evolving societal expectations of privacy. For many, smartphones and laptops now store some of the most intimate details of our lives.[44]

---

39. David Kushner, *The Darknet: Is the Government Destroying 'the Wild West of the Internet'*, ROLLING STONE (Oct. 22, 2015), *available at* http://www.rollingstone.com/politics/news/the-battle-for-the-dark-net-20151022.
40. *See* ELENA KATSELLI PROUKAKI, THE PROBLEM OF ENFORCEMENT IN INTERNATIONAL LAW: COUNTERMEASURES, THE NON-INJURED STATE AND THE IDEA OF INTERNATIONAL COMMUNITY (2011), *available at* https://books.google.com/books?id=1rSNA-gAAQBAJ&pg=PT461&lpg=PT461&dq=international+law+meaningless&source=bl&ots=sKN0I8c0UA&sig=3vdEUyDrxU6ch2I4nDOR-BEtgxk0&hl=en&sa=X&ved=0CDQQ6AEwBGoVChMIxsK8_6vayAIVU81jCh0h1AvW#v=onepage&q=meaningless&f=false ("Due to the decentralized character of the international legal order and in the absence of institutions empowered to enforce international law generally, implementation, through the application of countermeasures, is entrusted to each state individually which is called, by its own means, to protect its rights.").
41. United States v. Karo, 468 U.S. 705, 712 (1984).
42. Kyllo v. U.S., 533 U.S. 27, 31 (2001).
43. *See* Oliver v. U.S., 466 U.S. 170, 176 (1984) (government intrusion into "open fields" not unreasonable under the Fourth Amendment).
44. *See* Riley v. California, 134 S. Ct. 2473, 2490 (2014) ("Today . . . it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate.").

In 1967, the Supreme Court extended the Fourth Amendment to protect intangible interests, such as privacy, for the first time.[45] In *Katz v. United States*, the Court declared that, "[t]he Fourth Amendment protects people, not places,"[46] when it held that the unwarranted wiretapping of a citizen's conversation in a public phone booth was an unconstitutional search and seizure under the Fourth Amendment.[47] *Katz*, however, limited Fourth Amendment protection to activity in which an individual can establish a *subjective* expectation of privacy that is *objectively* reasonable.[48] While *Katz* extended Fourth Amendment protection to that which an individual takes measures to keep private, it expressly excluded from protection activities one "knowingly exposes to the public."[49] These "objects, activities, or statements . . . [one] exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to [one's self] has been exhibited."[50]

Though *Katz* expanded protection to certain privacy matters outside the home, it left several questions unanswered, such as how, if at all, the analysis may change depending on the purpose of the invasion (i.e., foreign intelligence, national security, criminal investigations), the legal status of those subject to the interception (i.e., U.S. versus non-U.S. persons), or the location of the search or seizure (i.e., whether the interception took place strictly within the U.S., between the U.S. and a foreign territory, or exclusively abroad).[51]

2. ***The Third Party Doctrine***

In the aftermath of *Katz*, the Court developed the third party doctrine, which states, "that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[52] The Supreme Court has generally held that where an individual makes information available to a third party, the government may obtain the information without a warrant, regardless of whether the act includes subjectively reasonable private behavior.[53] In essence, unless an activity is kept entirely within the access and control of one individual, it is regarded as having been exposed to the public under the law. The third party doctrine has long been a source of significant debate among privacy advocates given its breadth and outdated reasoning. The Supreme Court has not directly clarified how,

45. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).
46. *Id.* at 351.
47. *Id.* at 358.
48. *Id.* at 351-352 ("what [an individual] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.").
49. *Id.* at 351 ("[w]hat a person knowingly exposes to the public, even in his own home or office, is not subject to Fourth Amendment protection.").
50. *Id.* at 361.
51. Laura Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117, 206 (2015).
52. Smith v. Maryland, 442 U.S. 735, 743-44 (1979) (no expectation of privacy in phone numbers dialed). *See also* United States v. Miller, 425 U.S. 435, 442 (1976) (no expectation of privacy in information voluntarily conveyed to banks).
53. Marley Degner, *Riley and the Third Party Doctrine*, PILLSBURY WINTHROP SHAW PITTMAN LLP (Apr. 9, 2015), http://www.pillsburylaw.com/siteFiles/Publications/AR_Riley_and_the_thirdparty_doctrine_Degner_4915.pdf.

and to what extent, the third party doctrine applies to the Internet, and lower courts are in disagreement.[54]

In an attempt to limit the scope of the doctrine, Congress passed in 1986, the Electronic Communications Privacy Act (ECPA), and its counterpart, the Stored Communications Act (SCA). With both pieces of legislation, Congress intended to establish clearer standards surrounding Fourth Amendment searches in light of evolving technology. It is important to note that ECPA was written before the Internet became widely used by the public—well before many moved their personal identities online, and well before cloud computing.[55] While Congress failed to draft these statutes to allow for adequate privacy protection on evolving technology, both statutes have at least served to limit the expansiveness of the third party doctrine to some effect.

