Texas A&M Law Review

Volume 2 | Issue 4 Article 8

2015

National Security, Narcissism, Voyeurism, and Kyllo: How Intelligence Programs and Social Norms are Affecting the Fourth Amendment

Adam R. Pearlman

Erick S. Lee

NATIONAL SECURITY, NARCISSISM, VOYEURISM, AND *KYLLO*: HOW INTELLIGENCE PROGRAMS AND SOCIAL NORMS ARE AFFECTING THE FOURTH AMENDMENT†

By: Adam R. Pearlman & Erick S. Lee***

TABLE OF CONTENTS

† The public news reports of alleged government law enforcement and intelligence programs discussed herein are not cited for their truth or accuracy, but rather for their potential effect on public perceptions, expectations, and suppositions about technological capabilities and operations. The Authors have not further investigated and do not have any personal knowledge of the alleged programs or activities beyond what is contained in the cited news media reports, and intend neither to affirm nor deny any of the facts therein.

* Associate Deputy General Counsel, United States Department of Defense; Special Advisor, International and National Security Law Practice Group, The Federalist Society for Law and Public Policy Studies; Editor-in-Chief, UNVEILING THE SECRET COURT: THE OPINIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (forthcoming, 2016). B.A., UCLA; J.D., The George Washington University Law School; M.S.S.I., National Intelligence University. Special thanks to the *Texas A&M Law Review* editorial staff for their work on this Article, and for their patience. This Article is dedicated to Charlie, with hopes that these issues may one day be sorted out with a proper balance struck, and that you remain safe and free. The views expressed in this Article are those of the author(s) alone and do not necessarily reflect the official policy or position of the Department of Defense or the U.S. Government.

** Erick Lee is an attorney with a background in intellectual property and technology. B.S., UCLA; J.D., Whittier Law School; LL.M., Intellectual Property Law, George Washington University Law School.

I. INTRODUCTION

Advancements in technology, coupled with society's ever-increasing reliance on and acceptance of computer-based and online social media networking websites, have created a number of new legal quandaries. For instance, the 2007 tragedy surrounding the suicide death of Missouri teen Megan Meier[1] renewed debate as to whether there should be an expansion of the boundaries of tort law to make liable people's actions on social media websites.[2] Meier's case also revived debate regarding the propriety of traditional civil procedure notions of venue and personal jurisdiction concerning where to litigate matters involving alleged wrongdoing in cyberspace.[3]

Other areas of the law have created similar *sui generis* legal concerns in response to the increased popularity and infiltration of social media into modern life. Employers have actively begun investigating prospective employees' Facebook and other social media profiles and pages in search of any objectionable material that would raise any

1. *See, e.g.*, Christopher Maag, *A Hoax Turned Fatal Draws Anger but No Charges*, N.Y. TIMES, Nov. 28, 2007, at A23; Tamara Jones, *A Deadly Web of Deceit; A Teen's Online 'Friend' Proved False, and Cyber-Vigilantes Are Avenging Her*, WASH. POST, Jan. 10, 2008, at C1. Federal prosecutors alleged that Lori Drew, the mother of another student at Megan Meier's school, was behind the "flirtatious Internet chats" between Meier, and who Meier thought was a sixteen year old boy named Josh Evans. *See* William M. Welch, *Woman Indicted In 'Cyberbullying' Case; Federal Prosecutors Say MySpace Hoax Led to Death of Teenage Girl*, USA TODAY, May 16, 2008, at 3A. Drew created the account and communicated with Meier, ultimately sending hurtful messages to the young woman that were alleged to have pushed Meier to suicide. *See* Jennifer Steinhauer, *Verdict in MySpace Suicide Case*, NY TIMES, Nov. 26, 2008, *available at* http://www.nytimes.com/2008/11/27/us/27myspace.html.

2. *See, e.g.*, Jacqueline D. Lipton, *Combating Cyber-Victimization*, 26 BERK. TECH. L.J. 1103, 1129–37 (2011); Megan Rowan, *When Words Hurt More than "Sticks and Stones": Why New York State Needs Cyberbullying Legislation*, 22 ALB. L.J. SCI. & TECH. 645, 648–49 (2012); Matthew C. Ruedy, *Repercussions of a MySpace Teen Suicide: Should Anti-Cyberbullying Laws be Created?*, 9 N.C. J.L. & TECH 323 (2007); Darryn Cathryn Beckstrom, *State Legislation Mandating School Cyberbullying Policies and the Potential Threat to Students' Free Speech Rights*, 33 VT. L. REV. 283, 285–86 (2008–2009); Andrew M. Henderson, *High-Tech Words Do Hurt: A Modern Makeover Expands Missouri's Harassment Law to Include Electronic Communications*, 74 MO. L. REV. 379, 380 (2009); Kevin Turbert, *Faceless Bullies: Legislative and Judicial Responses to Cyberbullying*, 33 SETON HALL LEGIS. J. 651 (2008–2009); Nicholas R. Johnson, *Recent Development: "I Agree" to Criminal Liability: Lori Drew's Prosecution Under §1030(A)(2)(C) of the Computer Fraud and Abuse Act, and Why Every Internet User Should Care*, 2009 U. ILL. J.L. TECH. & POL'Y 561 (2009).

3. Federal prosecutors indicted Lori Drew with violating the Computer Fraud and Abuse Act, with the case heard in the Central District of California, even though Drew and Meier both lived in Missouri. *See* Indictment at 9, United States v. Drew, No. CR-08-582-GW (C.D. Cal. Feb. 2008), *available at* http://fl1.findlaw.com/news.findlaw.com/nytimes/docs/cyberlaw/usdrew51508ind.pdf). The prosecution believed that such venue was appropriate, because MySpace's servers which hosted the communications were located in Los Angeles, CA. *See* Steinhauer, *supra* note 1.

concerns about the employees' suitability.[4] That employees have been fired as a result of their social media postings, regardless of whether such postings were written about their employer, has led to debates concerning the legality of such employment actions.[5] In the intellectual property field, imposters have created pages purporting to be the "official" profile of unwitting companies or public figures, even though the companies or public figures often have no affiliation whatsoever with the pages.[6] Such actions may trigger

4. *See e.g.,* Rachel Ryan, *Yes, Employers Will Check Your Facebook Before Offering You a Job*, HUFFINGTON POST (Mar. 4, 2013), http://www.huffingtonpost.com/rachel-ryan/hiring-facebook_b_2795047.html. Many employees have been fired after their employers discovered social media content and postings that were controversial or objectionable. *See e.g.* Ismat Sarah Mangla, *Fired for Facebook: Don't Let it Happen to you*, TIME (Apr. 21, 2009), http://time.com/money/2792542/fired-for-facebook-dont-let-it-happen-to-you/fired-for-facebook-dont-let-it-happen-to-you/; Mike Simpson, *Social Networking Nightmares; Cyberspeak no Evil*, NATIONAL EDUCATION ASSOCIATION, http://www.nea.org/home/38324.htm (last visited May 1, 2015); Victor Luckerson, *Nordstrom Employee Fired Over Racially Charged Facebook Post*, TIME (Dec. 16, 2014), http://time.com/3636220/nordstrom-aaron-hodges/. The advice provided by many Career Offices at universities in recent years have warned students and graduates to avoid posting anything that may be construed as controversial or objectionable on their respective Facebook pages for fear that they may be viewed by potential employers. *See e.g.,* Kristen Uhl Hulse, *A Guide to e-Professionalism for Attorneys: Five Steps to Create and Maintain a Professional Online Persona*, GEORGETOWN UNIVERSITY LAW CENTER, https://www.law.georgetown.edu/academics/academic-programs/graduate-programs/careers/multimedia-library/career-toolbox/upload/eProfessionalism.pdf (last visited May 1, 2015). Anecdotal evidence has been reported that students have lost employment opportunities as a result of photographs and postings that portrayed the candidate in a negative light. *See, e.g.*, Joseph P. Kahn, *E-trails of trouble*, BOSTON GLOBE (Feb. 14, 2013), http://www.boston.com/jobs/2013/02/14/college-seniors-list-this-spring-complete-degree-credits-clean-online-profile/Nb0WYOg4ZpzlC00KclKitO/story.html (relating the story of a Boston law firm that rescinded an offer to a prospective employee after discovering a Facebook picture of the candidate at a party with illegal drugs visible).

5. *See* Melanie Trottman, *For Angry Employees, Legal Cover for Rants*, WALL ST. J. (Dec. 2, 2011), http://www.wsj.com/articles/SB10001424052970203710704577049822809710332 (reporting how the National Labor Relations Board has often received and acted on complaints by employees fired as a result of social media activity, and whether such firings have merit); Martha Neil, *When can workers be fired for Facebook posts and tweets*, ABA J. (Jan. 29, 2013, 5:09 PM), http://www.abajournal.com/news/article/worker_says_on_facebook_she_wants_to_be_fired_and_is_nlrb_rulings_offer_gui; Josh Eidelson, *Can You Be Fired for What You Post on Facebook?*, SLATE (July 3, 2012), http://www.slate.com/articles/news_and_politics/jurisprudence/2012/07/getting_fired_for_what_you_post_on_facebook.html; Jennifer Preston, *Social media History Becomes a New Job Hurdle*, NY TIMES (July 20, 2011), http://www.nytimes.com/2011/07/21/technology/social-media-history-becomes-a-new-job-hurdle.html.

6. *See e.g.* Sarah E. Needleman, *Companies Cope with Twitter Imposters*, WALL ST. J. (June 29, 2009), http://www.wsj.com/articles/SB124623159206366203; Aislinn Laing, *Twitter Cracks Down on Fake Accounts Amid Legal Threats*, TELEGRAPH (Sept. 20, 2009), http://www.telegraph.co.uk/technology/twitter/6211014/Twitter-cracks-down-on-fake-accounts-amid-legal-threats.html; Alexander Tsoutsanis, *Tackling Twitter and Facebook Fakes: Identity Theft in Social Media*, 12 WORLD DATA PROTECTION REP. (BNA) No. 4 (Apr. 2012), *available at* https://files.dlapiper.com/files/Uploads/Documents/.

violations of the profiled entities' rights of publicity or trademark rights.[7]

The role of social media has triggered debate in criminal law and national security law as well.[8] As this Article discusses, the use of social media as a meaningful tool for law enforcement has increased in recent years.[9] The law is still evolving as to whether and when the exploitation of information gleaned from those sources triggers a violation of the traditional constitutional protections against government intrusion. Given the vast resources the government has reportedly dedicated to national security, intelligence, and defense agencies to support data mining and analysis in recent years,[10] the boundaries between citizens' Fourth Amendment rights and government's role in providing for national security have become blurred to a point where citizens are growing concerned over whether such activities have led to an intrusion into civil liberties.[11]

---

7. The right of publicity prevents a party from using another person's notoriety to profit commercially at the expense of the targeted entity. *See, e.g.*, Zacchini v. Scripps Howard Broad. Co., 433 U.S. 562, 569–78 (1977) (recognizing the right of publicity as a protectable interest granting individuals exclusive control over the publicity given to their name or performance so they may "reap the rewards of [their] endeavors" in commercializing their talents and energy).

8. *See, e.g.*, Orin S. Kerr, *Applying the Fourth Amendment to the Internet*, 62 STAN. L. REV. 1005 (2010); Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741 (2008); Paul Ham, *Warrantless Search and Seizure of E-mail and Methods of Panoptical Prophylaxis*, 2008 B.C. INTELL. PROP. & TECH. F. 1 (2008), http://bciptf.org/wp-content/uploads/2011/07/16-warrantless-search-and-seizure-of-e-mail-and-methods-of-panoptical-prophylaxis.pdf; Jim Harper, *Reforming Fourth Amendment Privacy Doctrine*, 57 AM. U. L. REV. 1381 (2008); William Federspiel, *1984 Arrives: Thought (Crime), Technology and the Constitution*, 16 WM. & MARY BILL RTS. J. 865 (2008); Rachel S. Martin, Note, *Watch What You Type: As the FBI Records Your Keystrokes, the Fourth Amendment Develops Carpal Tunnel Syndrome*, 40 AM. CRIM. L. REV. 1271 (2003).

9. *See, e.g.*, Joel Mathis, *Report: Suspects in Gay Bashing Will Meet Police Today*, PHILADELPHIA MAGAZINE (Sept. 17, 2014), http://www.phillymag.com/news/2014/09/17/report-suspects-gay-bashing-will-meet-police-today (noting use of Twitter/Facebook by social media to provide police with clues and evidence to track down suspects).

10. *See, e.g.*, James Bamford, *The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)*, WIRED (Mar. 2012), http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1 (reporting that the National Security Agency has begun construction on a $2 billion dollar data center in Utah designed to "intercept, decipher, analyze, and store vast swaths of the world's communications as they zap down from satellites and zip through the underground and undersea cables of international, foreign, and domestic networks"). This facility was made possible in part by the NSA's near limitless budget, estimated to be "overflowing with tens of billions of dollars in post-9/11 budget awards." *Id.*

11. For instance, news that major technology companies including Google, Verizon, Facebook and Microsoft, had routinely provided the National Security Agency with records and information about its users spurred debate and criticism about whether such practices infringed the civil liberties of the nation's citizenry. *See, e.g.*, Charlie Savage, Edward Wyatt & Peter Baker, *U.S. Confirms That It Gathers Online Data Overseas*, NY TIMES (June 6, 2013), http://www.nytimes.com/2013/06/07/us/nsa-

This Article seeks to qualify somewhat the growing consensus that, at least as it was known in the twentieth century, "privacy is dead." Although this sentiment seems empirically correct, this Article argues it is an oversimplification that fails to account for American values and legal policy. Rather, the Authors recognize as a morally neutral proposition that privacy is a legal fiction. At the same time, this Article advocates that it is a fiction best maintained and protected to the extent possible and reasonable given the unambiguous willingness of people *en masse* to sacrifice their privacy for mere convenience and token benefits.

In Part II, the doctrines underlying the Fourth Amendment are briefly summarized and discussed to provide a foundation for analyzing whether government data mining of social media sites impinge on individual civil liberties. The legal history of law enforcement usage and acceptability of new technologies as means of gathering evidence against suspects is also summarized to provide a better understanding of the role and legality of new-found tactics. In Part III, the Authors discuss the origins and consequences of "the Wall" that once existed between federal law enforcement and national security investigations, and how national security imperatives accomplished through the Foreign Intelligence Surveillance Act ("FISA") differ from the traditional law enforcement missions. Part IV examines the evolving societal norms with respect to the increased prevalence and acceptability of new technology and social media sites. This includes the social and popular culture aspects as well as the government context and the role of society's lowered expectations of privacy in light of increased national security concerns. Finally, in Part V, this Article details the argument that privacy-sacrificing behaviors are creating new social norms in a way that meaningfully affects the constitutional calculus of "reasonableness" under the Fourth Amendment.

II. FOURTH AMENDMENT CONSIDERATIONS IN A RAPIDLY ADVANCING TECHNOLOGICAL AGE

A. *Fourth Amendment Foundations and the Reasonable Expectation of Privacy in the Twentieth Century*

The U.S. Constitution's Fourth Amendment provides basic protections against government intrusions.[12] It reads:

---

verizon-calls.html; Derek Satya Khanna, *The NSA Scandal*, NATIONAL REVIEW (June 12, 2013), http://www.nationalreview.com/article/350798/nsa-scandal-derek-satya-khanna?target=author&tid=903246; James Ball, *NSA's Prism Surveillance Program; How it Works and What it Can Do*, GUARDIAN (June 8, 2013), http://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google; Steven Levy, *How the NSA Almost Killed the Internet*, WIRED (Jan. 7, 2014), http://www.wired.com/2014/01/how-the-us-almost-killed-the-internet/.

12. U.S. Const. amend IV. *See also* United States v. White, 322 U.S. 694, 698 (1944) ("[The Fourth Amendment is] directed primarily to the protection of individ-

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[13]

The Amendment grew out of a compromise with Anti-Federalists concerned about too powerful a centralized government as a condition for voting to approve the Constitution that would initially lack a Bill of Rights.[14] Although certain provisions in the Bill of Rights are clearly directed at cabining the power and intrusiveness of military forces,[15] other protections, such as this one, reach further: the Fourth Amendment is "one of the pillars of liberty so necessary to a free government," the Second Circuit tells us, "that expediency in law enforcement must ever yield to the necessity for keeping the principles on which it rests inviolate."[16]

The Fourth Amendment, however, is not a blanket prohibition on all governmental searches, but only those warrantless searches that are deemed "unreasonable."[17] And, along with advances in and the proliferation of various technologies (particularly communications and remote-sensing technologies), notions of what constitutes a reasonable warrantless search have changed dramatically in the past century.

---

ual and personal rights."); Davis v. United States, 328 U.S. 582 (1946) ("[The] law of searches and seizures . . . is the product of interplay of [the Fourth and Fifth Amendments]. It reflects dual purpose—protection of privacy of the individual, his right to be let alone; protection of individual against compulsory production of evidence to be used against him."); Chandler v. Miller, 520 U.S. 305 (1997) ("[R]estraint on government conduct [under the Fourth Amendment] generally bars officials from undertaking search or seizure absent individualized suspicion [of wrongdoing]. [P]articularized exceptions to [this] rule are sometimes warranted based on 'special needs, beyond normal need for law enforcement.'"); Michigan v. Tyler, 436 U.S. 499 (1978) ((quoting Camara v. Municipal Court, 387 U.S. 523, 528 (1967) ("Basic purpose of [the Fourth Amendment] . . . is to safeguard privacy and security of individuals against arbitrary invasions by governmental officials.").

13. U.S. Const. amend. IV.

14. *See* Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 693–724 (1999); Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL.'Y 757, 875–81 (2014).

15. *See, e.g.*, U.S. Const. amend. III ("No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.").

16. United States v. 1013 Crates of Empty Old Smuggler Whiskey Bottles, 52 F.2d 49, 50 (2d. Cir. 1931).

17. *See, e.g.*, Terry v. Ohio, 392 U.S. 1 (1968) (quoting Elkins v. United States, 364 U.S. 206, 222 (1960) ("What Constitution forbids is not all searches and seizures, but unreasonable searches and seizures.")); Mincey v. Arizona, 437 U.S. 385 (1978) (quoting Katz v. United States, 389 U.S. 347, 357 (1967) ("Fourth Amendment proscribes all unreasonable searches and seizures, and . . . 'searches conducted outside judicial process, without prior approval by judge or magistrate, are per se unreasonable under Amendment, subject only to few specially established and well delineated exceptions.'")).

