UIC John Marshall Journal of Information Technology & Privacy Law

Volume 30 | Issue 3 Article 5

Summer 2014

The Problems with PRISM: How A Modern Definition of Privacy Necessarily Protects Privacy Interests in Digital Communications, 30 J. Marshall J. Info. Tech. & Privacy L. 571 (2014)

Adam Florek

THE PROBLEMS WITH PRISM: HOW A MODERN DEFINITION OF PRIVACY NECESSARILY PROTECTS PRIVACY INTERESTS IN DIGITAL COMMUNICATIONS

ADAM FLOREK*

I. INTRODUCTION

In June 2013, National Security Agency (NSA) analyst Edward Snowden revealed the existence of clandestine government programs, codenamed PRISM and XKeyscore, designed to collect and aggregate information from numerous service providers into a single searchable database.[1] *The Guardian* reporter Glen Greenwald first described the programs in a series of articles for the British paper, portraying PRISM as an Orwellian program that has infiltrated service providers from Microsoft to Apple, and from Facebook to Google.[2] The programs' directive is to collect usage data and communications directly from the service providers on virtually every aspect of online life.[3]

It is common knowledge that social media sites collect personal data from their users and in the majority of instances it is the user that is actually providing the information. How else would you be able to

* Adam Florek is the former owner-operator of River's Edge Group, Inc. He received his B.A. in Political Science from Purdue University in 2010 and is currently pursuing his J.D. at The John Marshall Law School, expected May 2015.

1. Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, THE GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

2. *Id*.

3. Glenn Greenwald, *XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet,'* THE GUARDIAN (July 11, 2013), http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

connect with your "friends" via Facebook or get technical support from Microsoft? Different sites, however, collect different types of information from their users. For instance, Google uses user search history to generate targeted ads[4] whereas Facebook monitors an individual's interests and activity to suggest friends and similar interests.[5]

In contrast, the PRISM program collects far more information. PRISM goes beyond the self-imposed limitations on data collection that private entities such as Google or Facebook adhere to.[6] The PRISM program collects "audio and video chats, photographs, e-mails, documents, and connection logs"[7] and additional information from Microsoft, Yahoo!, Google, Facebook, PalTalk, YouTube, Skype, AOL, Apple, and other participating service providers.[8] The information is allegedly collected directly from provider hardware via NSA technology and deployed at various private network locations allowing for more intimate access.[9] The information, collected in real time, is indexed for analysis and search ability.[10]

PRISM is authorized under the 2008 Amendments to Section 702 of the Foreign Intelligence Surveillance Act of 1974 (FISA).[11] The Act provides the federal government with expanded surveillance powers in connection with intelligence gathering and surveillance on foreign individuals in the digital world.[12] However, there are restrictions that appear to prohibit surveillance of American citizens: target(s) must be

---

4. *Privacy & Terms*, GOOGLE, http://www.google.com/policies/privacy (last visited May 22, 2014).

5. *Data Use Policy*, FACEBOOK, https://www.facebook.com/about/privacy/your-info (last visited May 22, 2014).

6. *Id.* (analyzing their respective privacy policies, Google and Facebook each outline the information that is collected from the user. For example, Facebook collects information that the user chooses to share with it as well as information other people connected to the user choose to share with the user. Though this seems very broad, the specifics are outlined in the Facebook Data Use Policy).

7. Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 6, 2013), http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

8. Greenwald & MacAskill, *supra* note 1.

9. *Id.* ("[T]he Prism program allows the intelligence services direct access to the companies' servers. . . . The Prism program allows the NSA, the world's largest surveillance organization, to obtain targeted communications without having to request them from the service providers and without having to obtain individual court orders.").

10. *Id.* ("With this program, the NSA is able to reach directly into the servers of the participating companies and obtain both stored communications as well as perform real-time collection on targeted users.").

11. 50 U.S.C. § 1881 (2008).

12. *Id.; see also* § 1881a(b)(l).

outside of the United States;[13] may not be a U.S. person living abroad;[14] and surveillance must be consistent with the Fourth Amendment.[15] Surveillance is allowed in the instance where a party is outside of the United States or under certain other circumstances.[16]

The presence of a data aggregation program, such as PRISM or XKeyscore, raises a number of new and unique legal issues. The right to privacy is a recognized and protected constitutional right. While that right may be circumvented, there are due process mechanisms in place to ensure that the government cannot wantonly invade the privacy of its citizens. PRISM, as it has been portrayed, seems to be in violation of a number of these fundamental privacy rights.

Because PRISM and other surveillance programs create a number of privacy concerns, it is doubtful that the current "reasonable expectation"[17] doctrine is sufficient to safeguard privacy interests in an increasingly monitored society. This Comment will first explore the right to privacy and its evolution from Warren and Brandeis's "right to be let alone"[18] to the modern two prong analysis established by Justice Harlan in *Katz v. United States*[19] and its application to an increasingly technological collection of cases. In Part II, this Comment will discuss the application of the right to privacy in cyberspace and society's expectation therein. Part III will explore the impact of surveillance, particularly the NSA's surveillance programs, on people and social interactions. Finally, this Comment will conclude by advocating for a modernized definition of privacy that affords increased protections to the individual in keeping with society's expectations and the dismantlement of the NSA's domestic data collection operations.

---

13. *See* § 1881a.

14. *Id.*

15. *Id.*

16. *Id.*

17. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("[T]he expectation be one that society is prepared to recognize as 'reasonable.'").

18. Samuel D. Warren & Louis D. Brandeis, Comment, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

19. *Katz*, 389 U.S. at 360 (Harlan, J., concurring).

II. BACKGROUND

A. THE PRISM PROGRAM

1. Purpose

The need for a comprehensive surveillance program was realized after the terrorist attacks on September 11, 2001.[20] The mandate of the PRISM program is to monitor and aggregate foreign communications in an effort to protect American interests from foreign threats.[21] The program is designed to give law enforcement officials an additional avenue to investigate terrorism and to "allow . . . intelligence professionals to quickly and effectively monitor the communications of terrorists abroad."[22] The 2008 Amendments to FISA provide a more comprehensive surveillance program while allegedly safeguarding American liberties and addressing the inadequacies and issues of its predecessors.[23]

2. How Did We Get Here? The History of Post-9/11 Surveillance and its Present Authorization

The PRISM program is only the latest iteration of a foreign surveillance program under FISA. In the months and years following the terrorist attacks of 9/11, the federal government initiated a number of programs and operations to expand the scope of surveillance in an effort to ensure that the events of 9/11 were not repeated. These programs were carried out with varying degrees of success, and met with a wide range of public apprehension.[24]

President George W. Bush authorized the first of these programs called "Terrorist Surveillance Program,"[25] via an Executive Order.[26]

---

20. NAT'L COMM. ON TERRORIST ATTACKS UPON THE U.S., U.S. SENATE, THE 9/11 COMMISSION REPORT 1-14, http://www.9-11commission.gov/report/911Report.pdf (last visited Nov. 23, 2013).

21. President George W. Bush, statement upon signing H.R. 6304 (July 10, 2008) (the President, when signing the bill into law said, "The bill I sign today will help us meet our most solemn responsibility: to stop new attacks and to protect our people").

22. *Id*.

23. President Bush indicated in his statement that the 2008 FISA Amendments would allow American intelligence agencies to know what terrorists abroad were plotting while protecting the liberties of American citizens at home. *Id*.

24. David E. Sanger & John O'Neil, *White House Begins New Effort to Defend Surveillance Program*, N.Y. TIMES (Jan. 23, 2006), http://www.nytimes.com/2006/01/23/politics/23cnd-wiretap.html?pagewanted=all.

25. Barton Gellman, Dafna Linzer, & Carol D. Leonnig, *Surveillance Net Yields Few Suspects*, WASH. POST (Feb. 5, 2006), http://www.washingtonpost.com/wp-dyn/content/article/2006/02/04/AR2006020401373.html.

26. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers without Courts*,

This program was put into place in early 2002, in the period directly following the attacks of September 11, 2001. This program had a similar directive and operating parameters to PRISM; however, it was conducted without any oversight.[27] It is unclear whether the program was bound by the same procedures that had been established under FISA, whether it was operating outside its purview, or whether the executive branch had the ability to bypass FISA procedures if they deemed necessary. When the program became public knowledge, outrage ensued leading to the warrantless wiretapping scandal.[28] The program was vigorously defended by its proponents as a necessary measure in the fight against terrorism.

The Terrorist Surveillance Program was the immediate predecessor to the "Protect America Act of 2007."[29] The Protect America Act was an attempt to legalize many of the surveillance procedures that were in place under the Terrorist Surveillance Program;[30] however, the Act had a sunset provision and was only in force for six months.[31] Although the broad scope of the Protect America Act was short lived,[32] many of the orders under Protect America were carried through under Transitional Procedures written into the 2008 FISA Amendments.[33]

Finally the 2008 FISA Amendments gave rise to the current surveillance program, PRISM. The program authorized under Section 702 of the FISA Amendments Act of 2008[34] allows for much of the same surveillance and monitoring as under its predecessors, but appears on its

---

N.Y. TIMES (Dec. 16, 2005), http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all&_r=0.

27. Sanger & O'Neil, *supra* note 24. The programs directive was to monitor international telephone and e-mail traffic where at least one party was outside of the United States and there was a reasonable belief that the overseas party had a link to Al Qaeda. *See id*.

28. *Id*.

29. Protect America Act of 2007, Pub. L. No. 110–55, § 121 Stat. 552 (2007).

30. Ellen Nakashima & Joby Warrick, *House Approves Wiretap Measure*, WASH. POST (Aug. 5, 2007), http://www.washingtonpost.com/wp-dyn/content/article/2007/08/04/AR2007080400285.html?nav=rss_politics (explaining that not only will the new bill allow the NSA to collect communications without a warrant but the bill will also allow the NSA to monitor domestic Americans).