Currently, the third party doctrine applies equally to both surface web and dark web activity.

3. ***The Fourth Amendment Beyond U.S. Borders***

The text of the Fourth Amendment extends only to "the people."[56] Construed in light of the Constitution as a whole, "'the people' . . . refers to a class of persons who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community."[57]

In *United States v. Verdugo-Urquidez*, the Court examined whether the Fourth Amendment applies to the search and seizure by U.S. agents of property located in a foreign country owned by a non-resident alien.[58] There, the Court held that a non-resident alien with no voluntary attachment to the U.S., whose property subject to the search was located outside the United States, did not have protection under the Fourth Amendment because he lacked "substantial connection" with the United States.[59] The Court found that, "the purpose of the Fourth Amendment was to protect the people of the United States against arbitrary action by their own Government" rather than, "to restrain the actions of the Federal Government against aliens outside the United States territory."[60]

---

54. *Id*. *See, e.g.,* United States v. Warshak, 631 F.3d 266, 286 (2010) ("the mere ability of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy").
55. *Under My Thumb: Governments Grapple With Law Enforcement in the Virtual World*, THE ECONOMIST (Oct. 10, 2015), *available at* http://www.economist.com/news/international/21672204-governments-grapple-law-enforcement-virtual-world-under-my-thumb?frsc=dg%7Cc [hereinafter *Under My Thumb*].
56. United States v. Verdugo-Urquidez, 494 U.S. 259, 265 (1990).
57. *Id.*
58. *Id*. at 262.
59. *Id*. at 271-275 ("For better or for worse, we live in a world of nation-states in which our Government must be able to 'functio[n] effectively in the company of sovereign nations.' [citation]. Some who violate our laws may live outside our borders under a regime quite different from that which obtains in this country. Situations threatening to important American interests may arise half-way around the globe, situations which in the view of the political branches of our Government require an American response with armed force. If there are to be restrictions on searches and seizures which occur incident to such American action, they must be imposed by the political branches through diplomatic understanding, treaty, or legislation.").
60. *Id*. at 266.

Several questions remain unanswered in the aftermath of *Verdugo-Urquidez* with respect to the meaning of "lawful presence" in the U.S. in the digital age, where information by both U.S. citizens and foreigners are stored in servers around the world.[61] Of particular importance are the following issues: whether online contacts with the United States, such as storing files on U.S.-based servers, become relevant for Fourth Amendment protection; whether the Fourth Amendment limits evidence obtained when law enforcement mistakenly believes an individual lacks Fourth Amendment rights, or their status is unknown; and finally, how the Fourth Amendment affects communications between individuals protected by the Fourth Amendment, and those lacking such rights.[62]

With regard to U.S. citizens searched extraterritorially, three circuit courts have considered the question of Fourth Amendment application beyond U.S. borders.[63] The Ninth Circuit approach to Fourth Amendment reasonableness requires the U.S. government to cooperate with foreign authorities to comply with foreign law in the jurisdiction of the search when conducting a search or seizure abroad.[64] The Second and Seventh Circuits have held that Fourth Amendment reasonableness pursuant to an extraterritorial search, where the U.S. is acting alone or through a joint investigation with a foreign sovereign, does not require a warrant but rather an evaluation of the government need on balance with the privacy interest at stake.[65]

4. ***National Security Exceptions***

Under *Katz*, the Fourth Amendment protects U.S. citizens from warrantless eavesdropping by the government,[66] unless the need falls within an exception to the warrant requirement, such as national security.

The Foreign Intelligence Surveillance Act (FISA) has defined the contours of the warrant clause of the Fourth Amendment regarding electronic interceptions on U.S. soil.[67] "FISA is the primary vehicle allowing the government to conduct covert surveillance of those suspected of terrorist activities in the United States," and allows "for electronic surveillance of communications between or among foreign powers," without a court order, in some circumstances.[68] Where a court order is required, the Foreign Intelligence Surveillance Court (FISC), a special court for FISA applications, may approve FISA applications "notwithstanding any other law."[69] Not only does FISC approve a wide majority of FISA applications, the process remains classified, and therefore largely unchecked due to the sensitive nature of national security.[70]

---

61. *See* Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285, 302.
62. *Id.* at 303.
63. *Id.* at 297.
64. *Id.*
65. *Id.*
66. *Katz*, 389 U.S. at 354.
67. Donohue, *supra* note 51.
68. Rebecca Copeland, *War On Terrorism or War on Constitutional Rights? Blurring the Lines of Intelligence Gathering in Post-September 11 America*, 35 TEX. TECH L. REV. 1, 2-3 (2004).
69. *Id.*at 3.
70. *See id.* at 15.