A discussion regarding the level of technological innovation permitted for use by law enforcement must begin with the background of the Supreme Court's seminal decision in *Olmstead v. United States*.[18] The lead petitioner Roy Olmstead was the head of a twelve-partner bootlegging conspiracy that employed more than fifty people in an operation that saw revenues of over $2 million a year (over $27 million in today's dollars).[19] In 1924, Olmstead and several others were charged with violating the National Prohibition Act[20] based on evidence that included months of stenographed transcripts from warrantless telephone wiretaps using equipment on telephone poles and in buildings located elsewhere than on property owned by the defendants.[21] Olmstead moved to suppress the wiretapping evidence and was denied. The Supreme Court granted *certiorari* to review "the single question whether the use of evidence of private telephone conversations between the defendants and others, intercepted by means of wiretapping, amounted to a violation of the Fourth and Fifth Amendments."[22]

Writing for the majority, Chief Justice William Howard Taft found that, since the government never entered the sacrosanct domain of the home, the question of the propriety of the government's actions never rose to the level of either a search or seizure.[23] In holding that there was not a Fourth Amendment violation, the Court reasoned that the constitutional right against unreasonable governmental seizure was akin to a real property right against common law trespass and limited to physical "things"[24] and did not prohibit mere listening in on conversations, even if that listening was accomplished through the use of technology.[25] Note that the government never argued, nor did the

18. Olmstead v. United States, 277 U.S. 438 (1928).

19. *See U.S. Inflation Calculator*, COIN NEWS MEDIA GROUP LLC http://www.usinflationcalculator.com/ (calculating the value of $2,000,000 in 1924, the year in which the wiretapping of *Olmstead* and other occurred, *see* United States v. Olmstead, 7 F.2d 760, 760–62 (D. Wash. 1925), in 2014 dollars) (last visited Feb. 17, 2015).

20. National Prohibition Act, Pub. L. 66-66, Stat. Ch. 85, 41 Stat. 305-323 (1919). The law was also known as the Volstead Act, after House of Representatives Judiciary Committee Chairman, Minnesota Congressman Andrew Volstead.

21. *Olmstead*, 277 U.S. at 455–57.

22. *Id.* at 455.

23. *Id.* at 464 ("The Amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants."). Declining to extend the exclusionary rule announced in *Weeks v. U.S.*, 232 U.S. 383 (1914), Chief Justice Taft drew a strict physical line around the home, opining that the Fourth Amendment should not be expanded to capture the "telephone wires, reaching to the whole world from [someone's] house or office . . . . [and, as such,] intervening wires are not part of his house or office, any more than are the highways along which they are stretched." *Olmstead*, 277 U.S. at 465.

24. *Olmstead*, 277 U.S. at 464 ("The [Fourth] [A]mendment itself shows that the search is to be of material things—the person, the house, his papers or his effects.").

25. *Id.* at 465–66 ("The language of the [Fourth] Amendment cannot be extended and expanded to include telephone wires, reaching to the whole world from the defendant's house or office . . . . The reasonable view is that one who installs in his house

Court suggest that wiretapping did not somehow affect a person's privacy interests;[26] rather, the issue before the Court merely was whether wiretapping was an unreasonable search or seizure that would require a warrant under the Fourth Amendment. The "right to privacy" as often asserted today was simply not cognizable in law at that time, and the Court's holding was limited accordingly.[27]

In dissent, however, Justice Louis Brandeis laid the groundwork for what would become a constitutional right to privacy, cautioning against a lax standard that would potentially provide the government with a manner to erode the protections traditionally offered to U.S. citizens.[28] At the same time, Justice Brandeis also recognized that Congress and the laws must be malleable enough to adapt to legal realities in a changing world.[29] Although earlier constitutional protections and laws were conceived to protect citizens from physical governmental intrusion and trespass, Justice Brandeis presciently predicted that the wiretapping at issue in *Olmstead* was only the beginning of potential technological intrusions upon privacy, which he equated to "individual security."[30]

Subsequent decisions affirmed the ability of the government to use technological means to secure evidence in criminal investigations without running afoul of the Fourth Amendment,[31] and for nearly

---

a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house and the messages while passing over them, are not within the protection of the Fourth Amendment.").

26. *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 949–50 (2012) (noting that the outcome of the *Olmstead* decision was based on the absence of a physical property intrusion based approach in the interpretation of finding a Fourth Amendment search, and not necessarily that notions underlying Fourth Amendment principles were not implicated).

27. *Olmstead*, 277 U.S. at 464 ("The [Fourth] [A]mendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants.").

28. *See id.* at 478–79 (Brandeis, J., dissenting).

29. *See id.* at 472 (Brandeis, J., dissenting) ("We have likewise held that general limitations on the powers of government, like those embodied in the due process clauses of the Fifth and Fourteenth Amendments, do not forbid the United States or the States from meeting modern conditions by regulations which a century ago, or even half a century ago, probably would have been rejected as arbitrary and oppressive. Clauses guaranteeing to the individual protection against specific abuses of power, must have a similar capacity of adaptation to a changing world." (internal citation and quotation omitted)).

30. *Id.* at 474 (Brandeis, J., dissenting) ("The progress of science in furnishing the government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the government, without removing papers form secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.").

31. *See, e.g.*, Goldman v. United States, 316 U.S. 129, 134–35 (1940) (holding that the installation and use of a listening apparatus and detectaphone to pick up and amplify sound waves from an adjoining office was not a violation of the Fourth Amendment). *But see id.* at 136–38 (Murphy, J., dissenting) (arguing that the Fourth

forty years following, this was the law of the land. So long as there was not a physical intrusion or seizure of the defendant, there was not a per se "search" subject to requirements of judicial issuance of a search warrant.[32]

However, the Court eventually chipped away at the requirement of a physical seizure as a condition-precedent to a violation of a defendant's Fourth Amendment rights,[33] moving toward an understanding of privacy rights that would constitutionally protect against evidence gathered through certain electronic surveillance means without warrants.[34] For instance, in *On Lee v. United States*, Justice Robert Jackson, writing for the majority Court, upheld the government's use of evidence collected through a microphone and transmitter secretly placed on the body of an informant.[35] The Court held that neither law enforcement nor the technology used in the case had "trespassed" on or "unlawfully seized" the defendant's person or property, and thus did not trigger the protections required by the Fourth Amendment.[36]

Amendment's protections against unwarranted intrusions includes non-physical intrusions, and that the Court should take care to ensure that the spirit of the Fourth Amendment is maintained in a changing world) ("The conditions of modern life have greatly expanded the range and character of those activities which require protection from intrusive action by Government officials. . . . It is our duty to see that this historic provision receives a construction sufficiently liberal and elastic to make it serve the needs and manners of each succeeding generation").

32. *See generally Olmstead*, 277 U.S. 438.

33. As discussed below, the Supreme Court's jurisprudence evolved following *Olmstead*, but change was not limited to judicial action. For instance, the Communications Act of 1934, Pub. L. 73-416, 48 Stat. 1064,1103 (codified as amended at 47 U.S.C. § 605) (2012), was noted by the Court in *Berger v. New York*, to have been a Congressional reaction to *Olmstead* and privacy concerns therein, to "specifically prohibit[ ] the interception without authorization and the divulging or publishing of the contents of telephonic communications." Berger v. New York, 388 U.S. 41, 51 (1967). *See also* Nardone v. United States, 302 U.S. 379, 382–83 (1937) (holding that federal law enforcement agents were prohibited under the Communications Act of 1934 from intercepting telephone messages without the authorization of the sender); Timothy Casey, *Electronic Surveillance and the Right To Be Secure*, 41 U.C. DAVIS L. REV. 977, 986 (2008) (noting that the "Communications Act of 1934, [was] the legislative response to Olmstead that banned all 'interception' of 'wire communications'").

34. *See, e.g.*, Silverman v. United States, 365 U.S. 505, 511 (1961) (foreshadowing the concerns raised that advances in science that would potentially permit the gathering of evidence by law enforcement without being in the immediate vicinity of the target).

35. On Lee v. United States, 343 U.S. 747, 751 (1952). Specifically, the government used an undercover agent who was wired with a microphone and antennae, to transmit the conversations between the undercover agents and the defendant, to an FBI agent listening outside the defendant's place of business. *Id.* at 749. At the defendant's trial for narcotics related charges, the government introduced the contents of the transmitted conversations. *Id.* at 750. Over the objections of defense counsel, the district court held that the use of such evidence did not violate the defendant's Fourth Amendment rights, as this was not considered a "search." *Id.* at 751.

36. *Id.* at 751–53; *see also Goldman*, 316 U.S. at 129. The Supreme Court in *Goldman* permitted the government to surreptitiously install listening devices and detectaphones in the offices of attorneys suspected of violating the Bankruptcy Act. *Id.* at 130–32. The Court rejected arguments to overrule their decision in *Olmstead*, and

Instead, the Court concluded that no such "trespass" had occurred since the defendant had by way of invitation consented to the informant's presence on his property.[37] The Court in *On Lee* determined that, without an actual trespass or seizure, it did not matter that ultimately electronic devices were utilized to capture the conversations at issue in the case.[38]

The *On Lee* decision was far from unanimous. A series of dissents by Justices William Douglas, Felix Frankfurter, and Harold Burton illustrated deep concerns regarding the government's exercise of its electronic abilities. Justice Frankfurter reiterated Justice Brandeis' warning in his *Olmstead* dissent,[39] and added that the *On Lee* case illustrated "how the rapid advances of science are made available for that police intrusion into our private lives against which the Fourth Amendment of the Constitution was set on guard."[40] Technological advancements, wrote Justice Frankfurter, promote "lazy" law enforcement, presumably allowing the government to exercise Constitutional shortcuts in their data- and evidence-gathering efforts.[41] Justice Douglas' dissent argued that the Court's *Olmstead* decision was incorrectly decided, and that the key determinant as to the constitutionality of law enforcement's actions and use of technology is not the "nature of the instrument that science or engineering develops," but rather whether there is an invasion of privacy that violates the Fourth and Fifth Amendments.[42]

By 1967, the rationale and holding of the *Olmstead* decision were in serious danger of being repudiated. The Court in *Berger v. New York* was asked to evaluate the legality of a New York statute that permitted warrantless eavesdropping by law enforcement, including through use of electronic recording devices.[43] The decision traced the history of eavesdropping, including the development of modern tactics and

instead held that the use of the technology in this case did not exceed that which was previously approved. *Id.* at 135–36.

37. *On Lee*, 343 U.S. at 751–52.

38. *Id.* at 753.

39. *Id.* at 759; *see also supra* note 30.

40. *Id.* at 759. Justice Frankfurter voiced significant concerns that sanctioning the evidence in the *On Lee* case would have the effect of rewarding "lazy and not alert law enforcement", and "led to a deep conviction that these short-cuts in the detection and prosecution of crime are as self-defeating as they are immoral." *Id.* at 761.

41. *Id.* at 761.

42. *Id.* at 765. As noted later in this Article, the increasingly blurred confluence between technology and privacy considerations makes it more difficult to determine whether law enforcement's tactics are consistent with Fourth Amendment jurisprudence.

43. Berger v. New York, 388 U.S. 41, 43–44 (1967) (citing N.Y. CODE CRIM. PROC. § 813-a (1958)). Specifically, evidence regarding bribes for liquor licenses in New York was obtained through the use of a recording device secreted by an applicant for such license, was introduced into evidence in the subsequent trial for conspiracy to bribe the Chairman of the New York State Liquor Authority. *Id.*; *see also supra* note 33.

the use of sophisticated electronic devices capable of transmitting and recording private conversations for significant distances.[44] Of note, the *Berger* Court acknowledged the concerns raised by several states which, on the basis of significant individual privacy implications, banned the use of surreptitious eavesdropping by mechanical or electronic device.[45]

Significantly, the *Berger* Court did not treat the electronically-acquired evidence as distinct from other types of evidence for the purposes of its Fourth Amendment analysis.[46] Instead, the Court implicitly acknowledged that electronic eavesdropping was subject to the same Fourth Amendment principles as any other search or seizure.[47] In other words, by treating evidence gathered by electronic means as no different than any other, the government would be required to establish probable cause before a proper authority to obtain warrants both empowering and limiting the scope of the search before being able to avail itself of the results of such a search.[48] Consequently, the Court invalidated the statute as exceeding the limitations of the Fourth Amendment holding that it failed to mandate the needed level of particularity as to the scope of the search to justify the potential intrusion on the privacy of search subjects.[49]

In a separate concurrence, Justice Douglas further argued against the use of electronic surveillance and eavesdropping as inherently conflicting with the Fourth Amendment's protections for privacy.[50] Justice Douglas additionally noted that such devices inherently are

44. *Id.* at 46–47 (noting that examples of such devices include those "complete detection systems which automatically record voices under almost any conditions by remote control;" items which may "increase[ ] the range of these powerful wireless transmitters to a half mile;" and "combination mirror transmitter[s] . . . which permit[ ] not only sight but voice transmission up to 300 feet").

45. *Id.* at 47 (noting that California, Illinois, Maryland, Massachusetts, Nevada, New York, and Oregon were states with such statutes).

46. *See generally id.* at 53–60.

47. *Id.*

48. *Id.*; *see also* Osborn v. United States, 385 U.S. 323 (1966). In *Osborn*, the Supreme Court upheld the use of conversations captured by a secret recording device on the basis that such use by law enforcement was done only after judges had "authorized the use of a recording device for the narrow and particularized purpose." *Id.* at 330. The Court noted that the government satisfied the "the procedure of antecedent justification before a magistrate" necessary as "a precondition of lawful electronic surveillance." *Id.* (citing Lopez v. United States, 373 U.S. 427, 464 (1963) (Brennan, J., dissenting)).

49. *Berger v. New York*, 388 U.S. at 58 (noting that New York's statute laid down no "precise and discriminate requirements," and instead authorized the "indiscriminate use of electronic devices as specifically condemned in *Osborn*" (internal quotations omitted)). Without such limitations, the statute facilitated the type of "unauthorized invasions of privacy [and] general searches by electronic devices, the truly offensive character of which was first condemned in [the 1795 English Law decision of *Entick* v. *Carrington*, 19 How. St. Tr. 1029]."

50. *Berger*, 388 U.S. at 64 (Douglas, J., concurring) ("[T]here persists my overriding objection to electronic surveillance, *viz*., that it is a search for 'mere evidence' which, as I have maintained on other occasions, is a violation of the Fourth and Fifth

nonspecific with respect to what types of information they may record, and thus would "constitute[ ] a dragnet, sweeping in all conversations within its scope—without regard to the participants or the nature of the conversations. . . . [Wiretapping also] intrudes upon the privacy of those not even suspected of crime and intercepts the most intimate of conversations."[51] Legislatively barring the introduction of evidence collected through electronic surveillance except where sufficient probable cause of a crime has occurred would not matter, he believed, because the search itself would violate civil liberties.[52]

Two years after the *Berger* decision, the Court in *Katz v. United States* expressly overturned the earlier constitutional standard that limited the warrant requirement only to protecting against physical intrusion only and expanded the Fourth Amendment's protections to certain conversations that could be overheard with the aid of electronic eavesdropping equipment.[53] In *Katz*, the Court was asked to determine whether law enforcement agents' use of a listening device attached to a phone booth to record the defendant's illegal interstate gambling calls was constitutional.[54] As a culmination of years of judicial decisions questioning the use of such tactics, the Court held that the use of electronic equipment and other technological advances in government activities would be considered a "search and seizure within the meaning of the Fourth Amendment"[55] and thus was subject to the warrant requirement if otherwise unreasonable. Rejecting the exclusivity of "constitutionally protected [physical] areas," the Court found "the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[56]

Amendments, no matter with what nicety and precision a warrant may be drawn . . . .").

51. *Id.* at 65 (Douglas, J., concurring).

52. *Id.* at 66 (Douglas, J., concurring) ("But such a [statutory] limitation would not alter the fact that the order authorizes a general search. Whether or not the evidence obtained is used at a trial for another crime, the privacy of the individual has been infringed by the interception of all of his conversations. And, even though the information is not introduced as evidence, it can and probably will be used as leads and background information." (internal citations omitted)).

53. Katz v. United States, 389 U.S. 347, 353 (1967); *see also* United States v. White, 401 U.S. 745, 748 (1971) ("[*Katz*], however, finally swept away doctrines that electronic eavesdropping is permissible under the Fourth Amendment unless physical invasion of a constitutionally protected area produced the challenged evidence."). Importantly, *Olmstead*'s limiting factor of physical trespass remains in force as well.

54. *Katz*, 389 U.S. at 353.

55. *Id.* (internal quotations omitted). Ultimately, the Court overturned the petitioner's conviction not because of the use of electronic surveillance equipment, but instead because the government failed to secure a warrant prior to employing the technology in this case. *Id.* at 351, 358

56. *Id.* at 351 (internal citations omitted).

The "reasonable expectation" concept was articulated in Justice John Marshall Harlan's concurrence. Justice Harlan reasoned that limiting Fourth Amendment protection to physical penetration of a premises "is, in the present day, bad physics as well as bad law, for reasonable expectations of privacy may be defeated by electronic as well as physical invasion."[57] In Justice Harlan's formulation, which endures to this day, a constitutionally reasonable expectation of privacy requires, "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.'"[58] In practice, after *Katz* many "reasonable expectation" inquiries turned on one's privacy interests in what could potentially be generally observable by (a) the public[59] or (b) select third-parties, who generally were commercial entities with whom the defendant had contracted to provide a service.[60]

Four years after *Katz*, Justice Douglas cautioned that the use of electronic surveillance could not be consistent with notions of privacy in the Fourth Amendment in his vigorous dissent in *United States v. White*.[61] In *White*, the defendant was convicted of drug-related crimes based on evidence collected by a radio transmitter on the body of a government informant.[62] The equipment used in the case transmitted the defendant's conversations to government agents hiding in the in-

57. *Id.* at 362 (Harlan, J., concurring).

58. *Id.* at 361 (Harlan, J., concurring); *see also* Rakas v. Illinois, 439 U.S. 128, 145 n.12 (1978) ("Legitimation of expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society.").

59. *See, e.g.*, Oliver v. United States, 466 U.S. 170, 179 (1984) (maintaining, post-*Katz*, the open fields doctrine announced in *Hester v. United States*, 265 U.S. 57 (1924), finding that "open fields do not provide the setting for those intimate activities that the [Fourth] Amendment is intended to shelter from government interference or surveillance"); California v. Ciraolo, 476 U.S. 207 (1986) (holding no reasonable expectation of privacy where illegal activities can be viewed via flyover in public airspace); Florida v. Riley, 488 U.S. 445 (1989) (same); United States v. Dunn, 480 U.S. 294 (1987) (holding police officer's use of a flashlight to view the inside of a barn from an open field does not transform his observations into an unreasonable search).

60. *See, e.g.*, United States v. White, 401 U.S. 745 (1971) (no reasonable expectations of privacy in conversations with third-party police informants, including conversations inside the defendant's home); United States v. Miller, 425 U.S. 435 (1976) (no protectable Fourth Amendment interest in bank records); Smith v. Maryland, 442 U.S. 735 (1979) (as distinct from wiretaps recording the substance of phone calls, there is no privacy interest in pen register-generated phone call metadata such as numbers dialed, time, and duration); California v. Greenwood, 486 U.S. 35 (1988) (no protectable reasonable expectation of privacy in garbage placed in opaque bags placed outside of home for pickup by trash collector).