31. Protect America Act of 2007, Pub. L. No. 110–55, § 121 Stat. 552 (2007).

32. *See* Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110–261, § 122 Stat. 2436 (2008) (in addition to the sunset provision written into the Protect America Act's text, a provision of the 2008 amendments also repealed the Arotect America Act).

33. *Id*.

34. 50 U.S.C. § 1881 (2008).

face to provide some additional security to Americans.[35] The PRISM program, while authorized by FISA and approved by the FISA Court, seems to operate without direct judicial supervision.[36] Instead, the FISA Court approves the general "Minimization Procedures"[37] that the program must adhere to, and ensures that any request made complies with these procedures.[38]

The difference between this and previous operations grows more distinct as the procedures and requisite levels of evidence are further examined. In *Amnesty International USA v. Clapper*, the court stated:

> [U]nder the preexisting FISA scheme the government had to submit an individualized application for surveillance identifying the particular target, facility, type of information sought, and procedures to be used, under the FAA, the government need not submit a similarly individualized application—it need not identify the particular target or facility to be monitored. . . . Second, whereas under the preexisting FISA scheme the FISC had to find probable cause to believe both that the surveillance target is a "foreign power" or agent thereof and that the facilities to be monitored were being used or about to be used by a foreign power or its agent, under the FAA the FISC no longer needs to make any probable-cause determination at all.[39]

These distinctions mean that while the current program may have repealed and replaced the less popular but better known Protect America Act, it still provides a very broad range of powers to the NSA, via FISA, with little real judicial supervision.

B. THE EVOLUTION OF THE RIGHT TO PRIVACY

The constitutional right to privacy cannot be found in the text of the Constitution; it is among our unenumerated rights.[40] The Supreme

---

35. *Id.* at § 1881a(b) (providing limitations on who may be surveyed and where they must be physically located to be subject to surveillance); *see* § 1881a(e) (requiring the adoption of "Minimization Procedures," designed by the Attorney General and Director of National Intelligence, to protect American citizens from undue search).

36. *NSA Slides Explain the PRISM Data-Collection Program*, WASH. POST, http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents (last updated July 10, 2013) ("The Foreign Intelligence Surveillance Court does not review any individual collection request.").

37. 50 U.S.C. § 1881a(e)(2) (2008) (establishing judicial review of minimization procedures to be implemented).

38. *Id.* at § 1881a(i)(2) (outlining what the FISA courts may review: (A) The courts may review certifications of the Attorney General or Director of National Intelligence affirming that all outlined procedures have been followed and the target(s) are not protected by § 1881a(b); (B) whether the Targeting Procedures are reasonably designed to meet their objectives while adhering to the established limitations).

39. Amnesty Int'l USA v. Clapper, 638 F.3d 118, 125-26 (2d Cir. 2011).

40. Griswold v. Connecticut, 381 U.S. 479, 486-87 (1965) (holding that although the

Court has found that the right to privacy, "[the] right to be let alone by other people,"[41] is protected by the Fourth Amendment: "[The Fourth] Amendment protects individual privacy against certain kinds of governmental intrusion. . . ."[42] The Supreme Court stated, "the Fourth Amendment cannot be translated into a general constitutional 'right to privacy.'"[43] However, the Court often finds a right to privacy based on both an individual's reasonable expectation of privacy and society's general acceptance of that expectation as outlined in Justice Harlan's concurrence[44] in *Katz v. United States*.[45]

Although courts often look to society's reasonable expectation to determine privacy interest, the "right to be let alone"[46] is at the genesis of modern privacy jurisprudence. This right stemmed from Judge Cooley's treatises on torts.[47] Justice Brandeis and Samuel Warren recognized that in a fast paced time, "the intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world . . . so that solitude and privacy have become more essential to the individual."[48] This meant that a person may, from time to time, need to retreat from the pressures of society and should be free to do so without unwanted intrusion into his personal spaces. In a time when photography and recording devices were becoming common place[49] and tabloids were publishing an increasing amount of gossip, retreat into solitude was sufficient to insulate the individual from the prying eyes of the outside world.[50]

"The right to be let alone" found significant support in the judiciary as well. The "right to be let alone" has been used to build the

---

Constitution fails to explicitly acknowledge a right to privacy, it does in fact "embrace the right of . . . privacy").

41. Katz v. United States, 389 U.S. 347, 350-51 (1967).

42. *Id.*

43. *Id.*

44. *Id.* at 361 (Harlan, J., concurring) ("My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

45. *Id.* at 360.

46. Warren & Brandeis, *supra* note 18.

47. *Id.* at 195.

48. *Id.* at 196.

49. *Id.* at 195. Since by 1890 newspapers and photographs were commonplace, Warren and Brandeis already feared that "what is whispered in the closet shall be proclaimed from the house-tops." *Id.*

50. *Id.* at 196.

foundation for a right to privacy for marital couples,[51] being relied upon to find a right to be free from intrusive state regulations.[52] In *Katz*[53] the right was expanded so that one may have a "right to be let alone" not only in his home, but also other places where an individual has a subjective and objective belief that he is free from observation.[54]

In *Katz*,[55] the Supreme Court held that an individual had a reasonable expectation of privacy in a public telephone booth[56] and that an electronic listening device attached to the outside of said booth was in violation of the freedom from search and seizure protected by the Fourth Amendment.[57] However, *Katz*[58] is most frequently cited for Justice Harlan's concurrence where he establishes the two prong (subjective and objective) test that would become the standard for evaluating privacy interests.[59]

1. Applying *Katz*

One such application of Justice Harlan's two prong approach is seen in *United States v. Salinas-Cano*.[60] Here, the court looked to an individual's reasonable expectation to privacy in a suitcase that had been kept with a friend. The court determined that if permission to access the contents had not been given, then neither the party in possession nor a third party could be permitted access to the container.[61]

---

51. *See generally* Griswold v. Connecticut, 381 U.S. 479 (1965).

52. *See generally* Roe v. Wade, 410 U.S. 113 (1973).

53. *See generally* Katz v. United States, 389 U.S. 347 (1967).

54. In *Katz*, the defendant made a call from a closed public phone booth that had a recording device discretely placed outside the booth to record the defendant's phone call. The court found in the defendants favor that he did in fact have a constitutionally protected right to privacy within the phone booth. *Id.* at 348-49.

55. *Id.*

56. Because both Mr. Katz and society had an expectation that the conversation would remain private and the government's action of affixing a listening device to the outside of the booth, while not physically invasive, was still an invasion of his right to privacy. *Id*.

57. "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated. . . ." U.S. CONST. amend. IV.

58. *Katz*, 389 U.S. at 360-62.

59. "My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'" Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

60. *See generally* United States v. Salinas-Cano, 959 F.2d 861 (10th Cir. 1992).

61. Id. at 863. ("[W]hen a guest in a private home has a private container to which the homeowner has no right of access . . . the homeowner . . . lacks the power to give effective consent to the search of the closed container.").

The test from *Salinas-Cano*[62] was expanded in subsequent cases. In *Garcia v. Dykstra*, plaintiffs brought an action against the owner of a storage unit who had been complicit in the unlawful search of their respective units.[63] The court found that in addition to authorization from the possessor (land owner) of the unit, law enforcement officers needed a reasonable belief that the party authorizing the search did in fact have authority to grant access.[64]

a. Third Party Disclosures and Forfeiting Reasonable Expectation

The Court has time and again looked back to the test established in *Katz* to determine whether the right to privacy extends to the area in question. In *United States v. Miller,* the Supreme Court found that an individual did not have a reasonable expectation to privacy in his banking records, checks, deposit slips, etc.[65] The information contained in the aforementioned documents had been turned over voluntarily and therefore stripped of privacy protections.[66] A robbery conviction was upheld in *Smith v. Maryland* although significant evidence was gathered through the use of a pen register installed without a warrant.[67] The Court found that because the pen register collected a limited cross section of data and the majority of subscribers know in some capacity that the telephone company has access to the numbers dialed, there could be no general expectation of privacy.[68]

In *California v. Greenwood*, the Court applied Justice Harlan's test to garbage bags placed at the curb and later intercepted by police.[69]

---

62. *Id.* at 864 (outlining the 3-element test: (i) does the container command a high degree of privacy; (ii) has the true owner taken precautions indicating an expectation of privacy; and (iii) does the consenting party lack authority to consent).

63. Garcia v. Dykstra, 260 F. App'x 887, 894 (6th Cir. 2008).

64. *Id.* at 900 (quoting Illinois v. Rodriguez, 497 U.S. 177, 188-89 (1990)).

65. United States v. Miller, 425 U.S. 435, 435-36 (1976).

66. *Id.* at 442-43 ("The checks are not confidential communications but negotiable instruments to be used in commercial transactions.").

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

68. *Id.* at 741-43 (rejecting the claim for a privacy interest because (i) a person must know that by dialing phone numbers, he is disclosing those numbers to the telephone companies, and (ii) that those companies are able to record the telephone numbers).

69. California v. Greenwood, 486 U.S. 35, 35 (1988). Police acting on a tip that the defendant may be involved in narcotics trafficking obtained the defendant's garbage once it had been left at the curb. Upon sifting through the garbage and finding drug paraphernalia the police obtained a search warrant for the defendant's home, probable cause was only available because of the search of the garbage. *Id.* at 37-38.