Section 702 of FISA allows for broad monitoring of Internet activity by non-U.S. persons believed to be located outside the United States.[71] However, purely domestic communications are often routed through extraterritorial servers without an individual's knowledge, subjecting them to collection pursuant to FISA. Given that data may cross borders several times in a single communication, Section 702 provides law enforcement with an avenue to collect information on U.S. citizens within the contours of the law. Beyond Section 702, several courts, including the FISC, have relied on the third party doctrine to uphold data surveillance of U.S. citizens in the name of national security.[72]

5. ***Current Methods for Catching Criminals on the Dark Web***

With the rising popularity of encryption, law enforcement is increasingly facing difficulties in conducting criminal investigations. Consumers are demanding more privacy, and are turning to technology that offers more security and anonymity. While privacy rights continue to evolve as technology advances, it is critical to note that the Fourth Amendment merely requires that searches and seizures be reasonable.

a. Memex

While special browsers such as TOR provide strong anonymity protection to dark web users, law enforcement has been fighting back within the ambits of the law.[73] The U.S. Defense Advanced Research Projects Agency (DARPA) has developed a search engine called Memex to help the Department of Defense fight human trafficking and potentially help uncover other illegal activity on the dark web.[74] In essence, Memex is scraping and indexing millions of web pages that cannot be accessed through traditional search engines, including thousands of sites featured on dark web browsers such as TOR.[75] While Memex does not unmask the IP addresses or identities of dark web users, it analyzes content to uncover patterns and relationships, which law enforcement has been able to track and trace back to the user.[76] Although much of the content Memex is designed to index is not accessible through a commercial search engine, the information is nevertheless still considered "public".[77] DARPA contends

71. *See* 50 U.S.C. § 1881a (2015).
72. RICHARD THOMPSON II, CONG. RESEARCH SERV., R43586, THE FOURTH AMENDMENT THIRD-PARTY DOCTRINE 1, 3 (2014).
73. *See* Charlie Osborn, *UK Gov't Tackles Dark Web With New Cybercrime Unit*, ZDNET (Nov. 9, 2015, 2:19 PST), http://www.zdnet.com/article/uk-govt-tackles-dark-web-with-new-cybercrime-unit/ (the U.K. has similarly begun to wage a war, and has designated an entire unit to fighting cybercrime on the dark web).
74. Anthony Cuthbertson, *Death of the Dark Web? DARPA's Memex Search Engine Allows Tor Tracking*, INTERNATIONAL BUSINESS TIMES (Feb. 16, 2015, 1:38 GMT), *available at* http://www.ibtimes.co.uk/death-dark-web-darpas-memex-search-engine-allows-tor-tracking-1488124.
75. *Id.*
76. *Id.*
77. Kim Zetter, *DARPA is Developing A Search Engine for the Dark Web*, WIRED (Feb. 10, 2015, 10:17 AM), http://www.wired.com/2015/02/darpa-memex-dark-web.

that its objective with Memex is not to de-anonymize the dark web, but rather to fight human trafficking.[78]

b. Network Investigative Techniques

In a 2012 investigation titled "Operation Torpedo," the FBI utilized a method called NIT, or a "network investigative technique," to unveil the IP addresses of at least twenty-five individuals who visited child pornography websites on the dark web.[79] Beginning with an investigation in the Netherlands, authorities from the Netherlands' national police force were able to write a web crawler that searched the dark web for TOR websites.[80] The authorities were able to narrow the websites to those related to child pornography, and eventually unveil the real IP address of one site called "Pedoboard," in Bellevue, Nebraska.[81] Upon being delivered the information, the FBI was able to track the address to Aaron McGrath, who was hosting three child porn sites.[82] After one year of surveillance, the FBI seized McGrath's servers and searched each server pursuant to a valid warrant.[83] As authorized by the warrant, the FBI modified the code on the servers to deliver the NIT to computers that accessed the illegal sites, allowing for delayed notification to the targets for thirty days.[84] Within two weeks, the FBI was able to collect the IP addresses of visitors to the sites and subpoena the ISPs for the home addresses and subscriber names of each subject.[85]

Recent litigation stemming from a similar dark web investigation has called the technique into question.[86] In a 2015 investigation involving a child pornography website named "Playpen," defendants have been challenging the government's use of the technique by arguing that the magistrate judge, located in the Eastern District of Virginia, had no authority under Federal Rule of Criminal Procedure 41(b)(1)[87] to issue the warrant authorizing a search beyond the Eastern District of Virginia.[88] Although courts have generally agreed that the magistrate judge lacked authority to issue the warrant

78. Cuthbertson, *supra* note 74.
79. Kevin Poulsen, *Visit the Wrong Website, and the FBI Could End Up In Your Computer*, WIRED (Aug. 5, 2014, 6:30 AM), http://www.wired.com/2014/08/operation_torpedo/.
80. *Id.*
81. *Id.*
82. *Id.*
83. *Id.*
84. *Id.*
85. Poulsen, *supra* note 79.
86. *See* United States v. Levin, No. 15-10271-WGY, 2016 WL 2596010 (D. Mass. May 5, 2016); United States v. Epich, No. 15-CR-163-PP, 2016 WL 953269 (E.D. Wis. Mar. 14, 2016); United States v. Michaud, No. 3:15-cr-05351-RJB, 2016 WL 337263 (W.D. Wash. Jan 28, 2016).
87. Rule 41(b)(1) grants a magistrate judge the authority to issue a warrant to search for and seize a person or property located within their district. As of December 1, 2016, Federal Rule of Criminal Procedure 41 has been amended to grant magistrate judges the authority to issue a warrant beyond their district where the suspect has either used technological means to mask the location of his or her computer, or where the crime involves the hacking of computers located across five or more different judicial districts.
88. United States v. Gabriel Werdene, No. 15-434, 2016 WL 3002376 (E.D. Pa. May 18, 2016).