61. *White*, 401 U.S. at 756–66 (Douglas, J., dissenting); *see also* Goldman v. United States, 316 U.S. 129, 136–38 (1942) (Murphy, J., dissenting) (arguing that "[o]ne of the great boons secured to the inhabitants of this country by the Bill of Rights is the right of personal privacy guaranteed by the Fourth Amendment. . . . [which] protects the individual against unwarranted intrusions by others into his private affairs", and that it was the responsibility of the Court to ensure that the principles provided by the Fourth Amendment therein could be preserved).

62. *Id.* at 746–47.

formant's home and in the surrounding area.[63] The Court's majority opinion affirmed the *Katz* decision and reiterated that the use of electronic surveillance or intervention as a substitute for physical intrusion was still considered a search under the Fourth Amendment.[64] However, the *White* opinion focused not on the use of electronic equipment itself but instead on the Court's jurisprudence concerning confidential informants.[65] The earlier court of appeals decision interpreted the case law in this area as distinguishing contemporaneously electronically collected evidence from testimony that was gathered by the informant.[66] That was contrary to existing jurisprudence that permitted informants or law enforcement to testify regarding conversations they had with the defendant.[67] Instead, the Court reasoned that to exclude such recorded evidence simply because it was concurrently generated by an electronic device seemed to impose an artificial and illogical distinction.[68] The Court therefore concluded that there was not a Fourth Amendment violation in *White*, declining to extend the reasonable expectation of privacy to such discussions.[69]

Justice Douglas argued in his dissent that the foundational concepts and principles of privacy laid down by the drafters of the Constitution would be significantly undermined if the government were permitted to utilize such electronic technology to eavesdrop.[70] Instead, he fur-

63. *Id.* at 747.

64. *Id.* at 748.

65. *Id.* at 749 (citing earlier Supreme Court decisions in *Hoffa v. United States*, 385 U.S. 293 (1966), *Lewis v. United States*, 385 U.S. 206 (1966), and *Lopez v. United States*, 373 U.S. 427 (1963)).

66. *White*, 401 U.S. at 749–50 (noting that "the Court of Appeals nevertheless read both *Katz* and the Fourth Amendment to require a different result if the agent not only records his conversations with the defendant but instantaneously transmits them electronically to other agents equipped with radio receivers. Where this occurs, the Court of Appeals held, the Fourth Amendment is violated and the testimony of the listening agents must be excluded from evidence").

67. *Id.* at 751.

68. *Id.* ("If the conduct and revelations of an agent operating without electronic equipment do not invade the defendant's constitutionally justifiable expectations of privacy, neither does a simultaneous recording of the same conversations made by the agent or by others from transmissions received from the agent to whom the defendant is talking and whose trustworthiness the defendant necessarily risks.").

69. *Id.* at 752–53.

70. *Id.* at 756 (Douglass, J., dissenting) ("At the same time the concepts of privacy which the Founders enshrined in the Fourth Amendment vanish completely when we slavishly allow an all-powerful government, proclaiming law and order, efficiency, and other benign purposes, to penetrate all the walls and doors which men need to shield them from the pressures of a turbulent life around them and give them the health and strength to carry on"). Justice Douglas' dissent in *White* was similar to the concepts espoused by Justice Murphy in his dissent in *Goldman*, where he argued that a "search of one's home or office no longer requires physical entry, for science has brought forth far more effective devices for the invasion of a person's privacy than the direct and obvious methods of oppression which were detested by our forebears and which inspired the Fourth Amendment. Surely the spirit motivating the framers of [the Fourth] Amendment would abhor these new devices no less." *Goldman*, 316 U.S. at 139 (Murphy, J., dissenting) (footnote omitted).

ther noted that electronic surveillance techniques are fraught with the possible danger of government agents overstepping traditional notions and expectations of privacy, and are "almost bound to lead to abuse of civil rights."[71] Citing Justice William Brennan's dissent in *Katz*,[72] Justice Douglas argued that electronic surveillance and new technologies could still be used appropriately by government officials with the caveat that their use must be consistent with traditional Fourth Amendment protections.[73] The protections offered by subjecting law enforcement to judicial review and the warrant requirement would provide further assurances against the "arbitrariness of any such" searches by the government.[74] Justice Douglas recognized the danger of allowing law enforcement officials to be the sole arbiters of the appropriateness of using electronic surveillance equipment, arguing that the fundamental principles of a free society weighed in favor of judicial intervention.[75] To allow otherwise would result in the possibility that individuals would constantly be in a state of electronic monitoring and surveillance, which could lead to a significant "chilling effect on people speaking their minds and expressing their views on important matters."[76]

In a similarly impassioned dissent, Justice Harlan cautioned against permitting unchecked widespread government use of electronic surveillance techniques.[77] Recognizing technology can be an effective law enforcement tool, he cautioned that courts should proceed "with specially measured steps in this field."[78]

To that end, Justice Harlan argued that the role of the judiciary was to ensure that the government did not overstep its boundaries in the pursuit of its law enforcement functions, with search warrants serving as a prophylactic measure to preserve the citizenry's private inter-

71. *White*, 407 U.S. at 757 (discussing FDR's authorization of wiretaps).

72. *Id.* at 759–60 (citing Lopez, 373 U.S. 427, 465–66 (1963) (Brennan, J., dissenting)).

73. *Id.* at 760 ("I would stand by [the Court's decisions in] *Berger* and *Katz* and reaffirm the need for judicial supervision under the Fourth Amendment of the use of electronic surveillance which, uncontrolled, promises to lead us into a police state." (footnote omitted)).

74. *Id.* at 761 (quoting Camara v. Municipal Court, 387 U.S. 523, 533 (1967) ("We simply cannot say that the protections provided by the warrant procedure are not needed in [the context of warrantless administrative searches] broad statutory safeguards are no substitute for individualized review, particularly when those safeguards may only be invoked at the risk of a criminal penalty.")).

75. *Id.* at 761–62 ("[T]hese extensive intrusions into privacy made by electronic surveillance make self-restraint by law enforcement officials an inadequate protection, that the requirement of warrants under the Fourth Amendment is essential to a free society.").

76. *Id.* at 765.

77. *Id.* at 769 (Harlan, J., dissenting).

78. *See generally id.* at 769–72 (relaying research by Professor Alan Westin, in his book *Privacy and Freedom*, which documented the ability of the government to utilize then existing technologies to create an "Orwellian Big Brother" scenario (ALAN WESTIN, PRIVACY AND FREEDOM 131 (1967)).

ests.[79] This would ensure that people would be able to maintain their private and intimate discussions "freely, openly and spontaneously" without worrying that their serendipitously recorded words could be later construed and analyzed by the government.[80] To provide otherwise would allow law enforcement officials unfettered discretion in their use of new technologies, which Justice Harlan argued was an untenable scenario.[81]

As this Article later argues, although the concerns raised by both Justices Douglas and Harlan in their dissents in *White* were prescient in notable ways, the changing nature of privacy, particularly as it relates to social media, has perhaps resulted in a strange dichotomy.[82] As discussed further below, the recent perception is that the populace has become more willing to give up certain aspects of their privacy as no longer sacrosanct if doing so yields a modicum of perceived additional convenience in their daily lives. The relationship between people's assertion of privacy rights with respect to safety and security, however, is more complex. As described further below, the public is inconsistent in its acceptance of the use of certain technologies to catch criminals and/or to counter national security threats. Nevertheless, how people actually behave makes a difference, at a minimum, to the objective "reasonableness" in the "reasonable expectation of privacy" paradigm.

B. *The* Kyllo *Test and Reasonableness as a Function of Technology*

Three months to the day before the September 11, 2001, attacks, the Supreme Court's decision in *Kyllo v. United States*[83] sought to provide a theoretically sound, but perhaps in practicality a completely unworkable, sliding scale test for high-tech law enforcement tools.[84] At

79. *Id.* at 789–90 ("The very purpose of interposing the Fourth Amendment warrant requirement is to redistribute the privacy risks throughout society [and] would prevent public officials from engaging in [electronic surveillance] unless they first had probable cause to suspect an individual of involvement in illegal activities and had tested their version of the facts before a detached judicial officer.").

80. *Id.* at 790 ("Interposition of a warrant requirement is designed not to shield 'wrongdoers,' but to secure a measure of privacy and a sense of personal security throughout our society.").

81. *Id.* ("The Fourth Amendment does, of course, leave room for the employment of modern technology in criminal law enforcement, but in the stream of current developments in Fourth Amendment law I think it must be held that third-party electronic monitoring, subject only to the self-restraint of law enforcement officials, has no place in our society.").

82. *See infra* Part IV.

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

84. Foreshadowing how complicated it would be to set clear rules in an era marked by dynamic technological developments and how new tech-based tools are used by both the government and the public, Justice Scalia wrote of his judicial philosophy in 1989:

> Just as that manner of textual exegesis facilitates the formulation of general rules, so does, in the constitutional field, adherence to a more or less

its core, the Court's *Kyllo* opinion tested whether law enforcement conducts an unreasonable search or seizure as a function of a piece of technology's availability to and use by society in general.[85] In essence, technological advances must be widely acceptable and available to the general populace before the government may employ them without warrants in their investigations.[86]

The *Kyllo* case involved an appellant, Danny Lee Kyllo, who argued that law enforcement's use of an external thermal scanner without a warrant violated his Fourth Amendment rights.[87] The police suspected that Kyllo was growing marijuana in his residence. Using a special thermal scanner capable of detecting infrared energy, law enforcement agents performed a scan of Kyllo's home from across the street, based on the knowledge that "[i]ndoor marijuana growth typically requires high-intensity lamps" that radiate a significant amount of heat. The resulting scan indicated that the "roof over the garage and a side wall of [Kyllo's] home were relatively hot compared to the rest of the home and substantially warmer than neighboring homes in the triplex," indicating a likelihood that high-intensity lights were in those locations.[88] Ultimately, the thermal scanner results, informant tips, and utility bills were presented to a magistrate judge and used as the basis for a warrant to search the appellant's home.[89] Kyllo entered a conditional guilty plea after the trial court denied his motion to suppress the thermal scanner results.[90]

The Ninth Circuit affirmed the conviction on the grounds that the appellant "had shown no subjective expectation of privacy because he had made no attempt to conceal the heat escaping from his home."[91] Furthermore, the court held that "there was no objectively reasonable

---

> originalist theory of construction. The raw material for the general rule is readily apparent. If a barn was not considered the curtilage of a house in 1791 or 1868 and the Fourth Amendment did not cover it then, unlawful entry into a barn today may be a trespass, but not an unconstitutional search and seizure. It is more difficult, it seems to me, to derive such a categorical general rule from evolving notions of personal privacy.

Antonin Scalia, *The Rule of Law as a Law of Rules*, 56 U. CHI. L. REV. 1175, 1184 (1989).

85. *See also* Olmstead v. United States, 277 U.S. 438, 472 (Brandeis, J., dissenting) (arguing that Constitutional protections "guaranteeing to the individual protection against specific abuses of power, must have . . . capacity of adaptation to a changing world."); Carroll v. United States, 267 U.S. 132, 149 (1925) ("The Fourth Amendment is to be construed in light of what was deemed unreasonable search and seizure when it was adopted, and in a manner which will conserve public interests as well as the interests and rights of individual citizens.").

86. *Cf.* Okla. Press Publ'g Co. v. Walling, 147 F.2d 658 (10th Cir. 1945), *aff'd* 327 U.S. 186 (1946) (The "Fourth Amendment must be construed so as to serve public interest as well as individual rights.").

87. *Kyllo*, 533 U.S. at 29.

88. *Id.* at 29–30.

89. *Id.* at 30.

90. *Id.*

91. *Id.* at 31.

expectation of privacy because the imager 'did not expose any intimate details of Kyllo's life,' only 'amorphous "hot spots" on the roof and exterior wall.'"[92]

On appeal, the Supreme Court began its discussion of the case by examining the parameters and criteria for a governmental search that would require a warrant.[93] As a general rule, the Court noted that "common law trespass"[94] or "an actual intrusion into a constitutionally protected area"[95] was a prerequisite to concluding that a search triggered Fourth Amendment protections. Furthermore, the Court reaffirmed the propriety of law enforcement using purely visual surveillance, since "'the eye cannot . . . be guilty of a trespass.'"[96]

Although purely visual surveillance was permissible, the use of "technology to shrink the realm of guaranteed privacy"[97] to allow the government into people's homes was beyond what the Court would permit.[98] The right of individuals to feel secure and private in their own homes was deemed the "minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*."[99] The use of technology to electronically "enter" the home without a warrant was thus an unconstitutional search under the Fourth Amendment, particularly where the technology used was not generally available.[100] Furthermore, the Court rejected the government's arguments that the technology utilized in the case was benign in that it did not "detect private activities occurring in private areas" of the home.[101] Instead, the Court announced that in one's home "*all* details are intimate details . . . [with] the entire area . . . held safe from prying government eyes."[102] Crude technologies could just as easily provide details as to the intimate activities occurring in the home, and the police could not ascertain with any level of certainty that their use of technology would not otherwise intrude on intimate activities.[103] "Where . . . the Gov-

92. *Id.*
93. *Id.*
94. *Id.* (citing Goldman v. United States, 316 U.S. 129, 134–36; Olmstead v. United States, 277 U.S. 438, 464–66). As the Supreme Court noted in *Kyllo*, the trespass prerequisite is no longer a necessary requirement to a finding of a search, as delineated by its decision in *Rakas v. Illinois*, 439 U.S. 128, 143 (1978).
95. Silverman v. United States, 365 U.S. 505, 510–12 (1961).
96. *Kyllo*, 533 U.S. at 31–32 (citing Boyd v. United States, 116 U.S. 626, 628 (1886)). This point was reaffirmed in the Supreme Court's holding in *California v. Ciraolo* where the Court concluded that "the Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares." California v. Ciraolo, 476 U.S. 207, 213 (1986).
97. *Kyllo*, 533 U.S. at 34.
98. *Id.*
99. *Id.* (emphasis in original).
100. *Id.* (citing Silverman v. United States, 365 U.S. 505, 512 (1961)).
101. *Id.* at 37.
102. *Id.* at 37–38 (emphasis in original).
103. *Id.* at 38.

ernment uses a device that is not in general public use, to explore the details of the home that would previously have been unknowable without physical intrusion," Justice Antonin Scalia concluded, "the surveillance is a 'search' and presumptively unreasonable without a warrant."[104]

Writing for the dissent, Justice John Paul Stevens, joined by Chief Justice William Rehnquist and Justices Sandra Day O'Connor and Anthony Kennedy, argued that the majority's decision was unnecessary in light of existing Fourth Amendment case law and that it instead proffered an "unwise[,] and inconsistent" standard seemingly to be applied solely in the instance of potential future technological intrusions.[105] Instead, Justice Stevens argued that existing case law in this area had consistently upheld the ability for law enforcement to search property that is in plain public view or that a person "knowingly exposes to the public."[106] In this case, the technology did nothing more than show areas of heat emanating from Kyllo's home, which the dissent argued could have just as easily been observed from outside the home.[107] Furthermore, the dissent noted that all the police did in this case was make an inference based on publicly available information, an action the dissent said was within the bounds of a reasonable search.[108]

Additionally, the dissent argued that the Court's standard would potentially be impracticable when actually applied to the facts of a case. Specifically, the dissent was concerned about the inability to quantify when a piece of new technology proliferates to the point that

104. *Id.* at 40.

105. *Id.* at 41 (Stevens, J., dissenting).

106. *Id.* (citing California v. Ciraolo, 476 U.S. 207, 213 (1986); Florida v. Riley, 488 U. S. 445, 449–50 (1989); California v. Greenwood, 486 U. S. 35, 40–41 (1988); Dow Chem. Co. v. United States, 476 U. S. 227, 235–36 (1986); Air Pollution Variance Bd. of Colo. v. W. Alfalfa Corp., 416 U. S. 861, 865 (1974)).

107. *Id.* at 42–43 ("[T]his case involves nothing more than off-the-wall surveillance by law enforcement officers to gather information exposed to the general public from the outside of petitioner's home. All that the infrared camera did in this case was passively measure heat emitted from the exterior surfaces of petitioner's home. . . . [A]ll that those measurements showed were relative differences in emission levels, vaguely indicating that some areas of the roof and outside walls were warmer than others . . . . [N]o details regarding the interior of petitioner's home were revealed. Unlike an x-ray scan, or other possible 'through the-wall' techniques, the detection of infrared radiation emanating from the home did not accomplish 'an unauthorized physical penetration into the premises,' nor did it 'obtain information that it could not have obtained by observation from outside the curtilage of the house.'").

108. *Id.* at 44, 46 ("For the first time in its history, the Court assumes that an inference can amount to a Fourth Amendment violation . . . . Since what was involved in this case was nothing more than drawing inferences from off-the-wall surveillance, rather than any 'through-the-wall' surveillance, the officers' conduct did not amount to a search and was perfectly reasonable.").

its warrantless use by law enforcement would be reasonable.[109] Justice Stevens warned that "it seems likely that the threat to privacy will grow, rather than recede, as the use of intrusive equipment becomes more readily available."[110] The dissent further argued that under the Court's ruling, new technologies that would serve as substitute means of investigation that would ordinarily be constitutional in nature (e.g., a mechanical means of drug detection in lieu of a drug-sniffing dog) could be deemed impermissible regardless of how limited the scope of the information that may be provided.[111]

Revisiting concerns and comments raised by its earlier case law and jurisprudence, the Court in *Kyllo* recognized that it faced much difficulty in balancing the constitutional rights of the people with the government's ability to utilize new technologies for law enforcement purposes without a warrant. In doing so, the Court specifically attempted to articulate a rubric for future courts to apply when grappling with difficult decisions as to the reasonableness of employing such new technologies. However, as the following Section illustrates, in practice, various applications of *Kyllo*'s test has often yielded curious results.

C. *Modern Applications of* Kyllo

In many ways, the Supreme Court's decision in *Kyllo* did not tread new ground. As discussed previously, the Court had already wrestled with deciding when emerging technologies such as wiretaps and electronic voice recorders may be used without a warrant to collect information in support of law enforcement. But since case law is always reactionary in that it develops based on specific sets of facts, it is sometimes difficult to apply general legal principles in *sui generis* situations, particularly in areas where legal determinations are subject to a reasonableness standard, where there looms the possibility that the determination could reflect what judges think is reasonable, versus objective social standards. The Court's opinion in *Kyllo* sought to provide generalizable standards and guidelines for law enforcement's use of technology that is constantly pushing boundaries, partially because of resourcing constraints, and partially in response to the demands of catching more sophisticated criminals. In theory, courts could apply *Kyllo*'s test to determine whether law enforcement's implementation of novel or advanced technological methodologies have intruded on areas viewed as sacrosanct.[112] In practice, nuanced fac-

109. *Id.* at 47 (arguing that the majority opinion did not quantify as to "how much use [of certain new technology] is general public use" for a determination as to what is reasonable).