The Court found that while the defendant may have had a reasonable expectation of privacy in his garbage, it was not one that society was willing to accept as reasonable.[70] The Court noted that the garbage was abandoned by the defendant to be collected later by a third party; therefore, the garbage had been left on the curb for "animals, children, scavengers, snoops, and other members of the public" to intercept.[71] The aforementioned cases show that where materials are turned over to third parties during the course of business or general life, this information is divulged to a third party and therefore the person does not retain any generally recognized expectation of privacy.

b. Reasonable Expectations and Advancing Technologies

Measures taken can be, and often are, an indication of a party's expectation of privacy in a given situation. In *Dow Chemical Company v. United States*, the plaintiffs went to considerable lengths to secure their manufacturing operations from intrusion or onlookers at ground level but did not obscure the view from above.[72] When the EPA conducted aerial surveillance of the facility using commercial camera equipment,[73] Dow argued that they had a reasonable expectation of privacy as evident by their significant security measures.[74] However, the Court held that the readily observable nature of the complex as well as the commercial availability of the camera overcame privacy concerns.[75]

However, in *Kyllo v. United States*, the government used a highly sophisticated thermal sensing camera to map the ambient temperature of a home and garage to determine that the residents were in fact growing marijuana.[76] The Court found that, though the police did not trespass, their utilization of such technology was in fact a violation of the Fourth Amendment and the defendant's right to privacy.[77] The Court held that the utilization of such technology would be prohibited if it were not commercially available and revealed otherwise unknowable characteristics.[78] Together *Dow Chemical Company*[79] and *Kyllo*[80]

---

70. *Id.* at 43.

71. *Id.* at 40.

72. Dow Chem. Co. v. United States, 476 U.S. 227, 228 (1986).

73. "The photographs at issue in this case are essentially like those commonly used in mapmaking. Any person with an airplane and an aerial camera could readily duplicate them." *Id.* at 231.

74. *Id.* at 229-31.

75. *Id.* at 236-39.

76. Kyllo v. United States, 533 U.S. 27, 27 (2001).

77. "To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment." *Id.* at 34.

78. "We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without

illuminate the lengths to which government agencies may or may not go to acquire information without violating the Fourth Amendment.

The *Kyllo* decision cemented the *Katz* test as the method of determining a reasonable expectation of privacy for new and forthcoming technologies.[81] Additionally, it added another facet to the objective prong of *Katz*: whether the technology being used to conduct surveillance was commonly available to the public and if not, did it reveal information that could not have been known without physical intrusion.[82]

c. Reasonable Expectation and E-mail

While the Supreme Court has applied the reasonable expectation test to new technologies, it has not extended the reasonable expectation of privacy to metadata.[83] In *United States v. Forrester*, the Ninth Circuit analogized an e-mail's sender/recipient metadata attached to the numbers dialed from a telephone; holding that like the outgoing phone number, the metadata had been turned over to a third party and received no privacy protection.[84]

Additionally, *Forrester* examined the expectation of privacy in websites visited by an individual and the collection of IP addresses[85] to determine which websites had been visited and to whom the defendant was sending e-mails.[86] The Court "conclude[d] that the surveillance techniques the government employed here are constitutionally

physical 'intrusion into a constitutionally protected area,' constitutes a search—at least where (as here) the technology in question is not in general public use." *Id.*

79. *See generally* Dow Chem. Co. v. United States, 476 U.S. 227 (1986).

80. *Kyllo*, 533 U.S. at 27.

81. *See generally id.*

82. *Kyllo*, 533 U.S. at 34.

83. *A Guardian Guide to Metadata*, THE GUARDIAN (June 12, 2013), http://www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance#meta=1111111 (discussing that metadata is the unique information that accompanies various forms of communication; typically it is information that will identify the intended parties, the devices used, time and date of the transmission).

84. United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (finding that IP addresses are qualitatively identical to telephone numbers for privacy expectation analysis).

85. *IP Address,* WIKIPEDIA, http://en.wikipedia.org/wiki/IP_address#cite_note-rfc760-1 (last visited May 22, 2014); *see* INFO. SCI. INST., UNIV. OF S. CAL., DOD STANDARD INTERNET PROTOCOL (1980), *available at* http://tools.ietf.org/html/rfc760; INFO. SCI. INST., UNIV. OF S. CAL., INTERNET PROTOCOL – DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION (1981), *available at* http://tools.ietf.org/html/rfc791.

86. *Forrester*, 512 F.3d at 510.

indistinguishable from the use of a pen register that the Court approved in *Smith*."[87] The Court reasoned by analogy that the pen register that was used in *Smith* was indistinguishable from the collection and monitoring of IP addresses in *Forrester*.[88]

United States v. Warshak saw the application of the Stored Communications Act[89] to a personal e-mail account in order to retrieve stored e-mail that implicated the defendant in criminal activity.[90] The Act allowed law enforcement officials to gather intelligence that otherwise would not have been available to them.[91] Later, the Sixth Circuit held that the reasonable expectation of privacy in e-mail was not unwarranted and that given the similarities between e-mail and traditional modes of communication, it would be incongruous to hold that e-mail deserved a lesser standard of protection from intrusion.[92] The Sixth Circuit noted that while it is more possible that, due to the nature of e-mail and its manor of transmission, "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."[93]

d. GPS, Physical Locations and a Reasonable Expectation Therein

In *People v. Weaver*, the New York appellate court held that the placement of a GPS receiver on the defendant's car was in violation of his right to privacy.[94] The Court did not argue its decision on the fact that a nominal trespass to chattel had occurred, but instead focused on

---

87. *Id.* at 510.

88. *Id.* (finding that IP addresses serve an almost identical purpose as telephone numbers insofar as service providers can know and record the incoming and outgoing addresses); *see generally* Smith v. Maryland, 442 U.S. 735 (1979).

89. Stored Wire and Electronic Communications and Transactional Records Access, 18 U.S.C. §§ 2701-2712 (2002) (creating a statutory realm of privacy for "wire or electronic communication . . . in electronic storage . . . ").

90. United States v. Warshak, 631 F.3d 266, 276 (6th Cir. 2010).

91. *Id.* at 288.

92. *Id.* at 285-86. The Court stated:

> Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection. . . . It follows that email requires strong protection under the Fourth Amendment; otherwise, the Fourth Amendment would prove an ineffective guardian of private communication, an essential purpose it has long been recognized to serve. *Id.*

93. *Id.* at 286.

94. People v. Weaver, 909 N.E.2d 1195, 1202-03 (N.Y. 2009). Police placed an unauthorized GPS device on the underside of the defendant's automobile and allowed the car to be monitored for sixty-five days, the device collected data about the time and date as well as location of every trip taken in the car during the length of the surveillance. At no point in time was any warrant obtained. *Id.* at 1195-97.

the expectation of privacy one had in his car.[95] Shortly thereafter, in *United States v. Jones*, the Supreme Court was faced with an identical situation where a GPS receiver was surreptitiously placed on the underside of the defendant's vehicle.[96] Unlike the court in *Weaver*, the Supreme Court chose "to decide [the] case based on 18th-century tort law."[97] The majority held that because there was a trespass, there was a privacy violation.[98]

2. Statutory Protections

a. The Electronic Communications Privacy Act and the Stored Communications Act

The Electronic Communications Privacy Act of 1986[99] ("ECPA") purports to create a statutory right to privacy[100] for "wire, oral or electronic communications."[101] Section (1) creates a class of people[102]—anyone who intentionally intercepts, attempts to intercept, uses, or discloses who shall be punished[103] and or liable[104] for such transgression. The Stored Communications Act[105] ("SCA"), like the ECPA, creates a statutory realm of privacy for "wire or electronic communication . . . in electronic storage. . . ."[106] The sum of these two statutory protections means that communications are protected both during transmission to and from a party and while in various stages of electronic storage.

---

95. *Id.* at 1205.

96. United States v. Jones, 132 S.Ct. 945, 948-49 (2012).

97. *Id.* at 957 (Alito, J., concurring).

98. *Id.* at 958.

99. Wire and Electronic Communications Interception and Interception of Oral Communications, 18 U.S.C. §§ 2510-2522 (2002).

100. In re Subpoena Duces Tecum to AOL, LLC, 550 F. Supp. 2d 606, 610 (E.D. Va. 2008); *see* S. REP. No. 99–541, at 3 (1986) ("The Privacy Act creates a zone of privacy to protect internet subscribers from having their personal information wrongfully used and publicly disclosed by 'unauthorized private parties.'").

101. 18 U.S.C. § 2511 (2008).

102. *Id.* (threatening punishment for any individual who intercepts, uses, tries to use, or discloses improperly-acquired communications).

103. *Id.* at § 2511(4).

104. *Id.* at § 2511(5)(a)(i).

105. Stored Wire and Electronic Communications and Transactional Records Access, 18 U.S.C. §§ 2701-2712 (2002).

106. *Id.* at § 2701(A).

II. ANALYSIS

Today the landscape of telecommunications technology is dramatically different from ten years ago and privacy jurisprudence has had to keep pace. It is highly unlikely that in 1890 when Samuel Warren and future Supreme Court Justice Louis Brandeis were penning their Harvard Law Review article, either of them could anticipate the Internet or any modern telecommunications; the first telephone call was made only fourteen years earlier.[107] However, they did recognize that the common law is "eternal[ly] youth[ful] [and therefore] grows to meet the demands of society."[108]

In the information age, communications no longer take place either over telegraph wires or through operators interconnecting two parties. Fiber optic cables encircle the globe, making communications instantaneous half a world away.[109] Business deals are brokered in real time with parties in geographically isolated areas.[110] Political negotiations take place between world leaders with neither having to leave the safety or comfort of their respective homes.[111] While still desirous of their right to be let alone in their homes and in their persons, people need to be protected in the digital realms as well, due to the interconnected and "fast paced" nature of the modern world. It is no longer a viable option to retreat into one's self and sever ties with the outside world for any prolonged period of time. In an era when business and politics move at hyper speed, absence from information for a day can result in incalculable loses both politically and economically.