under Rule 41, they have disagreed as to whether suppression is the appropriate remedy.[89] Notwithstanding a Rule 41 challenge, several courts have recently found that an individual has no reasonable expectation of privacy in his or her IP address,[90] thereby eradicating the need for a warrant given that the technique does not involve a search under the Fourth Amendment.[91]

c. Traditional Techniques

Despite Constitutional limitations, law enforcement is free to conduct investigations the old-fashioned way—traditional tactics such as infiltrating criminal rings through undercover operations and tracking individuals in public places remain fair game.

In November 2014, law enforcement agents successfully coordinated Operation Onymous, leading to the seizure of dozens of TOR hidden services.[92] While it remains unknown how law enforcement captured the sites, security researchers speculate that government hackers may have used "denial of service" attacks, which "flood Tor relays with junk data to force target sites to use Tor relays they controlled, thus tracing their IP addresses."[93] It is likewise entirely possible that law enforcement used traditional means, such as informants or undercover operations, to effectuate the takedown.

In the case of the Silk Road, law enforcement claims that Ross Ulbricht's own mistakes led to his capture, and that no illegal acts or sophisticated methods of intrusion were necessary to take down the drug kingpin.[94] Former FBI agent Christopher Tarbell contends that he and another agent merely found a misconfiguration on the Silk Road's login page, which divulged the server's IP address, and its physical location.[95] Police in Reykjavik, Iceland, where the server was located, then "accessed and secretly copied the server's data."[96] Ulbricht maintains that law enforcement illegally hacked the server

89. *Compare Michaud*, 2016 WL 337263, at 6-7 (finding there was a violation of Rule 41(b) but that suppression is inappropriate because the government acted in good faith and the defendant was not prejudiced), *Werdene*, 2016 WL 3002376 (finding a violation of Rule 41(b)(1) but denying suppression because Tor users have no reasonable expectation of privacy in their IP addresses while using Tor, therefore there was no Fourth Amendment violation), and *Epich*, 2016 WL 953269, at 2 (holding Rule 41 was not violated and that suppression would be inappropriate even if it was), *with Levin*, 2016 WL 2596010, at 7-15 (finding suppression appropriate).

90. *See* United States v. Farrell, 2016 WL 705197, at 1 (W.D. Wash. Feb. 23, 2016); United States v. Matish, 2016 WL 3545776 (E.D. Va. Jul. 28, 2017), at 20-21; *Werdene*, 2016 WL 3002376; *Michaud*, 2016 WL 337263, at 7.

91. *Matish*, 2016 WL 3545776, at 23.

92. Greenberg, *supra* note 37.

93. *Id*.

94. Andy Greenberg, *The FBI Finally Says How it 'Legally" Pinpointed Silk Road's Server*, WIRED (Sep. 5, 2014, 7:22 PM), http://www.wired.com/2014/09/the-fbi-finally-says-how-it-legally-pinpointed-silk-roads-server/.

95. *Id*. ("As they typed 'miscellaneous' strings of characters into the login page's entry fields, Tarbell writes that they noticed an IP address associated with some data returned by the site didn't match any known Tor 'nodes,' the computers that bounce information through Tor's anonymity network to obscure its true source. And when they entered that IP address directly into a browser, the Silk Road's CAPTCHA prompt appeared, the garbled-letter image designed to prevent spam bots from entering the site. . . . 'This indicated that the Subject IP Address was the IP address of the SR Server,' . . . 'and that it was "leaking" from the SR Server because the computer code underlying the login interface was not properly configured at the time to work on Tor.").

96. *Id*.

in violation of the Computer Fraud and Abuse Act (CFAA)[97], and that all evidence obtained following the alleged illegal search should be suppressed as fruit of the poisonous tree.[98] Prosecutors were careful not to concede, and countered that any hypothetical "hacking" of the Silk Road server would nevertheless be legal because the foreign location of the server, in conjunction with the Silk Road's reputation as a criminal marketplace, means that Fourth Amendment protection against unreasonable searches does not apply.[99] Moreover, the CFAA, which prohibits unlawful "hacking," contains an express exception for lawfully authorized law enforcement activity, provided it is reasonable.[100]

V. THE EXPECTATION OF PRIVACY ON THE DARK WEB

Changing expectations of privacy online, and the complexity of Fourth Amendment application to international crime on the Internet can make it unclear whether dark web users have any legitimate expectation of privacy in using encryption technology, or whether the analysis is identical to Internet use on the surface web, where third party doctrine and national security exceptions govern.