110. *Id.*

111. *Id.* at 47–48.

112. *But see* Jones v. United States, 132 S. Ct. 945, 954, 962 (2012) (in concurring opinions by Justices Sotomayor and Alito, both Justices noted the importance of

tual differences, subjective assessments of what is most relevant in any given fact pattern, and the rapid pace at which modern technology proliferates have made it difficult to develop a cohesive body of jurisprudence in this area, where, for example, people's use of communications technology subjects their exchanges to outside scrutiny, and police use of certain tracking technologies arguably mimics traditional law enforcement methods.

In *City of Ontario v. Quon*,[113] the Supreme Court grappled with whether individuals have any privacy rights in digital or text messages.[114] In an effort to help its police officers rapidly mobilize in response to emergency situations, the city government issued its police officers alphanumeric pagers.[115] During the next few months, Quon exceeded the limits included in his pager's monthly plan and had to reimburse the city for the excess charges.[116] After another overuse period, the city decided to audit Quon's messages to determine whether the bulk of the messages were for work or for personal purposes.[117] The audit found that the large majority of the text messages sent during the workday were non-work related and were sexually explicit in nature.[118] In accordance with prior warnings that text messages sent through the pagers would be treated the same as work emails, meaning that the government could audit and read those messages without notice, Quon was disciplined for the conduct.[119]

At issue was whether a city government could validly read the text messages sent from its pagers without violating the employee's Fourth Amendment rights.[120] The Ninth Circuit held that Quon had a reasonable expectation of privacy in his communications, and the warrantless city audit would therefore be unconstitutional unless no "less

---

weighing prevailing societal valuations of privacy in the calculus of evaluating whether a Fourth Amendment search has occurred).

113. City of Ontario v. Quon, 560 U.S. 746 (2010).

114. *Id.* at 750.

115. *Id.* at 750–51.

116. *Id.* at 752.

117. *Id.* at 752–53.

118. *Id.*

119. *Id.* at 751–53. In fact, the city's computer use policy specifically dictated that it "reserves the right to monitor and log all network activity including e-mail and Internet use, with or without notice. Users should have no expectation of privacy or confidentiality when using these resources." *Id.* at 751. While text messages were not explicitly covered under the policy, officers were informed "that the City would treat text messages the same way as it treated e-mails." *Id.*

120. *Id.* at 754. While recognizing that the respondent had an expectation of privacy in the messages, the district court held the city's audit did not violate any Fourth Amendment rights since the audit was not conducted for the purpose of snooping into the content of the respondent's messages, but rather to determine whether the city needed to increase its allocated usage. On appeal, the Ninth Circuit disagreed in part, finding the respondent had a reasonable expectation of privacy in the messages and that the search conducted by the city had exceeded what would be a reasonable scope. *Id.*

intrusive means were feasible" than the manner in which the search was conducted.[121]

In a unanimous decision, the Supreme Court reversed.[122] The Court recognized that the Fourth Amendment is not limited only to criminal matters, but protects citizens (including government employees) from governmental searches regardless of the context.[123] And, recognizing that it was wading into an area whose ramifications that had not yet fully been realized, the Court noted that it was not well equipped to dictate what would be considered a reasonable expectation of privacy in this context.[124] Nonetheless, assuming arguendo that there existed a reasonable expectation of privacy in the text messages, the Court still found no Fourth Amendment violation because the purpose of the search and its limited scope was reasonable.[125]

Specifically, the Court held that the city was justified in trying to determine if the text messaging plan was insufficient for the city's needs and that reviewing the messages was the most "efficient and expedient way to determine whether Quon's overages were the result of work-related messaging or personal use."[126] Furthermore, the review of the messages was limited to the most recent two-month period and only those messages sent during the workday.[127] Noting that the city had explicitly informed police officers that the messages were subject to review and that Quon's law enforcement background should have provided him with an understanding that his actions were subject to review, the Court rejected arguments that the messages were "immune from scrutiny."[128] The Fourth Amendment does not require

121. Quon v. Arch Wireless Operating Co., Inc., 529 F. 3d 892 (9th Cir. 2008).

122. *Id.* at 764–65.

123. *Id.* at 755–56 (citing Camara v. Municipal Court of City and County of San Francisco, 387 U.S. 523, 530 (1967) ("[The] Fourth Amendment's protection extends beyond the sphere of criminal investigations"), and Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 613–14 (1989) ("The Amendment guarantees the privacy, dignity, and security of persons against certain arbitrary and invasive acts by officers of the Government, without regard to whether the government actor is investigating crime or performing another function.")).

124. *Id.* at 759–60 ("[T]he Court would have difficulty predicting how employees' privacy expectations will be shaped by those changes or the degree to which society will be prepared to recognize those expectations as reasonable.").

125. *Id.* at 761. Specifically, citing the framework in its earlier decision in *O'Connor v. Ortega*, 480 U.S. 709 (1987), the Court noted that a government search is permissible if it is "'justified at its inception' and if 'the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of" the circumstances giving rise to the search." *Id.*

126. *Id.*

127. *Id*. at 761–62.

128. *Id.* at 762.

that the government always utilize the *least* intrusive means of conducting a search, but merely that the search was reasonable.[129]

Law enforcement's use of global positioning system ("GPS") trackers has also been the subject of much litigation. In one such case, *United States v. Cuevas-Perez*, the Seventh Circuit was asked to decide an appeal regarding the suppression of evidence gathered by a GPS device without a warrant.[130] Suspecting the defendant was engaged in a drug distribution enterprise, law enforcement agents had attached a GPS device to his car without a warrant to track the location of his vehicle every four minutes.[131] After failing on his suppression motion, the defendant entered a conditional guilty plea for drug distribution.[132] On appeal, the Seventh Circuit affirmed the finding that the warrantless use of the GPS tracker did not violate the defendant's Fourth Amendment rights.[133] Citing prior precedents involving GPS technology,[134] the court in *Cuevas-Perez* concluded that the use of GPS tracking in this instance was limited in scope and did not exceed the bounds permitted under the Fourth Amendment.[135] The court held that the defendant was tracked for only a "single trip" and, therefore, did not rise to the type of consistent ongoing surveillance that was deemed to be a search.[136]

Nonetheless, the court in *Cuevas-Perez* acknowledged that "the meaning of a Fourth Amendment search must change to keep pace with the march of science"[137] to avoid potential overreach by the government and law enforcement.[138] While recognizing that perhaps future forms of GPS tracking in the wrong hands may lead to "abuses fit for a dystopian novel," the court ultimately determined that the type of information that was collected in this case was readily available to the public (i.e., obtainable by observation from public streets, as with

129. *Id.* at 763 (citing Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 654–57 (1995) (noting that the Supreme Court has "repeatedly refused to declare that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment.")).

130. United States v. Cuevas–Perez, 640 F.3d 272 (7th Cir. 2011), *vacated*, 132 S. Ct. 1534 (2012).

131. *Id.*

132. *Id.* at 273.

133. *Id.* at 276.

134. *Id.* at 273–74 (citing United States v. Knotts, 460 U.S. 276 (1983) (holding that the use of a beeper device to track a person on public highways was not a Fourth Amendment search, as there was no expectation of privacy as to a person's movements on such roads); United States v. Garcia, 747 F.3d 994 (7th Cir. 2007) (finding that there was not a search through the use of GPS trackers which is akin to camera surveillance and satellite imaging which do not fall under the categorization of search under the Fourth Amendment). *But cf.* United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010) (holding that the warrantless use of a GPS device for an extended period of twenty-eight days may be a Fourth Amendment violation)).

135. *Id.* at 276.

136. *Id.* at 274–75.

137. *Id.* at 275 (citing *Garcia*, 474 F.3d at 997).

138. *Id.* at 275–76.

traditional law enforcement surveillance) and thus relatively benign.[139]

In light of a circuit split on the issue, the Supreme Court the following year addressed the propriety of the government's attachment of a GPS device on a suspect's car to track his movements in a drug distribution investigation in *United States v. Jones*.[140] Although in this case the government did have a valid warrant to install the GPS device, government agents failed to install the device on the car within the time period and within the jurisdiction of the stated bounds of the warrant.[141] The GPS device ultimately provided the government with twenty-eight days of data detailing the car's location and travels, information which was ultimately used to support the charges that the defendant was involved in a conspiracy to distribute cocaine.[142]

Though the Court's opinion in *Kyllo* required consideration of the contemporary role of the technology being used, which might suggest the ubiquitous nature of GPS to be a relevant factor, the *Jones* decision reminded that the foundational underpinnings of the Fourth Amendment cannot be ignored. The majority opinion in *Jones* found that, irrespective of the expectations of privacy at the time of a search, the Fourth Amendment provides a fundamental minimal level of protection against unreasonable searches.[143] As it had done eighty-four years earlier in *Olmstead*, the Court in *Jones* held that the physical intrusion on the defendant's property and person was sufficient to trigger Fourth Amendment protections, independent of the state of the technology employed to conduct the search;[144] unlike in *Olmstead*, here the Court found that the government had encroached on a "constitutionally protected area."[145] In fact, although the technological means used to track the defendant were central to the facts of the

139. *Id.* (noting that the information that was collected by law enforcement was "real-time information . . . that drivers make available by traversing public roads").

140. United States v. Jones, 132 S. Ct. 945, 948 (2012).

141. *Id.*

142. *Id.*

143. *Id.* at 953 (the standard the Court "appl[ies] is an 18th-century guarantee against unreasonable searches, which we believe must provide at *a minimum* the degree of protection it afforded when it was adopted," not the concurrence's suggestion to "apply *exclusively Katz*'s reasonable-expectation-of-privacy test, even when that eliminates rights that previously existed.").

144. *Id.* (noting that "situations involving merely the transmission of electronic signals without trespass would remain subject to *Katz* analysis"). In her concurrence to the *Jones* decision, Justice Sotomayor recognizes that in certain circumstances, the use of GPS tracking may affect how courts apply the test laid out in *Katz*, since the technology permits law enforcement to tacitly collect a wide range of information about the subject of the tracking and their movements. *Id.* at 956. Such collected information could then be data mined and analyzed by the government to ascertain often very personal aspects of someone's life, without there ever having been a physical intrusion. *Id.*

145. *Id.* at 951–52.

Jones case, the level of advancement in the technology was scarcely mentioned as a determining factor in the majority's decision.[146]

The Court further declined to consider how long a suspect could be tracked with GPS before the tracking would be considered a search (i.e., rejecting the Seventh Circuit's "single trip" factor in *Cuevas-Perez*).[147] The Court held that it would seem illogical to find "that 'relatively short-term monitoring of a person's movements on public streets'" is acceptable, "but that 'the use of longer term GPS monitoring in investigations of *most offenses*' is no good."[148] To find otherwise could effectively prohibit law enforcement from using such technology in cases in which the very nature of the conduct being investigated requires longer periods of surveillance.[149]

In her concurrence in *Jones*, Justice Sonia Sotomayor described her concerns as to the "premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties," particularly in today's society where "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks" such as phone numbers, websites visited, groceries purchased, etc.[150] Much like the majority's observation that bright-line rules may not be appropriate in all cases of GPS use, Justice Sotomayor further warned against the notion that private information provided by people to third parties for certain discrete purposes does not necessarily mean that the desire for privacy for that information has been waived in all instances.[151]

A step beyond GPS tracking of a suspect's vehicle is the alleged ability to conduct audio surveillance of him using his own cell phone as a surreptitious microphone. In *United States v. Oliva*,[152] the Ninth Circuit considered a defendant's arguments that law enforcement had turned his cellular phone into a "roving bug" capable of listening in on conversations even when the phone is not actively connected to a call.[153] Under the Omnibus Crime Control and Safe Streets Act of 1968 ("Omnibus Act"),[154] federal law enforcement officers are required to obtain judicial authorization to "intercept wire, oral and electronic communication."[155] These authorizations may either be

146. *See generally id.* at 954.
147. *Id.* at 954.
148. *Id.* (emphasis in original) (citing Jones v. United States, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring)).
149. *Id.* (noting that "there 'is no precedent for the proposition that whether a search has occurred depends on the nature of the crime being investigated'").
150. *Id.* at 957; *see also Jones*, 132 S. Ct. at 963 (Alito, J., concurring).
151. *Id.*
152. United States v. Oliva, 705 F.3d 390 (9th Cir. 2012).
153. *Id.* at 394, 397.
154. 18 U.S.C. §§ 2510–2522 (2012) [hereinafter Omnibus Act].
155. *Oliva*, 705 F.3d at 394. As the court's decision notes, among the requirements promulgated by the Omnibus Act in the government's application for a valid authorization is "a particular description of the nature and location of the facilities from

"standard," meaning covering a distinct location, or "roving," covering a particular person.[156] Because roving intercepts are more intrusive and capture any communications regardless of the target's location, the statute requires heightened application requirements.[157]

In *Oliva*, the government sought and received electronic surveillance orders to intercept background conversations that could be heard from cellular phones carried by the defendant and other subjects.[158] Oliva moved unsuccessfully to suppress the evidence that he claimed came from roving bugs unauthorized by the orders. Upon government representations that no evidence in the case came from "background conversations from cellular telephones that were powered on, but not connected to . . . a live call,"[159] the recorded conversations gathered from the challenged intercepts were used in the underlying criminal trial and led to the defendant's conviction for drug trafficking.[160]

The Ninth Circuit's evaluation of how to address the government's inclusion of the words "off the hook" in its application for intercept authorization is of particular interest.[161] Although landline phones have "hooks" that allow for the connection or disconnection of the receiver and transmitter from the telephone line,[162] cell phones have no such mechanism and instead rely on software to mimic this functionality. Under the language of the Omnibus Act, the failure of the government to succinctly and clearly define the scope of the authorization sought could have invalidated any resulting intercepts.[163] However, the court ultimately held that even if the defendant's reading of the orders in this case was accepted, no evidence was collected under such circumstances, making the arguable failure of the orders' lan-

---

which or the place where the communication is to be intercepted" so that the court can evaluate whether there is sufficient probable cause that the location being investigated has some relation to a crime. *Id.* at 395 (citing 18 U.S.C. § 2518(1)(b)(ii)).

156. *Id.* at 396.

157. *Id.*

158. *Id.*

159. *Id.* The court in *Oliva* did acknowledge that the language contained in the government's application for the intercepts under the Omnibus Act ("[B]ackground conversations intercepted in the vicinity of [a target phone number] while the telephone is off the hook or otherwise in use. . .") was sufficient to capture the type of remote surreptitious eavesdropping that the defendant argued had occurred in this case. *Id.*

160. *Id.* at 394, 397–98. While the government did not confirm that such technology existed, nor did the court make a determination as to the defendant's contentions, the court noted that such technologies were the subject of a 2006 news article, and a case from the Southern District of New York. *Id.* at 398 (citing Declan McCullagh & Anne Broache, *FBI taps cell phone mic as eavesdropping tool*, CNET (Dec. 1, 2006), http://news.cnet.com/FBI-taps-cell-phone-mic-as-eavesdropping-tool/2100-1029_3-6140191.html; United States v. Tomero, 462 F. Supp. 2d 565, 567 (S.D.N.Y. 2006)).

161. *Id.* at 398–99.

162. *Id.* at 398 (citing CYRIL M. JANSKY & DANIEL C. FABER, PRINCIPLES OF THE TELEPHONE 5 (1916)).

163. *See id.* at 400.

guage to meet statutory requirements harmless error.[164] Despite not evaluating the propriety of new or emerging technologies in light of *Kyllo*, the court recognized the need for and importance of specificity and clarity to avoid future similar situations, and to "take account of more sophisticated systems that are already in use or in development."[165]

Finally, law enforcement agents' use of software to locate a computer that had been connecting to a neighbor's WiFi network to facilitate the exchange of child pornography gave rise to *United States v. Stanley* in the Third Circuit.[166] During the district court proceedings, the defendant argued that the use of the software to conduct the search was unlawful under *Kyllo*.[167] The district court rejected this argument, finding that the defendant had no expectation of privacy in the WiFi signal that his computer sent out of the home, particularly where affirmative actions by the defendant were necessary to initiate the signal.[168] On appeal, while the Third Circuit acknowledged that the technology in this case in some ways mirrored the technology used in *Kyllo* (e.g., it was sense enhancing, examined into the interior of the defendant's home, and was not generally available technology),[169] the court nonetheless found the search valid because the defendant made no efforts to limit his illegal activities to the interior of his home.[170] The court therefore declined to extend defendant's claimed privacy rights to the signal simply because it was initiated from his home and, further noted that the unauthorized Internet signal was not something society would consider to be subject to a reasonable expectation of privacy.[171]

III. FISA AND THE NATIONAL SECURITY "WALL"

Importantly, the fact patterns of every case discussed above are what can colloquially be considered "regular," "traditional," even "standard" criminal cases, and thus the Fourth Amendment jurispru-

164. *Id.* at 399–400.

165. *Id.* at 399 (citing *Kyllo*, 533 U.S. at 36).

166. U.S. v. Stanley, 753 F.3d 114, 119 (3d Cir. 2014). In *Stanley*, police used "MoocherHunter" software in conjunction with a laptop and directional antennae to locate and track back the unique signal being sent out by the defendant's computer to the defendant's apartment complex. *Id.* at 117. After narrowing the presumed location of the signal to the defendant's home, police secured a search warrant for the home and found the defendant's computer, which matched the specifications of the computer connecting to the neighbor's WiFi router. *Id.*

167. *Id.*

168. *Id.* at 117–18.

169. *Id.* at 119.

170. *Id.* at 120.

171. *Id.* at 120–21.

dence is properly understood to apply in that context.[172] None of those cases dealt with national security, intelligence, or counterterrorism investigations. The Supreme Court even expressly reserved the question of national security cases as separate and apart from its Fourth Amendment holding in *Katz*.[173] Indeed, in the twentieth century, only one Supreme Court opinion addressed the constitutionality of intelligence surveillance head-on[174]—the 1972 case *United States v. U.S. District Court*,[175] commonly known as "the *Keith* case," named after Judge Damon Keith, the U.S. district judge subject to the mandamus petition litigated all the way to the high court. In the underlying case, the government had charged three members of the radical White Panther Party with conspiracy to destroy government property; one of them, Lawrence Plamondon was also charged with bombing an office of the Central Intelligence Agency in Michigan.[176] Some evidence in the case was obtained via warrantless electronic surveillance. Judge Keith found that such surveillance violated the Fourth Amendment, notwithstanding provisions of the Omnibus Act,[177] passed in part as a response to the *Katz* decision the year before, that expressly exempted from the warrant requirement investigations targeting foreign powers and those who attempt to overthrow the government by violence or illegal means.[178] He ordered the government to disclose

172. The Supreme Court has distinguished "ordinary crime" from cases involving security concerns. *See* United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 322 (1972).

173. *Katz*, 389 U.S. at 358 n.23.