The notion that the right to privacy is only the "right to be let alone" is no longer tenable. In the information age, it is necessary to constantly intermingle with outside sources in order to be and remain an active and integral part of society.[112] The right to privacy, like the rest of common law, has evolved and adapted over time to meet each

---

107. The first successful telephone call was made on March 10, 1876. *Invention of the Telephone*, WIKIPEDIA, http://en.wikipedia.org/wiki/Invention_of_the_telephone (last visited May 22, 2014).

108. Warren & Brandeis, *supra* note 18 ("eternal youth, grows to meet the demands of society").

109. *TeleGeography Submarine Cable Map*, SUBMARINE CABLE MAP, http://www.submarinecablemap.com/ (last visited May 22, 2014).

110. Qyou Stoval, *What are the Effects of Global Communications*, EHOW, http://www.ehow.com/info_8145378_effects-global-communication.html (last visited May 22, 2014); Majid Tehranian, *Global Communication and International Relations: Changing Paradigms and Policies*, INT'L. J. OF PEACE STUD. (1997), *available at* http://www.gmu.edu/programs/icar/ijps/vol2_1/Techrenian.htm.

111. Stoval, *supra* note 110; Tehranian, *supra* note 110.

112. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("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.").

era with new laws to govern an ever evolving world. Fourth Amendment jurisprudence must "keep pace with the march of science."[113] In *Katz,* the common law grew to recognize that the right to privacy was no longer tied to a physical invasion of property. The Katz Court "expressly held that the Fourth Amendment governs not only the seizure of tangible items, but extends as well to the recording of oral statements overheard without any technical trespass under local property law,"[114] effectively expanding the Fourth Amendment's reach beyond physical trespass.

In *Weaver*, Judge Lippman recognized that the nature of the automobile is in the public eye and it is easily observable, after all the purpose of a car is to travel easily through public streets.[115] Judge Lippman wrote in his opinion that an individual traveling in an automobile does not abandon any reasonable expectation of privacy where it is the case that the protections afforded by the Fourth Amendment would be significantly undermined.[116]

The arguments of the *Weaver* court were largely echoed by Justice Sotomayor in *Jones*.[117] Justice Sotomayor acknowledged that in a modern society one cannot be said to forfeit all Fourth Amendment protection every time he leaves his home.[118] Due to the precision of GPS and its incredibly intrusive nature, it has the capability of illustrating the comings and goings of an individual's car, and more importantly the individual, his destinations and his schedule, painting a very vivid picture of the person.[119] This power is augmented by the surreptitious and inexpensive nature of these GPS devices, allowing the government to

---

113. People v. Weaver, 909 N.E.2d 1195, 1200 (N.Y. 2009) (citing United States v. Garcia, 474 F3d 994, 997 (7th Cir 2007)).

114. Katz v. United States, 389 U.S. 347, 353 (1967) (citing Silverman v. United States, 365 U.S. 505, 511 (1961)).

115. *Weaver*, 909 N.E.2d at 1201.

116. *Id*. at 1200-01; *see* Delaware v. Prouse, 440 U.S. 648, 662–63 (1979).

117. *Jones*, 132 S. Ct. at 946 (Sotomayor, J., concurring). A GPS unit was surreptitiously placed on the defendant's car outside of the authorization of the warrant. Data was collected about the defendant's movement for the next twenty-eight days. The majority opinion held that because there was a nominal invasion of the defendant's property the data gathered was inadmissible. The majority's decision did not to address the issue of whether monitoring the defendant's movements was a breach of his privacy. *Id.*

118. United States v. Jones, 132 S. Ct. 945, 954-55 (2012) (Sotomayor, J., concurring).

119. *Id.* at 955-56; *see also* People v. Weaver, 909 N.E.2d 1195, 1199-1201 (N.Y. 2009).

monitor many subjects with little physical exertion.[120]

A. UBIQUITOUS SURVEILLANCE OF AMERICAN CITIZENS WILL HAVE A CHILLING EFFECT ON THE RELATIONSHIP BETWEEN THE STATE AND CITIZENSHIP

The most alarming impact of this type of surveillance is the impact it would have on the relationship between the citizens and their government. A citizen's "[a]wareness 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."[121] Furthermore, because the surveillance is digital, "the Government can store such records and efficiently mine them for information years into the future."[122] The presence of this technology and a privacy policy that allows the government unfettered discretion of when it chooses to use it and whom it chooses to use it on may "alter the relationship between citizen and government in a way that is inimical to democratic society."[123]

When privacy intrusions happen in cyberspace they are exponentially worse. Discreetly placed GPS receivers allowed the government to monitor the places defendants went in *Weaver* and *Jones*, and when they went there.[124] Social, political, religious, and other information could be gleaned from the agitated GPS date but it would be impossible to tell with whom the defendants met at any given location without visual surveillance to assist—the trips to a church could have been to meet a financial advisor, the doctor's office to rendezvous with a lover, and the cheap motel with an old friend at the bar across the street. In cyberspace, these observations are far more detailed.

The nature of data transmission in cyberspace means that when a defendant visits a web page, explicit information is available about what is contained on that page and when and where it was accessed.[125]

---

120. *Jones*, 132 S. Ct. at 956. (citing Illinois v. Lidster, 540 U.S. 419, 426 (2004)).

121. *Jones*, 132 S. Ct. at 956.

122. *Id.* at 955-56; *see* United States v. Pineda–Moreno, 617 F.3d 1120, 1124 (9th Cir. 2010).

123. *Jones*, 132 S. Ct. at 956 (citing United States v. Cuevas–Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)) (internal citations omitted).

124. *See generally* People v. Weaver, 909 N.E.2d 1195 (N.Y. 2009); United States v. Jones, 132 S. Ct. 945, 954-55 (2012).

125. When an individual accesses a website he is connecting to an IP address in cyberspace, in order to connect to that address his computer must send the specific information requested, the website, general parameters of the requesting computer and its location or IP address. These host computers log the time and date of the requests with the address the information is to be delivered to. *How do Computers Connect to Each Other over the Internet*, COMPUTER HOPE, http://www.computerhope.com/issues/ch001358.htm (last visited May 22, 2014).

Communications that are between multiple parties can be monitored, both the sender and receiver can be known, messages placed on chat rooms can be viewed, and each party who views the message can be identified and located by his IP address.[126] Cookies[127] can be retrieved by unauthorized web servers and can download financial information, user preferences, sites frequented, and more.[128] The NSA's PRISM program is a far greater intrusion than a GPS receiver surreptitiously placed on a car. In order to achieve the same level of surveillance in the real world that is possible online, a receiver would have to be placed on the individual himself, it would have to record the movements, communications, and interactions of its target, and even then it would fall short.

1. The Modern United States and Cyberspace

Today an unprecedented amount of interaction occurs on the Internet. A recent survey by the Pew Research Center states that eighty-five percent of American adults use the Internet to some degree and the number jumps to ninety-five percent for teens.[129] This means that of the almost 317 million Americans,[130] over 270 million of them have an online presence. Online activity varies and changes for adults.[131] The trends skew upward as the age of the person gets younger.[132] The new

126. Specific software exists exclusively for the purpose of identifying the physical location of a user by way of his IP address. *Geolocation Software*, WIKIPEDIA, http://en.wikipedia.org/wiki/IP_address_location (last visited May 22, 2014).

127. Cookies are small data files containing personally identifying information that can be retrieved by remote computers to ascertain the end user's personal information. *HTTP Cookie*, WIKIPEDIA, http://en.wikipedia.org/wiki/HTTP_cookie#cite_ref-1 (last visited May 22, 2014).

128. *Id.*

129. *Trend Data (Teens)*, PEW RESEARCH CTR., http://pewinternet.org/Static-Pages/Trend-Data-%28Teens%29/Whos-Online.aspx (last visited Oct. 18, 2013).

130. *U.S. and World Population Clock*, U.S. CENSUS BUREAU (Oct. 19, 2013, 4:15 PM), http://www.census.gov/popclock/.

131. The Pew Research Center surveyed adults about their Internet usage and concluded that ninety-one percent of adults use the Internet to search and learn; eighty-eight percent send and receive e-mail; seventy-eight percent learn about products and services and get their news online; seventy-one percent buy products; sixty-seven percent visit government websites; sixty-one percent bank and associate politically; and the activates go on and get increasingly intimate. *Trend Data (Adults): Online Activities Total*, PEW RESEARCH CTR., http://www.pewinternet.org/three-technology-revolutions/ (last visited Oct. 18, 2013).

132. *Compare id. with Trend Data (Teens)*, *supra* note 129.

generation is being exposed to technology and the Internet at an increasingly younger age, making it more likely and socially necessary to have a vast and varied online presence.

The NSA's PRISM program has the potential to monitor everything. The leaked PowerPoint slides indicate that PRISM can collect "email, chat (video, voice), videos, photos, stored data, VoIP [internet phone calls], file transfers, video conferencing, notifications of target activity – logins etc. . . . , online social networking details, and another category called 'special requests.'"[133] Hardware placed at service providers' strategic points allows for the real time collection and aggregation of virtually every online action into a single, searchable database that can be monitored and maintained indefinitely.[134] Recently, it was revealed that address books and buddy lists are monitored as well,[135] allowing the government to intimately monitor who an individual may know online and offline.

a. The Ubiquity of the Internet Allows for an Unprecedented Level of Surveillance

The level of intrusion is astonishing. Because of the amount of activity that takes place via the Internet it is hard to imagine how it has remained mostly unregulated. Applying common law principals, however, we are able to come to an understanding of the level of privacy protection that ought to be granted. Justice Sotomayor recognized a general expectation of privacy for online activity when she acknowledged that she "doubt[s] that people would accept without complaint the warrantless disclosure to the Government of a list of every web site they had visited in the last week, or month, or year."[136]

The argument has been made that because of the nature of the Internet, where Internet Service Providers collect miniscule amounts of data and advertisers monitor our search histories to better target products, there has been a forfeiture of most expectations of privacy.[137] This approach is no longer tenable in a world with such interconnected modes of communication and interaction. In order for Fourth Amendment protections to be forfeited, an individual must publish the

---

133. Charles Arthur, *NSA Scandal: what Data is Being Monitored and How Does it Work?*, THE GUARDIAN (Oct. 19, 2013), http://www.theguardian.com/world/2013/jun/07/nsa-prism-records-surveillance-questions.