A. Katz Reasonable Expectation of Privacy Test

Under *Katz*, we must first determine whether dark web users have a subjective expectation that their activity will be kept private. Individuals use services such as TOR for the specific purpose of keeping their online identity and activity a secret, as TOR's design encrypts activity several times over. Based on TOR's design, it is clear that dark web users subjectively believe their activity will remain anonymous, as that is the purpose of the dark web.

With a clear subjective expectation of privacy, we must next determine whether that expectation is objectively reasonable.[101] The third party doctrine, in its current form, makes very clear that it is objectively *unreasonable* for individuals to purport a reasonable expectation of privacy regarding online activity, regardless of whether that activity occurs on the surface web, or on an encrypted

97. Enacted by Congress in 1986, CFAA aims to reduce the instances of computer offenses by criminalizing individuals who intentionally access a computer without authorization.

98. United States v. Ulbricht, 2014 U.S. Dist. LEXIS 145553, *7 (2014). *See also* Gov't Resp. to the Decl. of Josh Horowitz 7, https://archive.org/stream/pdfy-bxSbsz636MwNIwsr/242138723-Prosecution-Response-to-Horowitz-Declaration_djvu.txt (last visited Dec. 10, 2016). *See also* U.S. v. Figueredo-Diaz, 718 F.3d 568, 574 (2013) ("fruit of the poisonous tree," a doctrine developed by the federal and state courts, operates to exclude from trial both primary evidence obtained as a direct result of an illegal search or seizure, as well as evidence later discovered and found to be derivative of an illegality).

99. Gov't Resp. to the Decl. of Josh Horowitz, *supra* note 98, at 7. *See also* Andy Greenberg, *Feds 'Hacked' Silk Road Without a Warrant? Perfectly Legal, Prosecutors Argue*, WIRED (Oct. 7, 2014, 9:41 AM), http://www.wired.com/2014/10/feds-silk-road-hack-legal/ ("Given that the SR Server was hosting a blatantly criminal website, it would have been reasonable for the FBI to 'hack' into it in order to search it, as any such 'hack' would simply have constituted a search of foreign property known to contain criminal evidence, for which a warrant was not necessary").

100. 18 U.S.C. § 1030(f).

101. *See* United States v. Jacobson, 466 U.S. 109, 122 (1984) ("The concept of an interest in privacy that society is prepared to recognize as reasonable is, by its very nature, critically different than from the mere expectation, however well justified, that certain facts will not come to the attention of the authorities.").

browser such as TOR.[102] Taken together with an all-encompassing national security exception, *any* privacy expectation online is essentially nonexistent, especially where the Internet is being used to further criminal activity.

B. The Constitutionality of Government Techniques on the Dark Web

Internet freedom advocates have raised concerns about government techniques to unmask the identity of dark web users, largely because there are few details on how such technology actually operates, and who has access to it.[103]

In *Kyllo v. United States,* the Court considered whether law enforcement's use of technology not generally available to the public constitutes a search, thereby triggering the Fourth Amendment probable cause requirement.[104] The Court held that the government's use of sense-enhancing technology "not in general public use," aimed at the interior of a home, is a physical intrusion of a constitutionally protected area and therefore a search.[105]

While the search in *Kyllo* involved activity directed into a home, where individuals have a strong expectation of privacy, activity on the dark web is distinguishable in that the Internet is a public space, therefore individuals have no legitimate expectation of privacy. Unlike *Kyllo*, the government is not invading a constitutionally protected area in analyzing patterns of activity or unveiling the identity of individuals who are violating the law. Instead, such activity is being done in the open in a public forum—the identity of each individual is merely encrypted. This is akin to an individual, covered with a full-bodied mask and a voice converter, committing criminal activity on a public street. Government techniques to unencrypt otherwise public activity would therefore not constitute a "search" under the Fourth Amendment.[106]

It should be noted that those who use the dark web for perfectly legal reasons, such as journalists, activists, and the politically oppressed, are left with diminished privacy due to law enforcement's strong interest in unveiling darknet activity. The policy herein lies in the harm such anonymity may

102. *See* United States v. White, 401 U.S. 745, 752 (1971) (the Supreme Court unambiguously held that an individual does not have a reasonable expectation of privacy in information voluntarily disclosed to a third party, even where that third party ends up being a government informant).
103. *Id*.
104. *Kyllo*, 533 U.S. at 34.
105. *Id*.
106. *See* United States v. Knotts, 460 U.S. 276, 281-82 (1983) ("A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. . . The fact that the officers in this case relied not only on visual surveillance, but on the use of the beeper to signal the presence of Petschen's automobile to the police receiver, does not alter the situation. Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case."). Since the first draft of this paper, multiple federal district courts have supported my proposition that an individual has no reasonable expectation of privacy in his or her IP address, and therefore government acquisition of an IP address on TOR through the network investigative technique does not constitute a search under the Fourth Amendment. See *Farrell*, 2016 WL 705197, at 1; *Matish*, 2016 WL 3545776, at 20-21; *Werdene*, 2016 WL 3002376, at 1; *Michaud*, 2016 WL 337263, at 7.

cause the public in the form of hiding criminals, on balance with the public's concern for privacy. Strong encryption is burdening investigations as more criminals are turning to the dark web. Alternatively, many argue this is merely an indicator that law enforcement must develop more effective methods to solve crimes without violating the public's evolving expectation of privacy.