174. In *Gouled v. United States*, 255 U.S. 298 (1921), the Supreme Court found that U.S. Army intelligence personnel's physical intrusion into the barracks of the defendant violated the defendant's Fourth Amendment rights. Although this case did involve intelligence, rather than law enforcement personnel, the Fourth Amendment finding was based upon the physical intrusion and trespass, rather than remote or electronic surveillance. Opinions of the Foreign Intelligence Surveillance Court (FISC), under the framework of the Foreign Intelligence Surveillance Act of 1978 (FISA), are discussed below.

175. *Keith*, 407 U.S. 297.

176. *Id.* at 299–300.

177. Omnibus Act, Pub. L. 90-351.

178. *Id.* at § 2511(3) ("Nothing contained in this chapter [generally prohibiting, subject to criminal prosecution, wiretapping or surveilling communications without a warrant] or in section 605 of the Communications Act of 1934 (48 Stat. 1143; 47 U.S.C. 605) shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities. Nor shall anything contained in this chapter be deemed to limit the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government. The contents of any wire or oral communication intercepted by authority of the President in the exercise of the foregoing powers may be received in evidence in any trial hearing, or other proceeding only where such interception was reasonable, and shall not be otherwise used or disclosed except as is necessary to implement that power.").

to the defense the relevant materials concerning the monitored communications. In so ruling, Judge Keith wrote:

> An idea which seems to permeate much of the Government's argument is that a dissident domestic organization is akin to an unfriendly foreign power and must be dealt with in the same fashion. There is great danger in an argument of this nature for it strikes at the very constitutional privileges and immunities that are inherent in United States citizenship.[179]

The government sought a writ of mandamus from the Sixth Circuit to order Judge Keith to vacate his order; the Court of Appeals denied the petition.[180] The Supreme Court, after determining Congress had not legislated with respect to national security surveillance,[181] applied the Fourth Amendment to *domestic* surveillance for *domestic* security purposes[182] and affirmed the intermediate court's decision. The Court expressly reserved the question of the Fourth Amendment's applicability to foreign intelligence surveillance.[183]

---

179. United States v. Sinclair, 321 F. Supp. 1074, 1079 (D. Mich. 1971). In arguing the surveillance was both lawful and non-discoverable in this and other cases at the time, *see, e.g.*, United States v. Smith, 321 F. Supp. 424 (C.D. Cal. 1971), the government relied heavily on historic executive branch practice in exercise of the President's national security powers, in particular a confidential 1940 memorandum by President Roosevelt authorizing the Attorney General to allow warrantless wiretapping in limited instances. *Smith*, 321 F. Supp. at 431 ("You are, therefore, authorized and directed in such cases as you may approve, after investigation of the need in each case, to authorize the necessary investigation agents that they are at liberty to secure information by listening devices direct to the conversation or other communications of persons suspected of subversive activities against the Government of the United States . . . ."). For the complete text and subsequent history of, and more thorough discussions about the Roosevelt directive, see *Smith*, 321 F. Supp. 427–32; Neal K. Katyal & Richard Caplan, *The Surprisingly Stronger Case for the Legality of the NSA Surveillance Program: The FDR Precedent*, 60 STANFORD L. REV. 1023 (2008).

180. United States v. U.S. Dist. Court, 444 F.2d 651 (6th Cir. 1971), *aff'd*, 407 U.S. 297 (1972).

181. *Keith*, 407 U.S. at 306.

182. *Id.* at 320 ("[W]e do not think a case has been made for the requested departure from Fourth Amendment standards. The circumstances described do not justify complete exemption of domestic security surveillance from prior judicial scrutiny. Official surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech. Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent. We recognize, as we have before, the constitutional basis of the President's domestic security role, but we think it must be exercised in a manner compatible with the Fourth Amendment. In this case we hold that this requires an appropriate prior warrant procedure.").

183. *Id.* at 321–22 ("We emphasize, before concluding this opinion, the scope of our decision. As stated at the outset, this case involves only the domestic aspects of national security. We have not addressed and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents. Nor does our decision rest on the language of [§] 2511(3) or any other section of Title III of the Omnibus Crime Control and Safe Streets Act of 1968. That Act does not attempt to

Shortly thereafter, the New York Times began publishing articles concerning what would become known as the CIA's Family Jewels—a series of internal reports by the CIA's own personnel that alleged wrongdoing within the agency, including certain surveillance practices.[184] Several oversight bodies were quickly established within the government, including the President's Commission on CIA Activities within the United States (known as the Rockefeller Commission, named after its chair Vice President Nelson Rockefeller, which included in its membership future President Ronald Reagan), the Pike Committee in the House of Representatives, and the Church Committee in the Senate,[185] all of which compiled evidence and some of which issued reports on deemed "CIA abuses."

This combination of events led to the passage of the Foreign Intelligence Surveillance Act of 1978 ("FISA"),[186] which, among other things, created the Foreign Intelligence Surveillance Court ("FISC") to oversee government surveillance of wire communications.[187] This statutory regime requires the government to obtain a FISC *order*, not

---

define or delineate the powers of the President to meet domestic threats to the national security.").

184. Seymour M. Hersch, *Huge C.I.A. Operation Reported in U.S. Against Antiwar Forces, Other Dissidents in Nixon Years*, N.Y. TIMES, Dec. 22, 1974, at 1, 26; Karen DeYoung and Walter Pincus, *CIA to Air Decades of Its Dirty Laundry*, WASH. POST (June 22, 2007), http://www.washingtonpost.com/wp-dyn/content/article/2007/06/21/AR2007062102434.html.

185. The latter two were the precursors to House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, respectively, which would be formally created by the Foreign Intelligence Surveillance Act (FISA). Both before and after FISA, the Department of Justice also promulgated a series of guidelines that would govern how the FBI conducted security investigations. For a discussion on the most important of these, see William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1, 68–74 (2000).

186. Pub. L. 95–511, 92 Stat. 1783, 50 U.S.C. ch. 36. Although this Article discusses electronic surveillance only, since 1994, FISA also governs certain physical searches for the purpose of collecting foreign intelligence information. *See* Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, 108 Stat. 3423 § 302(a)(1) (1994) (codified as amended at 50 U.S.C. § 1822 (Supp. IV 1998)). For a thorough discussion on FISA's history and parameters prior to the September 11, 2001 attacks, see Banks & Bowman, *supra* note 185. This excellent article was published less than a year prior to the 9/11 attacks by recognized national security law scholar Professor Banks, and former senior FBI lawyer Spike Bowman. As such, it reflects great scholarship, though readers should be aware that, because of its timing and the sensitivities of its subject matter, its completeness was limited to unclassified information. As noted below, important regulations concerning the sharing of information between intelligence and law enforcement personnel, critical to understanding certain aspects of how certain collected intelligence may be used, were classified at that time. It is nevertheless a commendable article that serves as a learned primer on the status of foreign intelligence surveillance at that time.

187. Several states also passed laws restricting police monitoring of political and other groups. *See, e.g.*, Matthew Waxman, *Police and National Security: American Local Law Enforcement and Counterterrorism After 9/11*, 3 J. NAT. SEC. L. & POL'Y 377, 397 (2009).

a warrant, in certain instances where it desires to collect foreign intelligence information.[188] As originally defined, "foreign intelligence information" means:

> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—
>
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> (B) sabotage or international terrorism by a foreign power or an agent of a foreign power;[189] or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—
>
> (A) the national defense or the security of the United States; or
>
> (B) the conduct of the foreign affairs of the United States.[190]

Such information may be collected under FISA against targets for which or whom there is probable cause[191] to believe they are a "foreign power"[192] or "agent of a foreign power."[193] Targets were generally envisioned to be foreign governments or people working on their

188. *See* 50 U.S.C. § 1803(a) (2012).

189. Subsection (e)(1)(B) has since been amended to include information relating to protection against international proliferation of weapons of mass destruction. *See* 50 U.S.C. § 1801(e)(1)(B) (2012).

190. *See* Pub. L. 95-511 at § 101(e) (codified at 50 U.S.C. § 1801(e)).

191. 50 U.S.C. § 1805(a).

192. As defined in the original version of FISA, "foreign power" meant:

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

Pub. L. 95-511 § 101(a).

193. FISA's original definition of "agent of a foreign power" was:

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

behalf against the interests of the United States, either inside its borders or overseas. At the same time, the statute accounted for "group[s] engaged in international terrorism,"[194] although establishing that a group qualified for that designation was not straightforward. As the Department of Justice's Office of the Inspector General ("OIG") explained:

> Whether a terrorist organization qualified as a "foreign power" under the FISA statute depended upon the intelligence developed about the group and its activities, and whether the FISA Court was convinced that the government had proven that the entity existed and was engaged in international terrorist activities. In practice, once the FBI developed the necessary intelligence about the existence of a terrorist organization, a particular subject was used as a "test subject" for pleading to the FISA Court that the organization was a foreign power. Although not dispositive, FISA applications might reference the fact that the State Department had designated an entity as a "foreign terrorist organization" [under the Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104-132 § 302].[195]

---

the conduct of such activities or knowingly conspires with any person to engage in such activities; or

(2) any person who—

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States;

(C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power; or

(D) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

Id. at § 101(b).

194. *Id.* at § 101(a)(4). "International terrorism" was and still is defined in the statute as activities that:

(1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State;

(2) appear to be intended—

(A) to intimidate or coerce a civilian population;

(B) to influence the policy of a government by intimidation or coercion; or

(C) to affect the conduct of a government by assassination or kidnapping; and

(3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

Id. at § 101(c).

195. *A Review of the FBI's Handling of Intelligence Information Related to the September 11 Attacks (Unclassified Version)*, UNITED STATES DEPARTMENT OF JUSTICE,

Furthermore, FISA required a Senate-confirmed official to certify that the purpose of surveillance was to obtain foreign intelligence information[196] and included additional safeguards for United States persons, including that they could not become surveillance targets "solely upon the basis of activities protected by the First Amendment."[197]

Despite the safeguards, the regime codified by FISA was never meant to mimic the Fourth Amendment standards that would be applied in criminal cases. Although Congress "anticipated that evidence of criminal conduct uncovered during FISA surveillance would be provided to criminal investigators,"[198] concerns arose within the Department of Justice ("DOJ") when criminal defendants began to challenge prosecutors' use of information collected pursuant to FISA orders.[199] Thus, in the 1980s, DOJ began to limit prosecutors' involvement in intelligence investigations to help ensure it could prove in court that any FISA-derived evidence used was collected in the course of an investigation whose "primary purpose" was intelligence collection.[200] This measure was designed with the idea of keeping criminal prosecutions untainted by intelligence gathering methods, notwithstanding the deference Courts of Appeals implicitly afforded FISC judges in their determinations about the purpose of the surveillance when issuing their orders.[201]

During the investigation into Aldrich Ames' espionage activities in 1993–1994, DOJ's office that litigated FISA applications, the Office of Intelligence Policy and Review (OIPR), became "concerned that no guidelines governed the contacts" between DOJ's Criminal Division and the FBI.[202] A series of memoranda from OIPR proposed the formal creation of a "wall" between not only intelligence investigators

---

OFFICE OF THE INSPECTOR GENERAL 45–46 (2006), *available at* http://fas.org/irp/agency/doj/oig/fbi-911/ [hereinafter DOJ OIG REPORT].

196. Pub. L. 95-511 § 104(a)(7) (codified at 50 USC § 1804(a)(7)).

197. *Id.* § 1805(a)(3)(A).

198. DOJ OIG REPORT, *supra* note 195, at 22 (citing S. 1566, 95th Congress, 2d Session, Report 95-701, Mar. 14, 1978); *see also* United States v. Duggan, 743 F.2d 59, 78 (2d Cir. 1984) ("Congress recognized that in many cases the concerns of government with respect to foreign intelligence will overlap with those with respect to law enforcement.").

199. *See, e.g.*, United States v. Truong Dinh Hung, 629 F.2d 908 (4th Cir. 1980); United States v. Pelton, 835 F.2d 1067 (4th Cir. 1987); United States v. Johnson, 952 F.2d 565 (1st Cir. 1991).

200. *See* DOJ OIG REPORT, *supra* note 195, at 22.

201. *See also* Banks & Bowman, *supra* note 185, at 84–85 ("Although the surveillance in each [case in which criminal defendants raised challenges to the purpose of the surveillance used when gathering evidence against them] was conducted by the FBI, rather than one of the pure intelligence agencies, the government's defense of its surveillance was aided by the prophylactic protection afforded by a FISC judge's prior approval of the surveillance."); DOJ OIG REPORT, *supra* note 195, at 27 (describing a January 1995 opinion of DOJ's Office of Legal Counsel that noted the courts "had shown great deference to the government in challenges to evidence gathered through intelligence searches that was used in criminal prosecutions").

202. DOJ OIG REPORT, *supra* note 195, at 25.

and prosecutors but also between intelligence and criminal investigators within the FBI.[203] During the subsequent development and drafting of intelligence sharing procedures, significant tumult resulted between OIPR, the Criminal Division, and the FBI,[204] as well as the United States Attorney's Office for the Southern District of New York ("SDNY") and the Office of the Deputy Attorney General.[205] The latter development resulted from a memorandum sent by Deputy Attorney General Jamie Gorelick to United States Attorney Mary Jo White in the midst of the SDNY's investigation into Omar Abdel-Rahman and the 1993 bombing of the World Trade Center.[206] Gorelick wrote that "during the course of [the Rahman and related counterterrorism] investigations significant counterintelligence information [had] been developed relating to the activities and plans of agents of foreign powers operating in this country and overseas, including previously unknown connections between separate terrorist groups."[207] It was thus decided to "initiate[ ] a separate full field counterintelligence investigation," which led Gorelick to inform White that the pen registers then in place in SDNY's criminal investigation would be discontinued, and all FBI memoranda and investigative reports would be segregated and those relating to potential future attacks would not be provided to criminal investigative agents or prosecutors.[208] "These procedures," Gorelick noted, "go beyond what is legally required."[209]

In response, White wrote directly to Attorney General Janet Reno that "the FBI labels of an investigation as intelligence or law enforcement can be quite arbitrary" and that "the most effective way to combat terrorism is with as few labels and walls as possible."[210] In response to the draft instructions shared with her, White said:

---

203. *Id.* at 26.

204. *See id.*

205. *See generally* FURTHER INTERNAL JUSTICE DEPT CORRESPONDENCE FROM 1995 ON THE SEPARATION OF CERTAIN FOREIGN COUNTERINTELLIGENCE AND CRIMINAL INVESTIGATIONS, AND THE ROLE OF DEPUTY ATTORNEY GENERAL GORELICK, DEP'T OF JUSTICE (released Apr. 2004) [hereinafter DOJ CORRESPONDENCE] (compiling a series of memoranda between DOJ and United States Attorney Mary Jo White concerning the draft procedures, declassified by James Baker, the Counsel for Intelligence Policy, on April 10, 2004), *available at* http://fas.org/irp/agency/doj/1995_wall.pdf.

206. Memorandum from Jamie S. Gorelick, Deputy Att'y Gen. to May. Jo White, U.S. Att'y S.D.N.Y., *et al. in* DOJ CORRESPONDENCE, *supra* note 205 (discussing instructions on separation of certain foreign counterintelligence and criminal investigations).

207. *Id.*

208. *Id.* at 3.

209. *Id.* at 2.

210. Memorandum from Mary Jo White, U.S. Att'y S.D.N.Y. to Janet Reno, U.S. Att'y Gen. *in* DOJ CORRESPONDENCE, *supra* note 205 (discussing Instructions on foreign intelligence and foreign counterintelligence Investigations).

> It is hard to be totally comfortable with instructions to the FBI prohibiting contact with the United States Attorney's Offices when such prohibitions are not legally required. These instructions leave entirely to OIPR and the Criminal Division when, if ever, to contact affective U.S. Attorneys on investigations including terrorism and espionage. . . .
> . . . [T]here should be an obligation on the Criminal Division so that U.S. Attorneys are made aware of potential criminal activity in their districts at the earliest possible—and permissible— time."[211]

Accepting some of White's suggestions and rejecting others, the Attorney General formally adopted a set of intelligence-sharing procedures a month later, requiring that OIPR and the Criminal Division each had to concur with an FBI field office's request to inform its respective U.S. Attorney's Office of a potential criminal action.[212] Over the next two years, the FBI also erected its own internal wall that separated intelligence and criminal agents, and in 1997 descriptions of the procedures used to wall-off criminal investigators was included in FISA applications, presumably to help OIPR establish that the "primary purpose" of the requested surveillance would be for intelligence-collection purposes.[213]

The evolving practice led to turf battles and confusion within different DOJ components (including the FBI) and between DOJ and the FISA court. In the little more than six years between the promulgation of the 1995 procedures and the September 11, 2001, terrorist attacks (which included the bombings of the U.S. embassies in Kenya and Tanzania in 1998 and the USS COLE in 2000), at least three separate government reports found fault with how they were implemented. A 1999 DOJ OIG report found that FBI intelligence agents "exhibited undue reluctance to disseminate intelligence information" outside their ranks;[214] a team created by the Attorney General reported that "soon after the 1995 Procedures were implemented, OIPR prevented the FBI from contacting the Criminal Division in contravention of the requirements of the procedures;"[215] the General Accounting Office (now the Government Accountability Office) similarly reported a dearth of contact between the FBI and Criminal Division because of OIPR's and FBI's concerns about FISA applica-

211. *Id.*

212. DOJ OIG REPORT, *supra* note 195, at 28–29.

213. *See id.* at 30–31.

214. *See* U.S. DEP'T OF JUSTICE AND OFFICE OF THE INSPECTOR GEN., SPECIAL REPORT: THE HANDLING OF FBI INTELLIGENCE INFORMATION RELATED TO THE JUSTICE DEPARTMENT'S CAMPAIGN FINANCE INVESTIGATION § 5(A)(2) (July 1999), *available at* http://www.justice.gov/oig/special/9907.htm.

215. DOJ OIG REPORT, s*upra* note 195, at 34 ((referring to The Bellows Report) OFFICE OF THE ATTORNEY GENERAL, *Final Report: Attorney General's Review Team on the Handling of the Los Alamos National Laboratory Investigation* 708, 710 (May 2000), *available at* http://fas.org/irp/ops/ci/bellows/).

tions.[216] Likewise, beginning in 2000, the FISC also began to impose restrictions on intelligence sharing in response to a series of errors on FISA applications that misrepresented the walling-off procedures being used in several cases.[217]

It would not be long before these classified deliberations came to light as smoke from the terror attacks of September 11, 2001, began to clear, Americans' shock turned to anger, and they began to seek accountability for that tragedy. The law enforcement/intelligence wall became an instant focus of oversight panels. A joint inquiry by the congressional intelligence committees found that, by wedging itself between the law enforcement and intelligence functions of the government, the wall lead to "a diminished level of coverage of suspected al-Qa'ida operatives in the United States."[218] Indeed, a month before the attacks, an agent in the FBI's New York Field Office learned that two of the hijackers were in the United States.[219] The DOJ Office of the Inspector General concluded, simply, that "because of the wall, in August 2001 when the New York FBI learned that [the two hijackers] were in the United States, criminal investigators were not allowed to participate in the search for them."[220]

Notwithstanding the later conclusion of the National Commission on Terrorist Attacks Upon the United States (also known as the 9/11 Commission) that even a combined law enforcement and intelligence search for those hijackers would have required "luck as well as skill" to find them in time to stop the attacks,[221] the political conditions of the 1970s that led to measures to cabin the intelligence community had evaporated and within a month and a half of the attacks the wall, as it had existed, was down. The October 26, 2001 enactment of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act, also known as the Patriot Act), *inter alia*, amended the FISA section requiring certification that *the* purpose of FISA surveillance would be to obtain foreign intelligence information to instead require only that those ends be "a significant purpose" of the surveil-

216. U.S. GEN. ACCOUNTING OFFICE, FBI INTELLIGENCE INVESTIGATIONS: COORDINATION WITHIN JUSTICE ON COUNTERINTELLIGENCE CRIMINAL MATTERS IS LIMITED (July 2001), *available at* http://www.gao.gov/assets/240/232031.pdf.