134. *Id.*

135. Barton Gellman & Ashkan Soltani, *NSA Collects Millions of E-mail Address Books Globally*, WASH. POST (Oct. 18 2013), http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html.

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

137. *See generally* United States v. Forrester, 512 F.3d 500 (9th Cir. 2008).

information to the public at large or at least to a third party who is willing to cooperate with the government's investigation.[138] "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."[139] Information revealed during the course of Internet activities ought to remain private because an application of the *Katz*[140] analysis would indicate that people and society have an expectation that activity conducted digitally will remain largely private.

b. The Steps Taken are Indicative of Both an Expectation and Strong Desire to Maintain Privacy Online

The majority of Americans are without a strong expectation of privacy online.[141] A recent survey conducted before the revelation of the NSA's PRISM program indicated that eighty-five percent of Americans expected their communication to be intercepted and collected by various groups and organizations.[142] While many Americans believe they are being monitored by either the government or another actor, over half of all respondents believed the data collection will have negative personal impacts.[143] Additionally, the respondents voiced an overall distrust of the government's use of personal data collected.[144] Finally, the FTI survey indicates that practically every American has taken steps to

138. United States v. Meregildo, 883 F. Supp. 2d 523, 526 (S.D.N.Y. 2012) (applying privacy jurisprudence to Facebook and finding that while an individual may not publish his information at large, there is no guarantee that his "friends" will not).

139. *Jones*, 132 S. Ct. at 957.

140. Justice Harlan's concurrence established the framework for the infamous reasonable expectation test. His test looked to both the individuals' subjective expectation to privacy and society's general acceptance of that privacy. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

141. Memorandum from the FTI Consulting on Allstate/National Journal Heartland Monitor XVII Key Findings to Allstate (June 4, 2013), *available at* http://www.theheartlandvoice.com/wp-content/uploads/2013/06/KeyFindings.pdf.

142. The FTI survey was conducted from May 29 – June 2, 2013, four days before the first article revealing the existence of the PRISM program and the NSA's domestic surveillance and data collection programs were published. *Id.*

143. Over half of Americans surveyed believed that personal information collection is mostly negative and will have personal privacy risks. Moreover, one-third of Internet users have purchased software to protect their personal privacy, in addition to taking any number of steps to safeguard personally-identifiable information. *Id.*

144. Only forty-eight percent of respondents indicated that they trust the government and thirty-seven percent trust political parties and candidates when it comes to "responsibly using their information." *Id.*

ensure that they remain private online and are not among those whose data is collected.[145] A second survey indicates that a growing number of people are attempting to remain anonymous on the Internet and simultaneously ensure their privacy.[146] Approximately "86% of internet users have taken steps online to remove or mask their digital footprints—ranging from clearing cookies to encrypting their email, [and] 55% of internet users have taken steps to avoid observation by specific people, organizations, or the government."[147]

The gravamen of the two surveys is that while people recognize that they have a limited expectation of privacy on the Internet and in their online activities, they are not willing to simply submit to surveillance and constant data mining but instead are taking steps to take back their privacy and anonymity. An individual in a public place can "reasonably expect to enjoy such privacy as the [place] afford[s]."[148] Here, the public place is the Internet and while it does not afford much protection by way of privacy, an individual user can expect to be afforded any protection that may be available. Additionally, the court should measure an individual's subjective expectation of privacy by any "outward manifestations . . . [in] his dealings."[149] The above surveys show that while most people have a tenuous expectation of privacy when conducing themselves on the Internet,[150] they are also taking any and all possible steps to ensure that they remain secure and anonymous where possible. The courts should consider this behavior when evaluating the objective exception of privacy.

c. Applying Common Law to Uncommon Situations; How the Katz Test has been applied to Cyberspace and Emerging Technologies

The *Katz* test has two prongs that must be satisfied.[151] The objective expectation prong of privacy is an "expectation . . . that society is prepared to recognize as 'reasonable.'"[152] Therefore, the court has a duty to evaluate each situation de novo and attempt to discern what

145. *Id.*

146. Lee Rainie, Sara Kiesler, Ruogu Kang, & Mary Madden, *Anonymity, Privacy and Security Online*, PEW RESEARCH CTR. (Sept. 5, 2013), http://pewinternet.org/Reports/2013/Anonymity-online.aspx.

147. *Id.*

148. Reinhold v. Cnty. of York, Pa., 2012 WL 4104793, at *18 (M.D. Pa. Aug. 31, 2012) (quoting People v. Kalchik, 407 N.W.2d 627, 631 (Mich. App. 1987)).

149. Med. Lab. Mgmt. Consultants v. Am. Broad. Cos., Inc., 306 F.3d 806, 813 (9th Cir. 2002); *see* Kemp v. Block, 607 F. Supp. 1262, 1264 (D. Nev. 1985); Dow Chem. Co. v. United States, 749 F.2d 307, 312-13 (6th Cir. 1984).

150. *Allstate/National Journal*, *supra* note 141; *Rainie*, *supra* note 146.

151. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

152. *Id.*

society expects from a particular situation. Here in the digital age, the court must look to the given situation as it is and to what society as a whole expects from the Internet, and not what has been done in years past with outdated technology.

In *Forrester*, the Ninth Circuit examined an individual's expectation of privacy in websites visited and e-mail sender/recipients through collection of the IP addresses.[153] The Court concluded "that the surveillance techniques the government employed here are constitutionally indistinguishable from the use of a pen register that the Court approved in *Smith*."[154] The Court reasoned by analogy that the pen register used in *Smith* was indistinguishable from the surveillance techniques used here.[155] The Court, however, failed to conduct the necessary *Katz* analysis and examine society's reasonable expectation to privacy under this new technology.

The Ninth Circuit analogized the routing information contained in the header portion of an e-mail to the information written on an outside of an envelope.[156] However, an envelope is highly distinguishable from an e-mail message. A letter carried by the United States Postal Service is a real object that is physically handled and carried from point A to point B, while an e-mail is a digital file that at no point requires a real person to come in contact with the message.[157] An application of the objective portion[158] of the *Katz* test would indicate that because e-mail is drastically difference compared to physical mail and the methods used to monitor e-mail are fundamentally different than a pen register, the Ninth Circuit should have come to a different conclusion about what privacy interest society expects in e-mail. The Ninth Circuit's failure to conduct the proper analysis and examine society's expectation of privacy is an error that demands reexamination.

---

153. *See generally* United States v. Forrester, 512 F.3d 500 (9th Cir. 2008); *IP Address*, *supra* note 85 (defining IP address); *see* INFO. SCI. INST., DOD STANDARD INTERNET PROTOCOL, *supra* note 85; INFO. SCI. INST., INTERNET PROTOCOL – DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION, *supra* note 85.

154. *Forrester*, 512 F.3d at 510.

155. *Id.*; *see generally* Smith v. Maryland, 442 U.S. 735 (1979).

156. *Id.* at 511 (discussing that although the technologies are two different forms, the surveillance done by the federal government is essentially indistinguishable).

157. *Email*, WIKIPEDIA, http://en.wikipedia.org/wiki/Email (last visited May 22, 2014).

158. "The expectation be one that society is prepared to recognize as 'reasonable.'" Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

Furthermore, the information ascertainable by monitoring IP addresses is far more than the equivalent of sender and recipient information, like on the face of an envelope. Since specific IP addresses correspond to specific webpages, the information that can be gleaned from monitoring IP addresses is necessarily content based in nature.[159] The wrongful disclosure of video tape rental records was statutorily prohibited by law[160] because the legislature recognized:

> It is nobody's business what [individuals] watch on television or read or think about when they are home. [I]n an era of interactive television cables, the growth of computer checking and check-out counters, of security systems and telephones, all lodged together in computers, it would be relatively easy at some point to give a profile of a person and tell what they buy in a store, what kind of food they like, what sort of television programs they watch, who are some of the people they telephone. I think that is wrong. I think that really is Big Brother, and I think it is something that we have to guard against.[161]

The wanton monitoring of IP addresses is a far greater intrusion into the home than the disclosure of rental records. Monitoring the IP addresses one visits would be akin to monitoring the video rental records,[162] library rentals,[163] and real movements[164] of an individual.

Finally, society's expectation of privacy can be gleaned from legislature enacted in the wake of a court decision that seems to limit an individual's privacy rights.[165] "After the Supreme Court decided that

---

159. When the IP addresses of an individual's visits are known, it is possible to know what information is being sought, because an IP address necessarily corresponds to a specific webpage or location and by visiting the web address the content the individual sought can be easily ascertained.

160. 18 U.S.C § 2710 (2008).

161. S. REP. NO. 100-599, at 5.

162. Websites such as Netflix provide online streaming services allowing a subscriber to benefit from a vast online catalog of films, documentaries, and television shows without having to leave one's home to rent or return a VHS cassette. *Netflix,* WIKIPEDIA, http://en.wikipedia.org/wiki/Netflix (last visited May 22, 2014).

163. Google Books provides a vast selection of literary works scanned and available for reading, much like a local library but without having to face monetary penalties for an overdue book, because they are in digital form, a user can download and read at his leisure. *Google Books*, WIKIPEDIA, http://en.wikipedia.org/wiki/Google_Books (last visited May 22, 2014).