C. Modernizing the Third Party Doctrine

Although the current state of the law indicates there may never be a reasonable expectation of privacy on the dark web, the scope of the third party doctrine should nonetheless be reevaluated to conform to the modern reality of Internet usage today. The benefits of sharing information on an anonymous platform such as TOR are plenty. Privacy furthers democracy, knowledge, and human rights, and should not be left entirely unprotected by outdated law.

The third party doctrine was developed in an era that did not contemplate the complexity of the Internet nor how widely used the Internet would eventually become. If left intact as technology continues to develop, the third party doctrine leaves little room for activity that our society would now consider objectively reasonable, and forecasts a bleak future where individuals cannot expect privacy in the most sacred dealings of life given the impracticability of participating in modern society without utilizing third party services in some respect.

The Supreme Court has taken note of this concern. In 2012, Justice Sotomayor evaluated the shortcomings of the third party doctrine with relation to technological advances:

> Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. . . . [I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.[107]

Justice Alito has likewise taken issue with the law in the face of technological advancements. "The *Katz* expectation of privacy test . . . is not without its own difficulties. It involves a degree of circularity, [citation], and judges are apt to confuse their own expectations of privacy with those of the hypothetical reasonable person to which the *Katz* test looks."[108] Justice Alito further recognized that, "[t]echnology can change those expectations."[109]

These observations certainly lay some foundation for evolving the law; however, privacy on the dark web will likely remain unaffected by any privacy advancements given its public nature and propensity to harbor criminal activity.

VI. JURISDICTIONAL CONSTRAINTS TO COMBATING INTERNATIONAL CRIME

107. United States v. Jones, 132 S. Ct. 945, 956-57 (2012) (Sotomayor, J., concurring).
108. *Id.* at 963 (Alito, J., concurring).
109. *Id.*

Today, cross-border data transfers are inevitable, and conflicting privacy laws across jurisdictions further the likelihood that one country will violate the privacy expectations of citizens in another culture. While the United States takes a particular stance on encryption, privacy, and the dark web, other jurisdictions may disagree with the limits law enforcement may go to unencrypt communications. Digital evidence is complex—it is "not only often stored outside a jurisdiction that might seek it, but highly mobile and split between several locations. It may be owned or operated from still others."[110] While a challenge, governments have managed to resolve jurisdictional questions with regard to other intangible goods, such as intellectual property.[111]

A. International Cooperation

One trend to overcoming jurisdictional obstacles is to engage in closer cooperation with foreign law enforcement agencies.[112] Some of the most famous cybercrime busts have occurred through international cooperation, such as the takedown of Shiny Flakes in Germany,[113] and Operation Onymous, where collaboration between Europol, the FBI, and the U.S. Department of Homeland Security led to the arrest of seventeen people across several countries in connection with various black market crime rings.[114] The international community has been taking collaboration and differing privacy standards seriously. In 2007, the OECD adopted the Recommendation on Cross-Border Co-Operation in the Enforcement of Laws Protecting Privacy to address privacy on a global scale.[115] In response, the U.S. Federal Trade Commission (FTC), together with enforcement authorities from around the world, founded the Global Privacy Enforcement Network to promote cross-border information sharing, investigation, and enforcement cooperation.[116] Most recently, INTERPOL and Europol have proposed establishing a Joint Cybercrime Cooperation and Compatibility Taskforce to help harmonize differing legal systems and create an efficient method for cooperation.[117]

One tool that has facilitated international cooperation is "mutual legal assistance," where one country may request the government of another country to get a local judge to issue a warrant for the information at issue. Mutual Legal Assistance (MLA), regarded as a solution to obtaining data held internationally, is an agreement, or often a treaty, between countries to provide assistance to one

110. *Under My Thumb*, *supra* note 55.
111. *Id.*
112. *Id.*
113. Rob Price, *Crazy Photos of Drugs Seized in the Largest Deep Web Drug Bust*, BUSINESS INSIDER (Mar. 13, 2015, 7:17 AM), http://www.businessinsider.com/german-police-bust-shiny-flakes-deep-web-drug-operation-2015-3?r=UK&IR=T.
114. Andy Greenberg, *Global Web Crackdown Arrests 17, Seizes Hundreds of Dark Net Domains*, WIRED (Nov. 7, 2014, 6:00 AM), http://www.wired.com/2014/11/operation-onymous-dark-web-arrests/.
115. PETER SWIRE & KENESA AHMAD, U.S. PRIVATE-SECTOR PRIVACY: LAW AND PRACTICE FOR INFORMATION PRIVACY PROFESSIONALS 1, 24-25 (Sarah Weaver ed., 2012) [hereinafter SWIRE & AHMAD, U.S. PRIVATE-SECTOR PRIVACY].
116. *Id.*
117. Kylie Bull, *Joint International Task Force Launched to Fight Cyber Crime,* HOMELAND SECURITY TODAY (Oct. 5, 2015), http://www.hstoday.us/focused-topics/cybersecurity/single-article-page/joint-international-task-force-launched-to-fight-cyber-crime/b097fcc64ba8a65d6fac899e14c18c8e.html.