217. *See* DOJ OIG REPORT, *supra* note 195, at 36–38.

218. U.S. SENATE SELECT COMM. ON INTELLIGENCE AND U.S. HOUSE PERMANENT SELECT COMM. ON INTELLIGENCE, JOINT INQUIRY INTO INTELLIGENCE COMMUNITY ACTIVITIES BEFORE AND AFTER THE TERRORIST ATTACKS OF SEPTEMBER 11, 2001, S. Rep. No. 107-351, H.R. Rep. No. 107-792, at xvii (2002) (pagination from unclassified version of report).

219. NATIONAL COMM'N ON TERRORIST ATTACKS UPON THE U.S., 9/11 COMMISSION REPORT 269–72 (2004) [hereinafter 9/11 COMMISSION REPORT].

220. DOJ OIG REPORT, s*upra* note 195, at 22.

221. 9/11 COMMISSION REPORT, *supra* note 219, at 272.

lance.[222] The law also permitted the FISC to authorize roving wiretaps[223] and further included what pejoratively became known as the "library records" provision, permitting the FBI to seek FISA orders "requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence" and providing that the individual required to produce such items keep the request and production confidential.[224]

Several other major national security initiatives followed in rapid succession, including the Intelligence Reform and Terrorism Prevention Act of 2004,[225] which permitted greater flexibility with regard to surveillance of persons who may not be acting as an agent of an international terrorist group, often called "lone wolves;"[226] the short-lived Protect America Act of 2007;[227] and the FISA Amendments Act of 2008, which granted broad authority to target for surveillance persons outside the United States[228] and broadened the pool of potential officials who can certify a FISA application to include the Deputy Director of the FBI, if designated by the President as a certifying official (which President Obama chose to do in Executive Order 13475).[229]

IV. Evolving Social Norms and Acceptance of Sacrifices to the Right to Privacy

As the Supreme Court recognized in *Quon*, "rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior."[230] Society is currently in the midst of tremendous change with respect to technology and how these advancements affect our daily lives. The increasingly ubiquitous nature of the Internet and the rise of the sharing economy have resulted in individuals more readily

222. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Pub. L. 107-56 § 218, 115 Stat. 272, 291 (2001) (codified at 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B)).

223. *Id.* at § 206 (codified at 50 U.S.C. § 1805(c)(2)(B)).

224. *Id.* at § 215 (codified at 50 U.S.C. § 1861).

225. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458, 118 Stat. 3638 (2004).

226. *Id.* at § 6001 (codified 50 U.S.C. § 1805(c)(2)(B)).

227. Protect America Act of 2007, Pub. L. 110-55, 121 Stat. 552 (2007). By its own terms, the Protect America Act was only in effect for six months. *See id.* at § 6(c).

228. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 Pub. L. 110-261 at § 101(a)(2), 122 Stat. 2436 (amending Foreign Intelligence Surveillance Act of 1978 (FISA) (2008); § 702 (codified at 50 U.S.C § 1881a) (providing "[p]rocedures for targeting certain persons outside the United States other than United States persons").

229. *Id.* § 104(1)(D)(ii) (for electronic searches); *id.* § 107(a)(1)(E)(ii) (for physical searches).

230. City of Ontario, Cal.v. Quon, 560 U.S. 746, 748 (2010).

sharing historically private information.[231] Total strangers can now utilize services that would allow them to stay in your home (e.g., AirBNB and VRBO), hitch a ride in your car (e.g., Uber and Lyft), or rent your car completely (e.g., RelayRides and FlightCars).[232]

The Supreme Court's jurisprudence has demonstrated that a key component of a constitutionally permissible warrantless search or seizure is whether it violates a reasonable expectation of privacy. This standard has become more difficult to apply in modern practice, particularly in the area of social media and online networks, where public use and applications have often provided contrary and diametrically opposed viewpoints of the definition of "reasonable." As discussed below, in the battle between privacy and convenience, the increased acceptance of permissive storage of personal information with third parties, and the prevalence of online social media activity, convenience appears to be winning. With this arguably resulting in a lower threshold of the privacy one can reasonably expect, it would seem directly to impact Fourth Amendment analysis.

A. *Private/Corporate Surveillance and Data Collection Capabilities*

In today's data-driven environment, every email, social media post, online purchase, and all web traffic generated by an individual has value to private companies,[233] particularly Internet-based marketers and advertisers because it allows them to provide more effective, nuanced, timely, and targeted ads to users in hopes of generating sales.[234] Analysis of the information may involve a review of intimate

231. *See, e.g.*, Jason Tanz, *How Airbnb and Lyft Finally Got Americans to Trust Each Other*, WIRED (Apr. 23, 2014, 6:30 AM), http://www.wired.com/2014/04/trust-in-the-share-economy/; *The Rise of the Sharing Economy,* ECONOMIST (Mar. 9, 2013), http://www.economist.com/news/leaders/21573104-internet-everything-hire-rise-sharing-economy; TOMIO GERON, *Airbnb and the Unstoppable Rise of the Sharing Economy*, FORBES (Feb. 11, 2013), http://www.forbes.com/sites/tomiogeron/2013/01/23/airbnb-and-the-unstoppable-rise-of-the-share-economy/; Lyndsey Gilpin, *We-commerce: The Sharing Economy's Uncertain Path to Changing the World*, TECHREPUBLIC, http://www.techrepublic.com/article/we-commerce-the-sharing-economys-uncertain-path-to-changing-the-world/ (last visited Mar. 13, 2015).

232. *See* sources cited *supra* note 231.

233. Elizabeth Dwoskin, *Study: Digital Marketing Industry Worth $62 Billion*, WALL ST. J., DIGITS BLOG, (Oct. 14, 2013, 4:40 PM), http://blogs.wsj.com/digits/2013/10/14/study-digital-marketing-industry-worth-62-billion/ (describing a report by a trade group, the Direct Marketing Association, finding that the online marketing industry was a $62 billion dollar industry).

234. Tanzina Vega, *New Ways Marketers Are Manipulating Data to Influence You*, N.Y. TIMES, June 20, 2013, at F2; Joshua Bernstein, *Start-Ups Seek to Help Users Put a Price on Their Personal Data*, N.Y. TIMES, Feb. 13, 2012, at B3; Stephanie Clifford, *Your Online Clicks Have Value, for Someone Who Has Something to Sell*, N.Y. TIMES, Mar. 26, 2009, at B9; Cecilia Kang, *Google to Put User Photos, Comments in Online Ads*, WASH. POST, (Oct. 11, 2013), http://www.washingtonpost.com/business/technology/google-to-put-user-photos-comments-in-online-ad-endorsements/2013/10/11/322e483e-3289-11e3-8627-c5d7de0a046b_story.html; Sarah Frier, *Facebook To Track Users Across Devices to Study Shopping Habits*, BLOOMBERG (Aug. 13, 2014, 12:00

information about an individual, leading to growing concern about the privacy interests of such activity.[235]

For instance, most commercial websites today include a link to the company's privacy policy on its homepage, which provides the site's users and visitors with a description of the type of information that the website collects,[236] likely to include the user's Internet Protocol address, the type of web browser used to access the website, and the specific pages on that website which a user visits.[237] The policies also offer a general description of what companies do with this information once collected, including, for example, how the company anticipates using such collected data internally and how such information may be shared with other parties.[238]

As people have become more cognizant of and sensitive to the use of their online data, they have tended to react adversely when they think a company's privacy policy exceeds acceptable norms. In 2013, Facebook was forced to delay the implementation and roll out of its revised privacy policy after public comments[239] raised concerns that the new policy did not adequately protect user's personal information.[240] Similar disapproval has been expressed regarding Google,[241]

PM), http://www.bloomberg.com/news/articles/2014-08-13/facebook-to-track-users-across-devices-to-study-shopping-habits.

235. *See, e.g.*, Bernstein, *supra* note 234; Mike Swift, *Battle Brewing Over Control of Personal Data Online*, SAN JOSE MERCURY NEWS, June 28, 2011, at A2, *available at* http://www.mercurynews.com/ci_18349132 (June 26, 2011); Cecilia Kang, *Google Tracks Consumers' Online Activities Across Products and Users Can't Opt Out*, WASH. POST, (Jan. 24, 2012), http://www.washingtonpost.com/business/technology/google-tracks-consumers-across-products-users-cant-opt-out/2012/01/24/gIQArgJHOQ_story.html.

236. *See, e.g.*, Google Privacy Policy, *available at* https://www.google.com/intl/en/policies/privacy/?fg=1 (last modified Dec. 19, 2014).

237. *Id.*

238. *Id.*

239. *See, e.g.*, *Comments from Facebook Users, Proposed Updates to Our Governing Documents*, FACEBOOK, (Aug. 29, 2013, 9:22 AM), http://web.archive.org/web/20131119201649/https://www.facebook.com/notes/facebook-site-governance/proposed-updates-to-our-governing-documents/10153167395945301 (accessed through web-archive); Letter from Marc Rotenberg, Exec. Dir., Elec. Privacy Info. Ctr.et al. to Edith Ramirez et al., the Fed. Trade Comm'n (Sept. 4, 2013) (regarding Facebook's Changes Regarding Sponsored Stories), *available at* http://graphics8.nytimes.com/packages/pdf/technology/privacy-groups-letter-ftc.pdf; Drew Guarini, *Hold Your Gasps, Facebook Is Under Fire For Its Privacy Policy Again*, HUFFINGTON POST (Sept. 5, 2013, 1:15 PM), http://www.huffingtonpost.com/2013/09/05/facebook-privacy-ftc_n_3873764.html.

240. *See, e.g.*, Vindu Goel & Edward Wyatt, *Facebook Privacy Change Is Subject to F.T.C. Inquiry*, NY TIMES (Sept. 11, 2013), http://www.nytimes.com/2013/09/12/technology/personaltech/ftc-looking-into-facebook-privacy-policy.html (Sept. 11, 2013) (relaying the comments of Senator Edward Markey, D-MA: "This troubling shift in policy raises a number of questions about whether Facebook is improperly altering its privacy policy without proper user consent and, if the changes go into effect, the degree to which Facebook users will lose control over their personal information"); *Facebook Delays Controversial Privacy Policy Change*, HUFFINGTON POST (Sept. 6,

Fitbit,[242] and AT&T's[243] privacy policies, and critics question whether such policies contain sufficient safeguards for protecting sensitive user information.

Public awareness of companies' use of their personal information and website activities also has opened the door to new privacy concerns. Web browsers now include options to help users limit information sharing about their website visits and history on a particular computer, along with other potentially identifying information that the software may otherwise retain.[244] Additionally, such software often includes options to block or limit the use of digital "cookies,"[245] which websites use to passively track users' activities.[246]

2013, 11:49 AM), http://www.huffingtonpost.com/2013/09/06/facebook-privacy-policy-change_n_3880288.html.

241. Google has been subject of significant investigations by European regulators over the company's user privacy responsibilities. *See e.g.*, Sam Schechner, *EU Privacy Watchdogs Warn Google About Its Policy*, WALL ST. J. (Sept. 25, 2014, 1:27 PM), http://www.wsj.com/articles/eu-privacy-watchdogs-warn-google-about-its-policy-1411666047; Danny Hakim, *Google Is Target of European Backlash on U.S. Tech Dominance*, N.Y. TIMES (Sept. 8, 2014), http://www.nytimes.com/2014/09/09/technology/google-is-target-of-european-backlash-on-us-tech-dominance.html; Charles Arthur, *Google Facing Legal Threats from Six European Countries Over Privacy*, GUARDIAN (Apr. 2, 2013, 12:53 PM), http://www.theguardian.com/technology/2013/apr/02/google-privacy-policy-legal-threat-europe. The company was alleged to have violated privacy rules in a number of countries including France and Spain. Arthur, *supra*.

242. Laura Ryan, *Fitbit Hires Lobbyists After Privacy Controversy*, NAT'L J. (Sept. 15, 2014), http://www.nationaljournal.com/tech/fitbit-hires-lobbyists-after-privacy-controversy-20140915.

243. Drew Guarini, *AT&T Is Going To Start Selling Your Data; So Here's How You Can Opt Out*, HUFFINGTON POST (July 8, 2013, 12:05 PM), http://www.huffingtonpost.com/2013/07/08/att-selling-data_n_3561263.html.

244. The feature has become ubiquitous among many popular web browsers, with each developer including information about how to utilize the functionality in the product descriptions. *See, e.g.*, *Browse in private (incognito mode)*, GOOGLE, https://support.google.com/chrome/answer/95464?hl=en (last visited Jan. 12, 2015); *Private Browsing - Browse the Web Without Saving Information About the Sites You Visit*, MOZILLA, *available at* https://support.mozilla.org/en-US/kb/private-browsing-browse-web-without-saving-info (last visited Jan. 12, 2015); *What is In Private Browsing?*, MICROSOFT, *available at* http://windows.microsoft.com/en-us/windows/what-is-inprivate-browsing#1TC=windows-7 (last visited Jan. 11, 2015).

245. *See, e.g.*, *How to Block Tracking Cookies*, WASH. POST (July 17, 2005), http://www.washingtonpost.com/wp-dyn/content/article/2005/07/16/AR2005071600111.html (describing how many of the common internet web browsing software contain options to stop tracking cookies).

246. *See* Adam Tanner, *The Web Cookie is Dying. Here's the Creepier Technology That Comes Next*, FORBES (June 17, 2013, 12:29 PM), http://www.forbes.com/sites/adamtanner/2013/06/17/the-web-cookie-is-dying-heres-the-creepier-technology-that-comes-next/. As Tanner's article explains, in an effort to circumvent software blocking tracking cookies, internet advertisers have developed a practice known as "fingerprinting" which "allows a web site to look at the characteristics of a computer such as what plugins and software you have installed, the size of the screen, the time zone, fonts and other features of any particular machine . . . [which collectively] form a unique signature just like random skin patterns on a finger." *Id.*; *see also* Olga Kharif, *The Cookies You Can't Crumble*, BUSINESSWEEK (Aug. 21, 2014), http://www.businessweek.com/articles/2014-08-21/facebook-google-go-beyond-cookies-to-reap-data-

Notwithstanding the primary goal of targeted advertising, companies have also been criticized for their data collection activities and for how they utilize this data in other contexts. For instance, in 2012, Target was lambasted in the media over reports that its internal data analytics resulted in sending a teen girl coupons for baby-related items before the girl had disclosed that she was pregnant.[247] Facebook Data Science, a research service that analyzes data trends of Facebook users, released the results of its study showing that it was able to estimate with fairly good accuracy based on user's activity on the social networking site when a relationship begins and ends.[248] The company has also been criticized for its "Facedeals" camera, which uses facial recognition technology to identify people to provide offers and special deals.[249] Similarly, Google has built a function into Google Maps that offers users specials and discounts at points of interest that are explored in the map.[250]

The mining of data is not limited to web traffic but also extends to email. For instance, in addition to keeping track of people's search histories,[251] Google also indexes both the text of emails and the contents of all attachments.[252] Although doing so may have beneficial and helpful aspects, including the ability to inform users when they

for-advertisers. For a summary of all the ways that Facebook tracks its users across the internet, see Byron Acohido, *Facebook Tracking Is Under Scrutiny*, USA TODAY (Nov. 16, 2011, 9:03 AM), http://usatoday30.usatoday.com/tech/news/story/2011-11-15/facebook-privacy-tracking-data/51225112/1.

247. Charles Duhigg, *How Companies Learn Your Secrets*, NY TIMES MAGAZINE (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html; Kashmir Hill, *How Target Figured Out a Teen Girl Was Pregnant Before Her Father Did*, FORBES (Feb. 16 2012, 11:02 AM), http://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/.

248. Kate Rogers, *Facebook Knows When You're off the Market Before You Do*, FOX BUSINESS (Feb. 18, 2014), http://www.foxbusiness.com/personal-finance/2014/02/18/facebook-knows-when-youre-off-market-before-do/ [hereinafter Rogers, *Facebook Knows*].

249. Mark Prigg, *The Facebook Camera That Can Recognize You Every Time You Walk into a Shop*, DAILY MAIL (Apr. 29, 2015), http://www.dailymail.co.uk/sciencetech/article-2187801/were-watching-The-camera-recognise-Facebook-picture-time-walk-shop.html.

250. *Google Maps Update Offers Indoor Walking Directions*, FOX NEWS (May 11, 2012), http://www.foxnews.com/tech/2012/05/11/google-maps-update-offers-indoor-walking-directions/.

251. *See, e.g.*, Zack Christenson, *Google's Data-Collecting Habits Draw More Scrutiny*, THE HILL (Oct. 29, 2012, 6:00 PM), http://www.thehill.com/blogs/congress-blog/technology/264685-googles-data-collecting-habits-drawing-more-scrutiny.

252. *See e.g.*, *Google Accused of Spying on Gmail Users,* RT (Oct. 12, 2012, 3:46 PM), http://rt.com/usa/news/google-gmail-users-plaintiffs-289/. In fact, recent pressure from student groups and privacy advocates resulted in Google agreeing to not data mine email accounts under its Google Apps for Education services. *See e.g.*, Alastair Barr, *Google Stops Scanning Student Gmail Accounts for Ads*, WALL ST. J. (Apr. 30, 2014), http://blogs.wsj.com/digits/2014/04/30/google-stops-scanning-student-gmail-accounts-for-ads/; Laura Northup, *Google Will Strop Data-Mining Student E-Mail Accounts*, CONSUMERIST (Apr. 30, 2014), http://consumerist.com/2014/04/30/google-will-stop-data-mining-student-e-mail-accounts/.

have bills to pay, many are concerned about the privacy interests implicated by the company actively keeping tabs on users' financial details.[253] While the outward impression is that Google is primarily a search engine or email provider, the core of the company's business is advertising and marketing.[254] Allowing the company to search and index one's private emails thus becomes the true cost of the free email that Gmail users enjoy.[255]

Apprehension surrounding the collection of personal data has not been limited to online activities; it also increasingly extends to smartphones capable of storing and providing large amounts of personal information and user activities[256] and the increased prevalence of global positioning devices and activity trackers.[257] Activity trackers such as those sold by FitBit, Garmin, Adidas, and Jawbone, among others, commonly provide users with pertinent information about their daily activities such as the number of steps that they have taken throughout the day, distance traveled, and calories burned.[258] More

253. Alistair Barr, *Google Can Read Your Emailed Bills and Remind You to Pay Up*, WALL ST. J. (Oct. 7, 2014), http://blogs.wsj.com/digits/2014/10/07/google-can-read-your-emailed-bills-and-remind-you-to-pay-up/.