164. Because of the limitless nature of the Internet, an individual can watch videos, read literary works, shop, converse with friends, and explore countless other virtual places all of which, if were done in the real world, would take the person to a number of different physical locations.

165. "Looking at the past history of how the Fourth Amendment and current statutes protect personal information, it seems probable that Congress will pass legislation at some point in order to protect [privacy interest]." Adam Schira, Note, *Protecting Progress and Privacy: The Challenges of Smart Grid Implementation*, 6 ISJLP 629, 651 (2011).

bank records were not governed by the Fourth Amendment in *Miller*,[166] Congress responded by passing the Right to Financial Privacy Act. The ECPA also was a response to the Supreme Court decision in *Smith v. Maryland*[167] that permitted government access to telephone toll records."[168] This general pattern[169] by the legislature indicates that the people, whom Congress represents, are unwilling to accept the conclusion that there is not a general expectation of privacy in banking, telephone, or other records. Therefore the courts, when deciding Fourth Amendment cases, should assume that society's general expectation seems to always favor privacy.

d. There is a Reasonable Expectation to Privacy in Online Storage

In Orin Kerr's law review article, he acknowledged that the digital space utilized by individual users is often treated as if it was a physical place, but it is not.[170] Kerr recognized that many people treat their e-mail inbox or cloud storage account as if it were a physical location they have a property interest in, when in fact it is a third party's computer that is being used to temporarily house a "block of ones and zeroes."[171] However, Kerr was incorrect in his analysis; his conclusion that once an individual places information on another individual's network, the Fourth Amendment protections are greatly diminished is not in line with judicial precedent.

Although the courts have not yet addressed the issue of whether the Fourth Amendment's protections extend to e-mail stored in inboxes or other digital storage, they have looked at physical analogs. Courts have looked to other containers and storage mediums to determine their Fourth Amendment protections and found that as long as the three prong test is satisfied, there can and should be a presumed privacy expectation.

---

166. *See generally* United States v. Miller, 425 U.S. 435 (1976).

167. *See generally* Smith v. Maryland, 442 U.S. 735 (1979).

168. Schira, *supra* note 165, at 651-52.

169. S. REP. NO. 100-599, at 2-4 (1988).

170. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1210 (2004) (noting that many users may treat online storage as a physical location because the nature of cyberspace means that it is not in fact a "real" space that users can exercise any control over).

171. *Id*.

The test is outlined in *United States v. Salinas-Cano*[172] and looks to: (1) is it the type of container that would historically command a high degree of privacy;[173] (2) has the true owner taken sufficient precautions to indicate his expectation of privacy in the container's contents;[174] and (3) what is the third party's[175] interest in the container.[176] An application of the *Salinas-Cano* test to the contents of an individual's digital storage "container" would indicate that the owner does in fact have a privacy expectation in the contents therein.

Because e-mail has been analogized to physical postal mail[177] and has been granted protections equal to its physical counterpart, it follows that the digital inbox should be granted the same privacy interest as the physical mailbox. The physical mailbox, and its digital counterpart, is certainly the type of container that an individual would have a strong privacy interest in. Furthermore, the digital inbox functions both as a destination for incoming e-mail, like the physical mailbox, and as a storage unit for opened e-mail, like a desk drawer or filing cabinet; therefore, the privacy interest an individual has in an e-mail inbox should be significantly greater than the traditional mailbox. Additionally, online storage is analogous to a suitcase or other storage locker that a person may be able to easily travel with or store with a trusted third party. Online storage provides storage for data and documents that can be secured via encryption and password protections, but still accessible from any location.

Regarding the second prong, precautions by the owner are indicative of a privacy expectation, as in the case of an e-mail inbox, far greater than the physical analog. E-mail subscribers need a unique password, akin to a key, in order to access their inbox. This is more than is commonly found on a mailbox and more similar to a key used to access a storage locker or safety deposit box. Although it could be argued that the precautions taken by a user are not unique, and therefore do not warrant any significant privacy interest, the argument would fail because the nature of consumer e-mail typically only allows for protection via password authentication and an individual can only be expected to take what precautions are available.

---

172. United States v. Salinas-Cano, 959 F.2d 861, 864 (1992).

173. "First, certain types of containers historically command a high degree of privacy, and the type of container at issue is therefore an important consideration." *Salinas-Cano*, 959 F.2d at 864.

174. "A second factor is the precautions taken by the owner to manifest his subjective expectation of privacy." *Id.*

175. *Id.*

176. *Id.*

177. United States v. Warshak, 631 F.3d 266, 285-86 (6th Cir. 2010).

Finally, what interest does the party consenting to the search have in the container's contents? Consider a government entity attempting to gain access to an e-mail account or other online storage facility. The Sixth Circuit in *Garcia v. Dykstra* clarified the third prong of the analysis.[178] It has been established that a third party may consent to a search if there is authority to give such permission however:

> even when the invitation to search is accompanied by an explicit assertion that the person has authority to consent . . . If the facts available to the officer would not support the belief "that the consenting party had authority over the premises," then "warrantless entry without further inquiry is unlawful . . ."[179]

Therefore a government agency attempting to access an individual's e-mail inbox or online storage must have a reasonable belief that the party authorizing the access has the authority to do so.

Law enforcement should not be permitted to gain authorization through a service provider's consent. A cursory glance at the relationship between a service provider, such as Google, Yahoo!, Verizon, or AT&T and an individual subscriber would indicate that it is highly unlikely that a service provider has been given explicit authority to authorize any access. Service providers have no interest in the contents of an individual's inbox and are unlikely to suffer any direct consequence from turning it over to a government agency, any loss or legal repercussions are likely to be the customer's and the customer's alone. Because a government representative cannot form a reasonable belief that the corporation has been given explicit authorization to access a specific individual's data, it should be strictly prohibited from gaining access to an e-mail account without either explicit user authorization or a court order.

e. There is an Objective Expectation to Privacy in Emerging Technology and Telecommunications

Online activity is typically targeted communications with other individuals or webpages. This type of closed and private communication cannot be said to have forfeited any reasonable expectation to privacy because other digital entities have handled the transmissions—it is not reasonable to expect that a telephone operator would continue to listen

178. *See generally* Garcia v. Dykstra, 260 Fed App'x 887 (6th Cir. 2008).
179. *Id.* at 900.

in on a private phone call once she has connected both parties.[180] "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."[181]

Digital communications such as e-mail, instant messages, VoIP calls, and video chats are all deserving of at least the same protection that was afforded to their analog counterparts. "As some forms of communication begin to diminish, the Fourth Amendment must recognize and protect nascent ones that arise."[182] The *Warshak* Court stated:

> Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection. . . . It follows that email requires strong protection under the Fourth Amendment; otherwise, the Fourth Amendment would prove an ineffective guardian of private communication, an essential purpose it has long been recognized to serve.[183]

This recognition that e-mail plays an increasing role in modern society cannot be ignored. In *Katz*, the Court recognized the increasing role the public telephone played at the time and recognized the importance of protecting the privacy interest in it.[184] Today the public telephone has been largely supplanted by the mobile phone but the principal remains the same. As new forms of technology play an increasing role in daily life and more people begin to depend on those modes of communication, the Court must take steps to ensure their security. "It goes without saying that like the telephone earlier in our history, e-mail is an ever-increasing mode of private communication, and protecting shared communications through this medium is as important to Fourth Amendment principles today as protecting telephone conversations has been in the past."[185] It is incongruous to say that the protection afforded to e-mail should not be extended to other modern avenues of communication; a person has no less of an expectation of privacy on a digital video conference or a private instant message session than he would on a telephone or when sending an e-mail. Therefore the precautions that are in place for both e-mail and more traditional forms of communication ought to be extended to new and emerging technologies.

---

180. In *Smith v. Maryland*, the Supreme Court held constitutional the use of a pen register, which recorded only the telephone numbers dialed; the Court recognized that it was a far less intrusive search then the one in *Katz* where officers recorded the content of the telephone call. Smith v. Maryland, 442 U.S. 735, 741 (1979).

181. United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010).

182. *Id.* at 285-86.

183. *Id.*; *see also* City of Ontario v. Quon, 560 U.S. 746 (2010).

184. Katz v. United States, 389 U.S. 347, 352 (1967).

185. Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007).

f. The Technology Necessary to Conduct Such Surveillance is Neither Publically Available nor is the Information Ascertained Vague Enough to Survive Analysis under Kyllo

The digital invasion of privacy is exponentially worse than in either the *Jones* or *Weaver* cases, and deserve the same protection or more. Digital communications cannot be said to be akin to driving down a public street where one may be readily observed by members of the public, as most members of the public lack access to sophisticated telecommunications and decryption equipment that would allow them to intercept and view digital transmissions. In *Kyllo*, the Court looked to the availability to the public of a thermal imaging device that was able to peer through the walls of a home and provide a general map of the temperature of the home.[186] The Court concluded that this device was not in general use by the public and produced details of a home that would otherwise be unknown and therefore a search had occurred.[187]

Applying the analytical principals in *Kyllo*, we must consider: (1) is the technology necessary to intercept Internet traffic and conduct digital surveillance "in general public use"[188] such that people should not have an expectation of privacy; and (2) does the surveillance provide "details . . . that would previously have been unknowable without . . . intrusion?"[189] Digital surveillance and data collection fails on both prongs of this analysis.

First, while there is no statistical indication that the sophisticated technology and expertise that is necessary to actively intercept Internet transmissions and decipher their content is widely available at present or in use by the general public, it seems like a safe assumption that the average user is not capable of conducting such surveillance. The personnel working on clandestine projects, like PRISM, are highly trained and educated in order to circumvent security measures generally in place. This specialized knowledge requires years of education and is far beyond what the typical Internet user possesses. Furthermore, the software developed to crack encryptions protecting global commerce and communications has reportedly cost billions of dollars and over a decade to develop.[190] The second prong of a *Kyllo* analysis asks whether the

186. Kyllo v. United States, 533 U.S. 27, 29 (2001).

187. *Id.* at 39-40.