another regarding criminal legal matters.[118] This process is determined by a combination of national law, and treaties on international crime.[119] "MLA is resilient because it is the only process that ties together the laws of both receiving and requesting country, making it legally robust at all stages."[120] MLA was instrumental in the case of the Silk Road, where authorities in Iceland assisted U.S. authorities and facilitated the capture of Ross Ulbricht in San Francisco.[121]

While MLA facilitates lawful collaboration, it also has its drawbacks. For instance, conflicts arise where one country prohibits disclosure of data, but the laws of another country compel its disclosure.[122] Further, it is often unclear how, with whom, and when data can be shared from jurisdiction to jurisdiction. Administrative inefficiencies pose another problem to MLA—the time it takes to process an MLA can render the mechanism practically moot. The procedure is long, requiring an administrative legal process, and duplicate checking of paperwork in each country.[123] For example in the U.K., it can take up to thirteen months to process an MLA request, and in the U.S., it can take up to ten months.[124] Because expediency is often critical to coordinate a meaningful response, such inefficiencies undercut the efficacy of MLA.

The reality of inconsistent approaches to privacy rights across jurisdictions emphasizes the need for a more fluid system of international cooperation. One solution is to streamline the MLA process by removing the red tape, where possible.[125] Another is to create a global clearinghouse to handle MLA requests according to a uniform body of rules.[126] Although this task would take many years to put in place, with no promise of success, such a coalition, if formed with the right partners, could entice others to join in due time.[127]

B. Choice of Law

In addition to, and as a part of MLA, courts must also determine which laws apply to data flowing across multiple jurisdictions, further complicating the issue. The international community has developed a deep distrust in U.S. intelligence practices as a consequence of the Snowden leaks, thereby making collaboration more difficult.[128]

---

118. Gail Kent, *The Mutual Legal Assistance Problem Explained*, THE CENTER FOR INTERNET AND SOCIETY (Feb. 23, 2015, 1:06 PM), http://cyberlaw.stanford.edu/blog/2015/02/mutual-legal-assistance-problem-explained.
119. *Id.*
120. *Id.*
121. Donna Leinwand Leger, *How the FBI Brought Down Cyber-Underworld Site Silk Road*, USA TODAY (May 15, 2014, 2:54 PM), *available at* http://www.usatoday.com/story/news/nation/2013/10/21/fbi-cracks-silk-road/2984921/.
122. SWIRE & AHMAD, U.S. PRIVATE-SECTOR PRIVACY, *supra* note 115, at 25.
123. *Id.*
124. *Id.*
125. *Under My Thumb*, *supra* note 55.
126. *Id.*
127. *Id.*
128. *See* Charlie Savage & Jonathan Weisman, *N.S.A. Collection of Bulk Call Data Is Ruled Illegal*, N.Y. TIMES (May 7, 2015), *available at* http://www.nytimes.com/2015/05/08/us/nsa-phone-records-collection-ruled-illegal-by-appeals-court.html; Alison Smale, *Germany Limits Cooperation with U.S. Over Data Gathering*, N.Y. TIMES

On the surface web, a heated battle is already being fought over whether U.S. law enforcement, with a valid search warrant, can require information owned by an American firm, stored in an off-shore data center, be turned over to facilitate a criminal investigation.[129] Since 2013, Microsoft has refused to turn over data stored oversees in Dublin, Ireland to the U.S. government, claiming that the foreign physical location of the data storage center means it is not subject to U.S. law, and that the U.S. government must obtain the information through collaborating with foreign authorities rather than compelling Microsoft to violate its users' expectations of privacy.[130] The U.S. government maintains that because Microsoft is a U.S. company, it is bound by U.S. laws and therefore must comply with the warrant.[131] The lower court sided with the government and held Microsoft in contempt for its failure to comply with the warrant.[132] On appeal, the Second Circuit reversed the district court, holding that "Congress did not intend the SCA's warrant provisions to apply extraterritorially" and that "the SCA does not authorize a U.S. court to issue and enforce an SCA warrant against a United States-based service provider for the contents of a customer's electronic communications stored on servers located outside the United States.[133] In interpreting Congressional intent, the court reasoned that the Stored Communications Act "[n]either explicitly nor implicitly . . . envision[ed] the application of its warrant provisions overseas," given that the statute was drafted at a time where data transfers across international boundaries were not routine as they are today.[134] The court further noted that the decision "serves the interests of comity that, as the MLAT process reflects, ordinarily govern the conduct of cross-boundary criminal investigations."[135] As a consequence of the *Microsoft* litigation, there is now a developing trend among technology companies to physically store data in countries beyond U.S. control to eliminate backdoor access by the U.S. government.[136]

World governments are carefully tracking the *Microsoft* decision, as an outcome in favor of the U.S. will threaten the sovereignty of other nations without delivering a similar benefit.[137] In addition to threatening the sovereignty of other governments, an outcome in favor of the U.S. will also affect the

(May 7, 2015), *available at* http://www.nytimes.com/2015/05/08/world/europe/germany-to-pull-back-on-helping-us-gather-intelligence.html (explaining that this distrust can be felt by the effect of Germany recently curtailing its cooperation with U.S. intelligence, following revelations that the U.S. had been spying on Germans).