254. *See, e.g.*, *Google Inc. Announces Fourth Quarter and Fiscal Year 2014 Results*, GOOGLE (Jan. 29, 2015), http://investor.google.com/earnings/2014/Q4_google_earnings.html (reporting that the company's websites generated nearly $12.43 billion dollars or 69% of the revenues for the Fourth Quarter of 2014).

255. This model (giving up privacy in exchange for a service) has been utilized by a number of different software applications. *See, e.g.*, Kim Komando, *Free Apps Collect Your Personal Data*, FOX NEWS (Nov. 8, 2014), http://www.foxnews.com/tech/2014/11/08/free-apps-collect-your-personal-data/ (finding that research at Carnegie Mellon University uncovered that many apps often seek access to user's personal information on their phones, even if such information is unrelated to the functionality of the app); Rogers, *Facebook Knows*, *supra* note 248 (noting the comments of social media reporter Jon Constantine who notes that "People talk a lot about [how] they care about privacy, but we ultimately won't give up services over it").

256. David Goldman, *Carrier IQ: Your Phone's Secret Recording Device*, CNN MONEY (Dec. 1, 2011, 6:28 PM), http://money.cnn.com/2011/12/01/technology/carrier_iq/index.htm; Gerry Smith, *Carrier IQ: Researcher Trevor Eckhart Outs Creepy, Hidden App Installed On Smartphones*, HUFFINGTON POST (Nov. 30, 2011, 12:11 PM), http://www.huffingtonpost.com/2011/11/30/carrier-iq-trevor-eckhart_n_1120727.html; John R. Quain, *Carrier IQ Not Alone: Most Smartphones Will Track You*, FOX NEWS (Dec. 7, 2011), http://www.foxnews.com/scitech/2011/12/06/in-tracking-companies-reveal-their-low-iq/; Shaun Waterman, *New Software Uses Smartphone Camera for Spying*, WASH. TIMES (Oct. 2, 2012), http://www.washingtontimes.com/news/2012/oct/2/new-software-uses-smartphone-camera-spying/ (describing software that can hijack users cell phones to combine images and GPS to create 3D maps of indoor spaces).

257. Mark Saltzman, *GPS Navigation Units More Popular as Prices Fall*, USA TODAY (May 13, 2009), http://usatoday30.usatoday.com/tech/products/services/2009-05-12-popular-gps-navigation-units_N.htm (noting that nearly 17 million GPS unites were sold in 2009); Don Reisinger, *After 23 Years Garmin Reaches 100 Million Devices Sold*, CNET (May 2, 2012), http://www.cnet.com/news/after-23-years-garmin-reaches-100-million-devices-sold/ (noting robust sales by GPS manufacturer Garmin, including 75 million units sold between 2007–2012).

258. Matthew Miller, *Data Accessibility is Key to Successful Activity Tracking System*, ZDNET (Nov. 8, 2014), http://www.zdnet.com/article/data-accessibility-is-key-to-a-successful-activity-tracking-system/; Christian Payne, *How Activity Trackers Re-*

advanced models offer users the ability to track their heart rate, their sleep patterns, and even the user's location.[259] While these activity trackers were intended to help users track and reach their fitness goals, the data captured is also of significant interest to the companies manufacturing the devices,[260] as well as third-parties offering related services or data analysis.[261] A number of insurance companies, for example, have offered members discounts on their health insurance premiums if data provided by activity trackers reflect the user having reached certain activity milestones.[262]

Notwithstanding the potential that personal health information could be used, parsed out, and sold, the market for those activity trackers has exploded over the last few years.[263] New models with varying price points and features have been introduced frequently,

---

move Our Rights to Our Most Intimate Data, THE GUARDIAN (June 3, 2014), http://www.theguardian.com/technology/2014/jun/03/how-activity-trackers-remove-rights-personal-data; Carol Mangis, *Are Activity Trackers a Privacy Nightmare?*, CONSUMER REPORTS (Aug. 13, 2014), http://www.consumerreports.org/cro/news/2014/08/are-activity-trackers-a-privacy-nightmare/index.html.

259. *See generally id. See also* Kelly Santos, *Can Fitness Trackers Threaten Your Privacy?,* CREDIT (Aug. 19, 2014), http://blog.credit.com/2014/08/can-exercise-apps-threaten-your-privay-93316/.

260. *See, e.g.*, Leo Hickman, *G2: Dear Digital Diary. . .: From Sleeping and Eating to Exercise and Travel, Technology Now Allows Us to Track and Analyse Every Detail of our Lives. But, asks Leo Hickman, How Can it Help Us Actually Improve Them?*, THE GUARDIAN (LONDON), Aug, 13, 2012, at 10 (noting concerns that "the default setting is that this data is shared. This is wrong. Users are asked to sync with Facebook. People who use these apps are thinking about their health, not about data privacy. But all this data is very valuable. More often than not, you don't even get to own the data you are generating. Most of it is stored on client-side data servers. This is turning into a huge business. Companies are circling at the moment."); *see also* Bryan Walsh, *Data Mine: The Next Revolution in Personal Health May Be the Little Step-Tracking Band on Your Wrist*, TIME, Nov. 24, 2014, at 35 (relaying the comments of Andrew Rosenthal, the group manager for wellness and platform at Jawbone (a manufacturer of activity trackers) who noted that parsing out the data gathered by such devices could allow for companies to "help steer people toward the health solutions that work best for them") [hereinafter Walsh, *Data Mine*].

261. For instance, some personal trainers are able to monitor the activities of its clients based on the data generated by the trackers, in part, to be able to offer additional guidance and services. Courtney Rubin, *Your Trainer Saw That*, NY TIMES, Apr. 17, 2014, at E7.

262. *See, e.g.*, Walsh, *Data Mine*, *supra* note 260, at 35 (noting how employees of the Cleveland Clinic are eligible for lowered health insurance premiums in exchange for using an activity tracker); Kate Knibbs, *An Insurance Company Will Pay You to Use Your Fitness Tracker*, GIZMODO (Dec. 9, 2014), http://gizmodo.com/an-insurance-company-will-pay-you-to-use-your-fitness-t-1668967153 (describing the program offered by NY based insurance company Oscar); *see also* Issie Lapowsky, *This Insurance Company Pays People to Stay Fit*, WIRED (Dec. 8, 2014), http://www.wired.com/2014/12/oscar-misfit/ (noting that the co-founder of Oscar has admitted that one of the driving forces behind providing fitness trackers to its members "is to collect more health data on its members to make sure doctors have the most information available on them").

263. *See* Walsh, *Data Mine*, *supra* note 260, at 35 (relaying the estimates of research showing that 42 million wearable activity trackers were shipped in 2014, compared with 32 million the prior year, an increase of over 31%).

with people seemingly weighing in favor of the functionality provided by such devices as a seemingly acceptable tradeoff for the potential intrusion on their privacy.[264]

B. *Known Vulnerabilities of Electronic Communications and Stored Data*

In part because of how valuable information has become, its security is constantly under threat.[265] Companies and governments have invested untold millions of dollars to upgrade their computer networks and data security protocols, both to thwart attacks by computer hackers and to assure their users that they can be trusted to hold users' personal information. No matter how much money has been invested in this area, however, nothing is truly foolproof.[266] Unfortunately, almost every segment of the population has been or could be affected by data breaches,[267] which has led to quantifiable losses (e.g.,

264. Brier Dudley, *Fitness Gadgets Raise Privacy Concerns Under New Health Insurance Rules*, SEATTLE TIMES (Feb. 9, 2014), http://seattletimes.com/html/businesstechnology/2022868569_briercolumn10xml.html; Walsh, *Data Mine*, *supra* note 260 (noting that internet security company Symantec reported that such activity trackers were vulnerable to potential data breaches).

265. David Barton, *When Will Your Data Breach Happen? Not a Question of If But When*, SECURITY INFO WATCH (Mar. 10, 2015), http://www.securityinfowatch.com/article/12052877/preparing-for-your-companys-inevitable-data-breach; Ingrid Lunden, *Business Services, Retail Saw the Most Online Security Breaches in 2014: FireEye*, TECH CRUNCH (Feb. 24, 2015), http://techcrunch.com/2015/02/24/fireeye-security-breaches-2014/; Laura Rosbrow, *Israeli Startup enSilo Raises Est, $2–3 Million Seed Round to Prevent Attacks*, GEEKTIME (Mar. 10, 2015), http://www.geektime.com/2015/03/10/israeli-cyber-startup-ensilo-raises-est-2-3-million-seed-round-to-prevent-attacks.

266. Nicole Perlroth & David Gelles, *Russian Hackers Amass Over a Billion Internet Passwords*, NY TIMES (Aug. 5, 2014), http://www.nytimes.com/2014/08/06/technology/russian-gang-said-to-amass-more-than-a-billion-stolen-internet-credentials.html (noting the view of "some in the security community that keeping personal information out of the hands of thieves is increasingly a losing battle").

267. *See, e.g.*, John Roberts, *Exclusive: Drones vulnerable to Terrorist Hijacking, Researchers Say*, FOX NEWS (June 25, 2012), http://www.foxnews.com/tech/2012/06/25/drones-vulnerable-to-terrorist-hijacking-researchers-say/ (relaying that GPS receiver in drones could be surreptitiously taken over by hackers); John D. Sutter, *Facebook pulls location tracking feature*, CNN (June 26, 2012), http://www.cnn.com/2012/06/26/tech/social-media/facebook-pulls-find-friends-nearby/index.html (noting that after user complaints, Facebook retracted a feature that would allow users to see the location of nearby friends); *Facebook Flaw Means Anyone Can See Private Photos*, FOX NEWS (Dec. 6, 2011), http://www.foxnews.com/tech/2011/12/06/facebook-flaw-means-anyone-can-see-your-photos/ (noting that a flaw in the website would allow even photographs marked as private by individuals to be viewed publicly; since the news report, Facebook has addressed and closed the flaw); Eric Yoder, *TSP Discloses Hacking of Accounts*, WASH. POST (May 25, 2012), http://www.washingtonpost.com/blogs/federal-eye/post/tsp-discloses-hacking-of-accounts/2012/05/25/gJQAsM4kpU_blog.html (disclosing that the federal Thrift Savings Plan was the target of a "sophisticated cyber attack", whereby social security numbers from the affected accounts were taken); David Goldman, *More Than 6 Million LinkedIn Passwords Stolen*, CNN MONEY, (June 7, 2012), http://money.cnn.com/2012/06/06/technology/linkedin-password-hack/index.htm (reporting on the breach of passwords to user LinkedIn accounts); James Rogers, *Expert: Dropbox Leak Highlights Password Security Dangers*,

financial, identity theft, stolen passwords, and credit card numbers), as well as unquantifiable ones (e.g., invasion of privacy and embarrassment over the information made public).

For instance, recent reports by the *New York Times* noted that a Russian crime ring had collected nearly 1.2 *billion* usernames and passwords to various websites, as well as 500 million email addresses.[268] Computer security experts noted that this information has been used by the thieves for advertisement purposes but that its real value is its potential to be used for identity theft.[269] Less than a month later, it was reported that hackers breached JPMorgan Chase & Co., taking gigabytes of sensitive financial information.[270] News reports relaying instances of online data breaches have seemingly become *de rigueur*, as companies of all sizes and industries have become the victim of online thieves for financial information.[271] One cyber

---

FOX NEWS (Oct. 14, 2014), http://www.foxnews.com/tech/2014/10/14/expert-dropbox-leak-highlights-password-security-perils/ (noting that login credentials for hundreds of users of cloud storage service Dropbox were compromised); Charles Arthur, *Cyber-Attack Concerns Raised Over Boeing 787 Chip's 'Back Door'*, THE GUARDIAN (May 29, 2012), http://www.theguardian.com/technology/2012/may/29/cyber-attack-concerns-boeing-chip (discussing how two researchers believe that the computer chip in the Boeing 787 and other military aircraft could be taken over through the internet, via a back door flaw in the design of the chip); *State Department Shuts Down Email System After Suspected Hacker Attack*, FOX NEWS (Nov. 16, 2014), http://www.foxnews.com/politics/2014/11/16/state-department-shuts-down-email-system-after-suspected-hacker-attack/ (reporting that the U.S. State Department shut down its entire unclassified email system after security experts detected a suspected data breach); Ed Pilkington, *Playstation and Xbox Facing Issues After Christmas Day Attack*, THE GUARDIAN (Dec. 25, 2014), http://www.theguardian.com/technology/2014/dec/25/playstation-xbox-down-lizard-squad-hack-christmas (describing a denial of service attack on the Playstation and Xbox online gaming communities which resulted in both services being taken offline).

268. *See* Perlroth & Gelles, *supra* note 266.

269. *Id.* As Perlroth and Gelles relay, because many people use similar login credentials on various websites, the information collected by the Russian crime ring may potentially be used to try to access any number of financial institutions. *Id.*

270. Michael Riley & Jordan Robertson, *FBI Said to Examine Whether Russia Tied to JPMorgan Hacking*, BLOOMBERG (Aug. 27, 2014), http://www.bloomberg.com/news/articles/2014-08-27/fbi-said-to-be-probing-whether-russia-tied-to-jpmorgan-hacking.

271. *See, e.g.*, Rachel Abrams, *Target Puts Data Breach Costs at $148 Million, and Forecasts Profit Drop*, NY TIMES (Aug. 5, 2014), http://www.nytimes.com/2014/08/06/business/target-puts-data-breach-costs-at-148-million.html (noting that personal data and credit card information was stolen for nearly 12 million of Target store's guests); Amitra Jayakumar, *Michaels Says 3 Million Customers Hit by Data Breach*, WASH. POST (Apr. 4, 2014), http://www.washingtonpost.com/business/economy/michaels-says-nearly-3-million-customers-hit-by-data-breach/2014/04/18/3074e432-c6fc-11e3-8b9a-8e0977a24aeb_story.html (noting that nearly 3 million customers of craft stores, Michaels and Aaron Brothers, had their credit or debit card accounts taken); Michael Calia, *P.F. Chang's Says Data Breach Affected 33 Locations*, WALL ST. J. (Aug. 4, 2014) http://www.wsj.com/articles/p-f-changs-says-data-breach-affected-33-locations-1407159131 (noting that for a nearly eight month period, customers at 33 of the restaurant chain's locations may have had credit card numbers, names and expiration dates stolen); Maggie McGrath, *Home Depot Confirms Data Breach, Investigating*

security expert has noted that such occurrences will likely remain commonplace in the foreseeable future.[272]

Even when financial information is not directly taken by thieves and hackers, the damage to victims can be substantial. In November 2014, Sony Entertainment suffered a massive data breach.[273] Included in the trove of information taken were employees' social security numbers, medical records, confidential internal communications, and even five previously unreleased movies. The leaked information included embarrassing comments made by the company's leadership about other Hollywood individuals, harming the company's reputation.[274] The leak also resulted in the early release of the movie *The Interview* to online streaming services that do not provide for the same level of revenue generation as traditional movie theaters.[275]

Transactions From April Onward, FORBES (Sept. 8, 2014), http://www.forbes.com/sites/maggiemcgrath/2014/09/08/home-depot-confirms-data-breach-investigating-transactions-from-april-onward/; *Jimmy John's Reveals Breach of Credit, Debit Data*, CHI. TRIB. (Sept. 24, 2014), http://www.chicagotribune.com/business/breaking/chi-jimmy-johns-data-breach-20140924-story.html.

272. Jay Johnson, *If 2014 Was The Year Of the Data Breach, Brace For More*, FORBES (Jan. 2, 2015), http://www.forbes.com/sites/danielfisher/2015/01/02/if-2014-was-the-year-of-the-data-breach-brace-for-more/.

273. *See generally* Gregg Kilday & Tatiana Siegel, *Sony Hack: Studio Security Points to Inside Job*, HOLLYWOOD REPORTER (Dec. 3, 2014), http://www.hollywoodreporter.com/news/sony-hack-studio-security-points-753509; Shannon Pettypiece, *Sony Hack Reveals Health Details on Employees, Children*, BLOOMBERG (Dec. 11, 2014), http://www.bloomberg.com/news/2014-12-11/sony-hack-reveals-health-details-on-employees- and-their-children.html; Andrew Wallenstein, *Sony's New Movies Leak Online Following Hack Attack*, VARIETY (Nov. 29, 2014), http://variety.com/2014/digital/news/new-sony-films-pirated-in-wake-of-hack-attack-1201367036/; Ben Fritz & Danny Yadron, *Sony Hack Exposed Personal Data of Hollywood Stars*, WALL ST. J. (Dec. 5, 2014), http://www.wsj.com/articles/sony-pictures-hack-reveals-more-data-than-previously-believed-1417734425; Sam Frizell, *Report: Sony's Security Team Was Unprepared for Hack*, TIME (Dec. 5, 2014), http://time.com/3620288/sony-hack-unprepared/.

274. Todd Cunningham & Sharon Waxman, *Sony Struggles to Fight #GOP Hackers Who Claim Stolen Data Includes Stars' IDs, Budget and Contract Figures*, THE WRAP (Nov. 28, 2014), http://www.thewrap.com/sony-execs-working-on-chalkboards-while-hackers-claim-stolen-data-includes-stars-ids-budget-and-contract-figures/; Philip Caulfield & Corky Siemaszko, *Sony Email Hack Shows Scott Rudin, Amy Pascal Making Racist Jokes about Obama; Producer Apologies*, NY DAILY NEWS (Dec. 11, 2014), http://www.nydailynews.com/entertainment/gossip/rudin-pascal-made-racist-jokes-obama-sony-hacks-article-1.2041618; Charlie Campbell, *Sony Pictures Chief Amy Pascal Joked About Obama's Race*, TIME (Dec. 11, 2014), http://time.com/3629480/sony-pictures-hack-amy-pascal-emails/; Terence McCoy, *Sony's Amy Pascal's future in Hollywood in Doubt Following Disastrous E-mail Hack*, WASH. POST (Dec. 12, 2014), http://www.washingtonpost.com/news/morning-mix/wp/2014/12/12/sonys-amy-pascals-future-in-hollywood-in-doubt-following-disastrous-e-mail-hack/.