188. *Id.* at 34.

189. *Id.* at 40.

190. Grant Gross*, Report: NSA Defeats Many Encryption Efforts*, PC WORLD (Sept. 5, 2013), http://www.pcworld.com/article/2048222/report-nsa-defeats-many-encryption-

information is beyond what can be gleaned without intrusion. This analysis seems almost absurd. Of course the information collected from in-depth digital surveillance is more significant than what can be gathered by simply observing an individual. It is impossible to know what an individual sitting inside his home, or any other place, is doing on his computer without either a direct line of sight to his computer screen or monitoring his Internet activity remotely. The results from data collection conducted remotely would certainly net results that would otherwise require court approval to obtain. Because the technology and expertise required to conduct panoptic surveillance, and the information gathered from such surveillance is so incredibly intimate it is obvious that the PRISM program would not survive scrutiny under *Kyllo* analysis and therefore must be prohibited.

B. PANOPTIC SURVEILLANCE WILL CHILL FREE EXPRESSION, ASSOCIATION, AND QUASH THE AMERICAN SPIRIT

The impact of such pervasive surveillance is incredible. Justice Sotomayor in her *Jones* concurrence[191] recognized that trespass based privacy jurisprudence was no longer tenable in a post-Internet era,[192] stating:

> [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. 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.[193]

Justice Sotomayor continued, arguing regardless of the expectation, there ought to remain a privacy interest for information voluntarily

---

efforts.html (discussing that "[t]he NSA has cracked much of the encryption that protects global commerce, banking, trade secrets, and medical records, according to the report, which cites documents leaked by former NSA contractor Edward Snowden. The NSA has invested billions of dollars in efforts to defeat encryption since 2000, according to the report").

191. United States v. Jones, 132 S. Ct. 945, 954-57 (2012).

192. *Id.* at 955; *see* United States v. Pineda–Moreno, 617 F.3d 1120, 1125 (9th Cir. 2010) (Kozinski, J., dissenting from denial of rehearing en banc).

> [P]hysical intrusion is now unnecessary to many forms of surveillance. With increasing regularity, the Government will be capable of duplicating the monitoring undertaken in this case by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones. . . . In cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance. As Justice Alito incisively observes, the same technological advances that have made possible nontrespassory surveillance techniques will also affect the *Katz* test by shaping the evolution of societal privacy expectations. *Id.*

193. *Jones*, 132 S. Ct. at 957; *see* Smith v. Maryland, 442 U.S. 735, 742 (1979); *see also* United States v. Miller, 425 U.S. 435, 443 (1976).

disclosed for a limited purpose.[194] Additionally, Sotomayor doubted "that people would accept without complaint, the warrantless disclosure to the Government of a list of every website they had visited in the last week, or month, or year."[195]

"Awareness that the Government may be watching chills associational and expressive freedoms."[196] Justice Sotomayor's thoughts are echoed again and again by academics and scholars.[197] As expressed by Ken D. Kumayama in a law review article:

> If every word someone types can be traced back to that person, people will likely choose their words with greater care. While more thoughtful communication may not be a bad thing, knowledge of ongoing surveillance will inevitably result in self-censorship. The fact that an individual's words, once uttered, may be chiseled onto the Internet's memory—perhaps for all time—will likely give some individuals added pause. . . . The danger of self-censorship applies equally to expressive activities as it does to expression through words.[198]

For example the troubled teen may be less likely to seek help if he knows that one day his moment of weakness could be thrust into the spotlight. The depressed parent may be less likely to seek comfort in her faith if she knows the government is watching Muslims. The party politician may be less willing to discuss alternative policy positions, even in private, if he knows disloyalty could destroy his career.

Additionally, with the government monitoring every move made in the digital realm, it is unlikely that individuals will be motivated to study and research controversial topics for fear of federal reproach, as indicated by Kumayama's article. Kumayama acknowledges a "tradition of anonymous exploration" as a necessity to free thought and the Internet is a major thoroughfare for information and ideas that, if it were subject to constant surveillance, it would have a chilling effect on the access to information and popular ideas.[199]

---

194. *Jones*, 132 S. Ct. at 957; *see Smith*, 442 U.S. at 749 (Marshall, J., dissenting).

195. *Jones*, 132 S. Ct. at 957.

196. *Id.* at 956.

197. Stan Karas, *Privacy, Identity, Databases*, 52 AM. U. L. REV. 393, 412-13 (2002). ("A frequently iterated rationale for restricting collection of consumer data is that it creates a surveillance society and panoptic effects. In monitoring consumers' activities, this surveillance society encourages self-censorship and generally impedes the path to self-realization.").

198. Ken D. Kumayama, Note, *A Right to Pseudonymity*, 51 ARIZ. L. REV. 427, 439 (2009).

199. *Id.* at 439-40.

1. Surveillance will Discourage Social Interaction and Digital Association

If the populace is subjected to unfettered government observation of their online activities, it is unlikely that many people will feel comfortable building and maintaining digital social relationships. Currently, sixty-seven percent of adults are members of online social networking websites.[200] These websites serve a myriad of purposes: Facebook serves as a social conduit for a younger generation; LinkedIn works to highlight professional relationships among colleagues, facilitating professional networking; and dozens of others cater to special interests and individuals who are passionate about them. The U.S. Supreme Court "has recognized the vital relationship between freedom to associate and privacy in one's associations . . . [w]hen referring to the varied forms of governmental action which might interfere with freedom of assembly."[201] The active monitoring of social networking sites designed to foster relationships between like-minded people would surely infringe upon an individual's freedom of association.[202]

If the government were to monitor Facebook and other social networking sites, it would essentially be requiring every user or visitor to such a website to disclose his or her affiliation to a variety of special interest groups. This disclosure flies in the face of the principle restated in *NAACP v. Alabama*.[203] The argument that these meetings and affiliations are made known because of Internet activity is unconvincing; it would liken visiting a website in the privacy of one's own home to attending a public meeting in a conspicuous location. If this were the case it would certainly deter membership from groups that have an unpopular or stigmatized belief system. For example, it would deter those with substance abuse problems from seeking counseling; it would deter closeted homosexuals from seeking support from a community of their peers; it would deter membership to any socially stigmatized group that has found support online.

While courts have routinely found that information posted to social media sites has been published to third parties and therefore has abandoned Fourth Amendment privacy protection,[204] the surveillance that is being conducted by the NSA is far more intrusive. Monitoring and

---

200. *Trend Data (Adults)*, *supra* note 131.

201. Nat'l Ass'n for Advancement of Colored People v. State of Ala. ex rel. Patterson, 357 U.S. 449, 462 (1958) (citing Am. Commc'ns Ass'n v. Douds, 339 U.S. 382, 402 (1950)).

202. The freedom of association implications are far too numerous to consider in this limited context and thus will be limited to the brief preceding consideration.

203. *Nat'l Ass'n for Advancement of Colored People,* 357 U.S. at 449.

204. *See generally* Ann K. Wooster, Annotation, *Expectation of Privacy in and Discovery of Social Networking Web Site Postings and Communication*, 88 A.L.R. 319 (6th ed. 2013).

logging every visitor to a given webpage would be akin to placing a federal agent at the threshold of countless venues in order to take diligent notes of who enters and what she does once inside. Various courts have held that when information is published publicly via Facebook or another social media site, there can be no reasonable expectation of privacy and while some courts have found that privacy settings and other measures may lend themselves to some privacy exception,[205] those opinions are the exception and not the rule. The surveillance conducted here monitors which users visit a specific page; the activity monitored is the completely passive viewing of a webpage, where users could reasonably conclude that they have acted anonymously.[206] This is fundamentally different from the active posting or participation of a discussion on an online forum where the comments can be seen by any member of the general public who happens across that web address. Because the monitoring of social media websites is so destructive, essentially chilling free association, it must not be allowed to continue. Otherwise, websites of this nature need to be exempted from persistent government surveillance.

2. Surveillance will beget Censorship and the Loss of the Inviolate Personality Leading to the Rise of a Dystopia

Supreme Court Justice Louis Brandeis and Samuel Warren advocated for more than just the ability to retreat into one's self and be free from encroachment by the government or press.[207] They advocated for the protection of one's self, one's identity, what was called one's "inviolate personality."[208] Their position was that the law ought to vest some protection beyond traditional property and tort remedies from trespass into a man's most private thoughts even when expressed in some tangible medium absent injury.[209] The law, they believed, should be crafted to protect the "private life, habits, acts, and relations of an individual, and have no legitimate connection with his fitness for a public office . . . and have no legitimate relation to or bearing upon any act done by him

205. *Id.* at § 28.

206. An individual would not reasonably expect that she has been monitored accessing a benign website and would conclude that she has visited that page anonymously.

207. Warren & Brandeis, *supra* note 18, at 196. (stating "the press is overstepping in every direction the obvious bounds of propriety and of decency").

208. *Id.* at 205 (discussing that the inviolate personality was described as an expression of a man's sentiments, emotions, feelings, etc.).

209. *Id.* at 196.

in a public or quasi public capacity."[210] In an earlier era, the right to be let alone was sufficient to protect that inviolate personality. Today, man must be free to learn, conduct business, and form new social bonds without intrusion.