129. *See* In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014), rev'd and remanded sub nom. Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016).
130. *Id*.
131. *Id*.
132. *Under My Thumb*, *supra* note 55; Nora Ellingson, *The Microsoft Ireland Case: A Brief Summary*, LAWFARE (Jul. 15, 2016, 10:34 AM), https://www.lawfareblog.com/microsoft-ireland-case-brief-summary.
133. In the Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, 2016 WL 3770056 *19 (2d Cir. July 14, 2016).
134. *Id*. at 1.
135. *Id*. at 18.
136. Murad Ahmed & Guy Chazan, *Microsoft Data Centres: The Key to Internet Security?*, FINANCIAL TIMES (Nov. 11, 2015, 2:42 PM), *available at* http://www.ft.com/cms/s/2/bc57c152-886d-11e5-9f8c-a8d619fa707c.html#axzz3rJ2LXAvo.
137. *Id*.

reputation of technology companies before their consumers. If law enforcement can compel U.S. companies to disclose data physically stored abroad, businesses with international clients may further erode—a setback many companies are fearful of in light of the damage caused by the Snowden leaks and the National Security Agency's program PRISM.[138] Driven by consumer privacy demands, technology companies are increasingly reconfiguring their services to strengthen security to protect against data breaches and government-compelled information requests.[139] As a result, the FBI, now hindered by an inability to access data even with a valid warrant, has devoted an entire unit to fighting the war on encryption.[140]

C. Public Policy

While international cooperation and legal formalities are the ideal method preferred by data subjects and the international community alike, countries have regularly bypassed collaboration by obtaining evidence unilaterally through less formal methods. The drawbacks of this approach include less accountability and less transparency, which can encourage governments to work around the law without being subjected to public accountability.

As a policy matter, it is critical to accept the reality that while governments will always act in self-interest to preserve national interests, a country's citizens are also foreigners of other nations. Underhanded behavior at the expense of international relations and diplomacy will encourage other sovereigns to reciprocate and infringe on the privacy rights of the U.S. and its citizens.[141] It is within the interests of the U.S. to respect the varying privacy standards from jurisdiction to jurisdiction, and pursue lawful, cooperative means to facilitate criminal investigations.[142] In the end, combating crime on the dark web is an international objective, shared by all nations. Recognition that privacy is a fundamental human right of *all* people, irrespective of citizenship, will strengthen rapport between sovereigns and among consumers, and will result in more effective cooperation, better intelligence, and more security for all in the long run.[143]

VII. CONCLUSION

138. *See id*.
139. *See* Ellen Nakashima, *Apple Vows to Resist FBI Demand to Crack iPhone Linked to San Bernardino Attacks*, THE WASHINGTON POST (Feb. 17, 2016), *available at* https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html. *See also* Vibhushan Waghmare, *Encryption—A Strategy Business Can Ill-Afford to Ignore*, SECUREDB (Apr. 29, 2015), https://securedb.co/blog/encryption-a-strategy-businesses-can-ill-afford-to-ignore/.
140. Mark Greenblatt et al., *FBI Opens New Chapter In War On Encryption, 'Going Dark'*, KIVI (Nov. 5, 2015, 4:07 AM), http://www.kivitv.com/news/national/fbi-opens-new-chapter-in-war-on-encryption-going-dark?google_editors_picks=true.
141. David Cole, *We Are All Foreigners: NSA Spying and the Rights of Others*, JUST SECURITY (Oct. 29, 2013, 12:48 PM), https://www.justsecurity.org/2668/foreigners-nsa-spying-rights/.
142. *See id*.
143. *Id*.

Privacy on the Internet is difficult to define, as the purpose of the Internet was to create a network to facilitate the sharing of information. As we move toward a world where the most intimate details of our lives are now recorded and stored online for an indefinite duration, and further toward a world where the public is fighting to modernize the concept of Internet privacy under the law, the current U.S. framework must be reevaluated as our society continues to evolve and innovate. In the end, it is in the best interests of both individuals and the U.S. to maintain a system whereby the government, with probable cause and a valid warrant issued from a neutral magistrate, retains a lawful avenue to access encrypted data to facilitate criminal investigations and gather effective, relevant intelligence. Likewise, to gain allies in the fight against dark web crime, the U.S. government should continue to employ collaborative efforts to facilitate extraterritorial investigations within the legal framework of the particular sovereign housing the data at issue. The fate of our privacy, as a fundamental human right, will depend largely on the policy debates surrounding the extent to which we, as a nation, and as a world, value privacy on balance with security.