The net result of omnipresent government monitoring is the stifling of the individual. Warren and Brandeis advocated for the protection of an individual's inviolate personality—"the right to one's personality"[211]—but in 2013, the Information Age, it is no longer possible for an individual to become fully self-aware by being "left alone." "Information privacy is a necessary precondition for the formation of one's identity. . . . Information privacy allows for greater freedom of action and interaction by protecting individuals from being misdefined and judged out of context . . . "[212]

It was necessary in the "fast paced" 1890s for a man to be free to retreat from the world to reflect inwards and discern his identity for himself. In the hyper paced twenty-first century, it is not enough anymore for a man to simply look inwards, he must be free to explore the world and learn and experience a range of information, he must be free to explore taboo topics and understand unpopular viewpoints before coming to a decision about his individual morals.

George Orwell's dystopian novel *1984*[213] is a favorite among scholars who wish to emphasize the impact an overbearing government can have on its population, so much so that the analogy borders on cliché. Unfortunately, however, it is illustrative of the result of an over surveyed population. The characters of *1984* were the subjects of constant surveillance and as a result the population was stagnant, many were unaware of the possibility of alternative viewpoints and those that were too terrified of reproach to do anything. The result was a population that had been intellectually castrated by government monitoring and self-censorship.[214]

The NSA's surveillance programs, while not as omnipresent as Orwell's infamous Big Brother, is certainly close. The programs' reach into every facet of digital life, masquerading as a security measure, will pay particularly close attention to members of society on the fringe:

---

210. *Id.* at 216.

211. *Id.* at 207.

212. Kumayama, *supra* note 198.

213. GEORGE ORWELL, 1984 (1948).

214. *Id.* Orwell's 1984 told the story of life in a world where government surveillance was constant and complete. The population's every move was monitored at any given moment and those who behaved incongruously were subject to government reprisal, typically in the form of torture and execution. As a result the educated population was no longer intellectually free to explore different points of view or even past events without fear of being subject to reconditioning and the uneducated paroles were unaware of anything other than the propaganda produced by the state. *Id.*

politically, socially, and religiously as other non-digital programs have.[215] This will undoubtedly result in the curtailing of those viewpoints, either through government action or self-censorship. To insulate the population from government encroachment, a modern definition of privacy must be adopted. Such a definition must necessarily be one that protects an individual's ability to interact online and explore taboo topics in order to develop his own individual identity.

C. DUE PROCESS CONSIDERATIONS[216]

The Fourth Amendment explicitly allows for an exception from the protection of an individual's right to privacy "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[217] However, this exception requires that before a person can be subject to any invasion of his privacy, certain Due Process considerations are afforded.[218] The statute that authorizes the NSA's surveillance initiative, PRISM,[219] allows for a broader collection of information with a diminished standard of authorization. Essentially, the statute makes an end around the established due process paradigm mandated to initiate surveillance of an individual.[220]

---

215. Conor Friedersdorf, *The Horrifying Effects of NYPD Ethnic Profiling on Innocent Muslim Americans*, THE ATLANTIC (Mar. 28, 2013), http://www.theatlantic.com/politics/archive/2013/03/the-horrifying-effects-of-nypd-ethnic-profiling-on-innocent-muslim-americans/274434/.

216. Obviously there are a range of other due process implications and considerations to be made concerning the NSA's surveillance program and its statutory authorization. Those considerations however, are beyond the scope of this Comment and to attempt to discuss them here in this limited space would only do a disservice.

217. U.S. CONST. amend. IV.

218. U.S. CONST. amend. IV (requiring "probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized" before a warrant can be issued).

219. 50 U.S.C. § 1881 (2008) (Section 702 of the Foreign Intelligence Surveillance Act of 1974's 2008 Amendments).

220. Amnesty Int'l USA v. Clapper, 638 F.3d 118, 125-26 (2d Cir. 2011) (highlighting the differences between the pre- and post-FAA upon the government's ability to conduct clandestine surveillance, the procedures to be followed before surveillance is conducted, and the courts' ability to oversee such surveillance).

III. CONCLUSION

A. A MODERN EXPECTATION OF PRIVACY FOR A MODERN SOCIETY

The omnipresence of the Internet and its necessity to everyday life means that traditional notions of privacy vested in property are becoming increasingly antiquated. In their law review article, Warren and Brandeis advocated for a general privacy right that was not tied to property interests, but rather they chose to advocate instead for an individual's right to his personality.[221] Over time the Court made strides in expanding privacy interests from those based strictly on property to those based on society's general expectation.[222]

Today, however, the right to be let alone is no longer sufficient to safeguard privacy interest. Daily life requires an increasing amount of intermingling between people and the Internet, Justice Sotomayor recognized that modern society requires individuals to disclose a great deal of personal information in order to conduct ordinary business and routine tasks.[223] In *Jones*, the Court was required to "apply the Fourth Amendment's prohibition of unreasonable searches and seizures to a 21st-century surveillance technique. . . . Ironically, the Court . . . chose to decide this case based on 18th-century tort law."[224] However, both Justices Sotomayor[225] and Alito[226] wrote concurring opinions in which they recognized and stated that the reliance on property interests to secure privacy rights was no longer sufficient.

While privacy jurisprudence has created several recognized "zones of privacy"[227] and developed a test to determine the reasonableness of an expectation to privacy,[228] these are no longer enough to protect

---

221. Warren & Brandeis, *supra* note 18, at 207 (discussing "a part of the more general right to the immunity of the person, the right to one's personality").

222. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

223. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

224. *Id.* at 957 (Alito, J., concurring).

225. *Id.* at 955 (Sotomayor, J., concurring) (noting that because physical trespass is no longer necessary for many forms of surveillance, the government may be able to utilize already available factory or user installed tools to monitor smartphones or other digital devices).

226. *Id.* at 963 (Alito, J., concurring) (discussing the recent emergence of many digital devices over the past decade (such as CCTVs, smartphones, automated toll roads), it is becoming increasingly easy to survey the general population; additionally, the advances in personal technology and the ability and availability of such devices is coloring individuals' privacy expectations).

227. *See* Roe v. Wade, 410 U.S. 113, 152 (1973) ("[T]he Court has recognized that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution."); *see also* Griswold v. Connecticut, 381 U.S. 479, 485-86 (1965) (recognizing a zone of privacy within "marital bedrooms" and "the marriage relationship").

228. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

digital privacy interest. Individuals need to be given the right to control third party access to their own identifying information. Judge Posner recognizes when individuals "decry [a] lack of privacy, what they want . . . is mainly something quite different from seclusion; they want more power to conceal information about themselves that others might use to their disadvantage."[229] This sentiment is perfectly applicable to modern privacy concerns where the government is able to collect and aggregate data to use against its citizens. In 2013, individuals are constantly involved in an incessant exchange of information via the Internet. Individuals disclose banking information, contact information, associations, *inter alia*, to third party corporate entities for the purpose of carrying out a transaction or utilizing a service. They exchange photographs, communications, feelings, and emotions with friends and family via "private"[230] web services. Individuals necessarily need to be given greater latitude in deciding who has what access to personal information. The traditional notion that once information is put into the world, it is devoid of a privacy interest is not tenable going forward.

Moving forward, privacy analysis must be sensitive to the idea that though individuals have disclosed select information to a specific third party in order to achieve a specific end they have not abandoned all privacy interest. Obviously, exceptions exist. If an individual published a photograph or statement to the general public, via a public Twitter account or open Facebook wall post, then it is without doubt that he has forfeited any reasonable expectation of privacy. If, however, he has taken all available steps to ensure that his exchanges with family and friends have been kept private then there is a subjective expectation of privacy, and that is an expectation that is generally recognized by society. The courts must consider an individual's outward manifestation of his expectation of privacy when conducting privacy analysis instead of simply deeming a privacy interest forfeited when a third party is involved. Individuals should be able to dictate the terms of use of their own information, as long as they have taken reasonable steps to keep that information private and the *Katz* test is satisfied; it cannot be said that a necessary disclosure to a third party waives all rights to privacy. People after all have a default expectation of privacy in their affairs and personal information.

---

229. Karas, *supra* note 197, at 411.

230. In this context "private" refers to commercially offered services that, while available to the general public, require a username and password to access and authorization from the initial party for third party access.

B. SOCIETY'S EXPECTATIONS AS A LIMIT TO THE NSA'S AUTHORITY

While personally I would advocate for the complete decommission of the PRISM and XKeyscore programs' domestic capabilities, I am sensitive to the security issues posed in the twenty-first century. With that said, any surveillance conducted must be sensitive to a modern definition of privacy, obviously I have a preference for the afore-described definition, but regardless any definition will have to give way to proper due process. The due process standards outlined in Section 702 of the 2008 FISA Amendments[231] are insufficient. The statutory paradigm outlined in Section 702 is contrary to the standard articulated by our founding fathers in the Fourth Amendment to the Constitution.[232] Failure to adhere to the time tested standards applicable to all other modes of search and seizure will result in a populace that grows increasingly fearful of their government.

The Supreme Court already stated in *Kyllo* that the use of technology to conduct clandestine surveillance is limited by two factors, applying that test to the current NSA programs clearly indicates that the surveillance being conducted is far afield from what is permissible. Though some of the surveillance being conducted is done by observing new and emerging forms of communication, those methods are not absent privacy protection, existing privacy laws must necessarily extend to these burgeoning forms of communication. Furthermore, while some of these programs are operating in tandem with various service providers, their consent is not sufficient to overcome the privacy expectation that individuals have in their various online accounts.

Big Brother's looming presence may be a cliché metaphor to express concerns over an omnipresent government, but it is more than a knee jerk reaction to another government program. Left unchecked, the current surveillance mechanism could penetrate even further into society. With the intermingling of technology into every facet of daily life it may be the case that no area of life is untouched by the Internet and therefore subject to the NSA's dominion. The above definition of privacy would allow government actors to use any information that is freely available in cyberspace while still insulating the individuals from unreasonable and unauthorized probes into their private activities without proper judicial leave.

---

231. 50 U.S.C. § 1881 (2008).

232. U.S. CONST. amend. IV (providing that "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").