275. David Carr, *How the Hacking at Sony Over 'The Interview' Became a Horror Movie*, NY TIMES (Dec. 21, 2014), http://www.nytimes.com/2014/12/22/business/media/hacking-at-sony-over-the-interview-reveals-hollywoods-failings-too.html; Bernard Condon, *Sony Hacking Fallout Explodes As Theaters Cancel 'The Interview' Showings*, HUFFINGTON POST (Dec. 17, 2014), http://www.huffingtonpost.com/2014/12/17/sony-hack-theaters_n_6338246.html; Melissa Locker, *Did North Korea Hack Sony Pictures Over The Interview?*, VANITY FAIR (Nov. 29, 2014), http://www.vanityfair

Embarrassment and invasion of individual privacy were also at the center of two similar data breaches involving the public dissemination of intimate user photographs by hackers. In October 2014, hackers were able to access Apple's iCloud data backup systems containing photographs taken by owners of iPhones.[276] Many of the images taken were private, intimate photographs of celebrities, which were subsequently cataloged and released on public online message boards.[277] Similarly, hackers breached security for the app Snapchat despite the company's claims that the disappearing nature of the communications passed through the site was a main security feature.[278] Private and intimate images that users mistakenly believed would be deleted from existence seconds after they had been viewed were found posted online.[279] Hackers were able to exploit a security flaw in

.com/hollywood/2014/11/north-korea-james-franco-seth-rogen. It has been alleged that the data breach was the result of North Korean computer hackers, who had sought to retaliate against Sony for producing the film. *See generally id.* The movie centers around a fictional plot to assassinate the leader of North Korea, Kim Jong Un. *Id.*

276. Mark Rogowsky, *Yes, Celebs Had Their iCloud Accounts Hacked. No, You Shouldn't Shut Yours Off*, FORBES (Sept. 3, 2104), http://www.forbes.com/sites/markrogowsky/2014/09/03/the-celeb-hack-has-people-telling-you-to-turn-off-cloud-backup-ignore-them/; Alan Duke, *5 Things to Know About the Celebrity Nude Photo Hacking Scandal*, CNN (Oct. 12, 2014), http://www.cnn.com/2014/09/02/showbiz/hacked-nude-photos-five-things/; Brian X. Chen, *Apple Says It Will Add New iCloud Security Measures After Celebrity Hack*, NY TIMES (Sept. 4, 2014), http://bits.blogs.nytimes.com/2014/09/04/apple-says-it-will-add-new-security-measures-after-celebrity-hack/; Mike Isaac, *Nude Photos of Jennifer Lawrence Are Latest Front in Online Privacy Debate*, NY TIMES (Sept. 2, 2014), http://www.nytimes.com/2014/09/03/technology/trove-of-nude-photos-sparks-debate-over-online-behavior.html.

277. Stuart Oldham, *Jennifer Lawrence, Kate Upton, Ariana Grande Among Celebrities Exposed in Massive Nude Photo Leak*, VARIETY (Aug. 31, 2014), http://variety.com/2014/biz/news/jennifer-lawrence-kate-upton-ariana-grande-exposed-in-massive-nude-photo-leak-1201295180/.

278. *See, e.g.*, Alyssa Newcomb, *Snapchat Settles with FTC Over Claims It Deceived Users About Disappearing Messages*, ABC NEWS (May 8, 2014), http://abcnews.go.com/Technology/snapchat-settles-federal-trade-commission-claims-deceived-users/story?id=23642852 (May 8, 2014); Christina Warren, *Ghost in the Shell, The Snapchat Privacy Illusion*, MASHABLE (Oct. 13, 2014), http://mashable.com/2014/10/13/snapchat-inherently-insecure/ (noting the "inherent security flow within Snapchat's product. . . [is] the promise of disappearing images is really just an illusion"). Snapchat was recently the target of a Federal Trade Commission investigation over deceptive claims that the touted ethereal nature of messages passed through the service was not accurate. *Snapchat 'Deceived Users' About Disappearing Messages, Will be Monitored by Gov't*, RT (May 9, 2014), http://rt.com/usa/157960-snapchat-deceived-users/. Ultimately Snapchat settled with the government over the false promises that messages would disappear, as well as over misleading statements made about the amount of personal data it collected and security features. *See Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False*, FEDERAL TRADE COMMISSION (May 8, 2014), https://www.ftc.gov/news-events/press-releases/2014/05/snapchat-settles-ftc-charges-promises-disappearing-messages-were.

279. Brian Fung, *A Snapchat Security Breach Affects 4.6 Million Users. Did Snapchat Drag Its Feet on a Fix?*, WASH. POST (Jan. 1, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/01/01/a-snapchat-security-breach-affects-4-6-million-users-did-snapchat-drag-its-feet-on-a-fix/; James Rogers, *Leaked Snapchat*

a third-party application that worked with the Snapchat service and were able to copy and publicly leak Snapchat users' images, despite bypassing the Snapchat's own servers.[280]

With potentially billions of dollars, credit card numbers, and passwords and innumerable emails, documents, and pictures at stake, the solution remains unclear. Technical means such as firewalls, encryption, and access protocols are only as effective as the expertise of the programmer and engineer. As the data breaches of 2014 illustrate, loopholes and flaws can render even the most robust security methods ineffective in the hands of motivated and skilled hackers.[281]

Websites have attempted to add a user element to enhance security and ensure that only the account holder can access particular resources. This has often involved including asking extra questions of a personal nature, in addition to the usual username and password. For example, some websites require users to provide answers to personal questions when creating accounts (mother's maiden name, first school, name of first pet, model of first car, name of the street you grew up on, etc.), which are referenced when users are unable to remember their login information or sometimes to confirm a user's identity when logging into the site.[282]

In a vacuum and as isolated measures, these security features can be very effective, but in the aggregate, they mean that users are forced to reveal yet more personal information about themselves. Further, websites' protocols that disallow repetition of old passwords indicates

---

Images Should Serve as a Wake-Up Call to Users, Expert Says, FOX NEWS (Oct. 13, 2014), http://www.foxnews.com/tech/2014/10/13/expert-leaked-snapchat-images-should-serve-as-wake-up-call-to-users (noting that nearly 200,000 images, including possibly child pornography, were released as a result of the Snapchat breach); *Snapchat Blames Other Apps for Breach,* TIME (Oct. 10, 2014), http://fortune.com/2014/10/10/snapchat-blames-other-apps-for-breach/.

280. *See generally* Alyssa Newcomb, *How Hackers Got Private Photos Without Ever Breaching Snapchat's Servers*, ABC NEWS (Oct. 13, 2014), http://abcnews.go.com/Technology/hackers-private-photos-breaching-snapchats-servers/story?id=26156997.

281. Rogowsky, *supra* note 276. As Rogowsky explains, the cause of the breach to the Apple iCloud service in the celebrity nude photo scandal was due to a flaw that "Apple left a big hole in iCloud that allowed hackers to try an unlimited number of guesses at passwords without being locked out (since fixed)." *Id.*

282. *See, e.g.*, Melinda Beck, *Health Website Security Questions Leave Some Flummoxed*, WALL ST. J. (Oct. 22, 2013), http://www.wsj.com/articles/SB10001424052702304384104579145933319187114; Kristen J. Mathews, *Security Questions: What is Your Pet's Name?*, PROSKAUER ROSE, http://www.proskauer.com/files/Media/dccb2c51-ffa7-4a26-b99d-0773fa10c782/Presentation/TranscriptFile/Security%20Questions_What%20is%20your%20pets%20name.pdf (last visited Mar. 13, 2015); Joe Kissell, *When password security questions aren't secure*, MACWORLD (Nov. 29, 2012), http://www.macworld.com/article/2016925/when-password-security-questions-arent-secure.html; SURVEILLANCE SELF-DEFENSE: CREATING STRONG PASSWORDS, ELECTRONIC FRONTIER FOUNDATION (2015), *available at* https://ssd.eff.org/en/module/creating-strong-passwords; Jessica Griggs, *'Secret' Questions Leave Accounts Vulnerable*, NEW SCIENTIST (June 22, 2009), http://www.newscientist.com/article/dn17347-secret-questions-leave-accounts-vulnerable.html.

that the sites are storing those old passwords. Even if the system administrators can be assumed to be trustworthy in all instances, these practices incentivize hacking of seemingly innocuous systems likely to be soft targets[283] not for the substantive information, but for the answers to the questions and password patterns remembered by the systems. As the Russian hacking incident illustrates, sometimes information and systems can be accessed and gleaned through brute force and repeated attempts with compromised information from another website. The end result is a cascading effect whereby the information acquired from a website storing significant personal information about a user might then be used to access subsequent websites using the same or similar information. In this way, users (and, ironically, their compliance with security policies) enable and facilitate the equivalent of electronic dumpster diving.[284]

C. *Behavioral Factors*

Despite the knowledge that more and more private and personal information is being collected by companies and that these companies are often helpless against rising threats to data security, people are increasingly entrusting their information to these outside entities.

As noted by social media reporter Jon Constantine, at the core of this quandary is that "[p]eople talk a lot about [that] they care about privacy, but we ultimately won't give up services over it."[285] Despite great interest and significant debate about the right balance, it is apparent that for users, convenience and services have won out. The dangers and warnings offered by experts in data security have not dissuaded the general public from putting their private information at risk. This behavior is relevant here for two reasons: (1) the lip service paid to the importance of privacy when convenience is a demonstrably more influential factor; and (2) the unprompted sharing of information, most commonly via social media networks, that has led to a blur-

283. The network effect that allows soft targets to be gateways to harder ones is also why, for example, Transportation Security Administration (TSA) screening standards are the same for small rural airports as they are for large urban ones that might be more attractive to potential attackers. The weakest spots of any network are the ones most likely to be exploited.

284. For a fantastic discussion of the vulnerability paradox of redundant security measures, see Scott D. Sagan, *The Problem of Redundancy Problem: Why More Nuclear Security Forces May Lead to Less Nuclear Security*, 24 RISK ANALYSIS 934 (2004), *available at* http://iis-db.stanford.edu/pubs/20274/redundancy_risk_analysis.pdf (discussing examples where additional redundant systems meant as failsafes can increase the possible points of failure).

285. Rogers, *Facebook Knows*, *supra* note 248. *But c.f.* Steve Lohr, *The Privacy Paradox, a Challenge for Business*, N.Y. TIMES (June 12, 2012), http://bits.blogs.nytimes.com/2014/06/12/the-privacy-paradox-a-challenge-for-business/ (discussing how a recent study indicated that "People around the world are thrilled by the ease and convenience of their smartphones and Internet services, but they aren't willing to trade their privacy to get more of it").

ring of the previously established lines between public and private spheres.

With respect to the first, individuals' desires to access services, conveniences, and benefits often outweighs any corresponding privacy concerns, as demonstrated by consumer trends. As discussed previously, users willingly use email services, smartphone apps, activity trackers, and GPS devices even though each service—and even more so collectively—collects information about the user that he may not otherwise feel comfortable disclosing publicly. The use of these services, therefore, provide the implied and tacit consent for companies to passively track these individuals.[286] Users enjoy the benefits of having connected smart devices, which use the Internet to remotely operate light bulbs, appliances, and home security systems, even though doing so results in making vulnerable the user's entire home network.[287] The ability to map a workout and jog has taken a priority over concerns that one's route can also be viewed in real time to track the user's location with precision.[288] Users do all this while being on notice that online communications and transactions are remarkably vulnerable.

Secondly, the decline of privacy can also be illustrated by the rise of popularity in social media networks and similar applications. Websites and apps such as Facebook, Twitter, Instagram, and Snapchat allow users to post unprompted and private information about their thoughts, activities, and whereabouts. Behaviors such as sexting and bragging about criminal activity have become common fodder on social media, notwithstanding the ease at which salacious material can "go viral." As one researcher has argued, the motivations behind such postings may stem from narcissistic impulses and users' desires to emphasize qualities they believe are important to their public persona.[289] Alternatively, their activities illustrate a perhaps mistaken trust in the

286. Consider also something as seemingly innocuous as a grocery store loyalty card. While grocery stores often tout the card as a means for shoppers to access sale prices and specials, the card also links shoppers' purchases to a database that compiles buying histories and other trends. This information can then be sold to marketers, or used internally for targeted advertisement, as was the case of Target's algorithm correlating purchase patterns with likely pregnancy. *See* text accompanying note 247, *supra*.

287. *See* Kim Zetter, *How Thieves Can Hack and Disable Your Home Alarm System*, WIRED (July 23, 2014), http://www.wired.com/2014/07/hacking-home-alarms/; Kashmir Hill, *How Your Security System Could Be Hacked To Spy On You*, FORBES (July 23, 2014), http://www.forbes.com/sites/kashmirhill/2014/07/23/how-your-security-system-could-be-used-to-spy-on-you/.

288. Applications include Greenalp's "Real-Time GPS Tracker" (https://www.greenalp.com/RealTimeTracker/), Map My Tracks (http://www.mapmytracks.com/sports/running), and Revel Mob's "Where M I" (http://www.revelmob.com/blog/real-time-tracking-iphone-app-perfect-marathoners).

289. *See* Sanja Kapidzic, *Narcissism as a Predictor of Motivations Behind Facebook Profile Picture Selection,* J. CYBERPSYCHOLOGY, BEHAV., & SOC. NETWORKING (2012), http://www.ncbi.nlm.nih.gov/pubmed/23249240.

providers of these services that their data and information can be restricted according to each user's preferences.

This is the irony of the "information age." Information is more valuable than ever, and yet, on a personal level, we seem to give it up more freely than ever. A corollary to the open, sharing society is the effect that such behavior has on societal notions of privacy. As this forms a key determinate as to the reasonable expectations of privacy under Supreme Court jurisprudence, society must examine whether current trends in this area are the right path forward as the law catches up to what people are actually doing.

V. AMENDMENTS TO REASONABLENESS AND FUTURE PROTECTIONS OF PRIVACY

This final Part of the Article will juxtapose Part IV's exploration of private and commercial capabilities and behaviors with a sampling of media reports concerning supposed law enforcement and intelligence practices at the federal, state, and local levels.[290] As explained further below, any potential parity between non-government technologies and practices with government counterparts does not end, but can inform the inquiry into what properly can be considered citizens' reasonable expectations of privacy for Fourth Amendment purposes.

As discussed in Part III, the October 2001 passage of the Patriot Act ushered in an era of increasingly intertwined U.S. national security and criminal law enforcement practices, particularly with respect to counterterrorism efforts. This began a somewhat paradoxical period for law, policy, and public discourse—on the one hand, increased focus on security (both domestic and abroad) became extremely high-profile and sparked renewed public focus and debate on the scope of governmental efforts to prevent attacks. This included fundamentally altering the FBI from an agency focused on the *post-hoc* investigations of crimes into one driven to prevent any further attacks.[291] Indeed, the debates as early as Fall 2001 over the Patriot Act's "library records" provision highlight the vigor with which the scope of

290. Now that the reader has further context as to the scope and framework of this Article, it bears repeating (as noted in the initial disclaimer at the beginning of this Article) that the news media reports, opinions, and other similar content cited herein that purport to discuss federal, state, and local law enforcement and intelligence practices, tactics, and technologies are not necessarily cited for the truth of the matters they assert. The Authors' reliance upon such sources here is to recognize the reporting itself, and the public discussion about the reports; the selection of the articles cited is meant to sample and be representative of public suppositions about technological capabilities and their use, and should not be read to confirm the existence of any particular program, technology, or practice, nor attest to the accuracy of how any such program, technology, or practice's deployment or use is described.

291. *See* JOHN ASHCROFT, NEVER AGAIN: SECURING AMERICA AND RESTORING JUSTICE 133 (2006); Robert S. Mueller III, American Bar Association Standing Committee on Law and National Security breakfast program ("The FBI: Safeguarding National Security") keynote address, Feb. 24, 2015.

counterterrorism programs were examined, more than a decade before anybody had ever heard of Edward Snowden. Not long after the September 11 attacks, rumors about rendition programs, kinetic targeting programs, and eventually cyber capabilities all became the subjects of front-page news reports, lawsuits, and campaign stump speeches.[292]

With much of the intelligence/criminal wall dismantled in law, policy, and public conscience, and with the consequential knowledge that law enforcement and intelligence functions can interact in meaningful ways in an era of ever-more-capable and prolific technological tools, the *Kyllo* test would imply it is reasonable to suspect that certain high-tech measures might be used in the law enforcement context, notwithstanding their development for intelligence purposes. Further, if capabilities or activities that are supposed to be secret are readily discussed out in the open, it is possible that, too, has Fourth Amendment implications. The American Civil Liberties Union ("ACLU") has adopted a corollary argument in FOIA litigation over the secrecy of alleged, publicly-referred-to targeting programs.[293] Further, *Kyllo*'s sliding scale for reasonableness, with respect to technological innovations and graduated invasiveness based on the pervasiveness of technology and very publicly discussed intelligence collection authorities in the Patriot Act and other public laws,[294] appears to dictate that, as technology develops and proliferates, reasonable expectations about how that technology might be used also evolves.

Any contemporary discussion of government surveillance programs generally begins with the materials attributed to Snowden, published starting in June 2013.[295] Among other things, the leaks gave impetus

---

292. *See, e.g.*, Dana Priest and Barton Gellman, *U.S. Decries Abuse but Defends Interrogations; 'Stress and Duress' Tactics Used on Terrorism Suspects Held in Secret Overseas Facilities*, WASH. POST (Dec. 26, 2002) (cited by Bootie Cosgrove-Mather, "Outsourcing Torture," CBS NEWS OPINION (Sept. 22, 2009), http://www.cbsnews.com/2100-215_162-619513.html); *Campaigners Demand US 'Torture' Probe*, BBC NEWS (Dec. 27, 2002), http://news.bbc.co.uk/2/hi/americas/2607629.stm; Adam R. Pearlman, *Legality of Lethality: Paradigm Choice and Targeted Killings in Counterterrorism Operations* (Mar. 23, 2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1583985; Adam R. Pearlman, *Federal Cybersecurity Programs* (May 7, 2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1655105.

293. *See* ACLU v. CIA, 710 F.3d 422 (D.C. Cir. 2013); Raffaela Wakeman, *Appellant Brief Filed in ACLU v. CIA (Drone Program FOIA Request)*, LAWFARE (Mar. 16, 2012), http://www.lawfareblog.com/appellant-brief-filed-aclu-v-cia-drone-program-foia-request (summarizing the ACLU's arguments).

294. We should note early on in this discussion that, although a lack of secrecy (a/k/a, public knowledge) logically impacts expectations, and the resulting conversation is, perhaps, legally relevant in the Fourth Amendment context, any doctrine accepting this proposition should be careful not to incentivize leaks as a means of deliberately degrading privacy expectations. We would expect, however, that security concerns would seem to be a natural check against such practice.

295. In 1984, then-Prime Minister of Singapore Lee Kuan Yew said:

> Because American officials release secrets, that is supposed to be the 'in' thing. It shows that yours is a free society where if any ministers or courts

to rebooting the presidentially appointed Privacy and Civil Liberties Oversight Board ("PCLOB"), created by IRTPA in 2004[296] but dormant since 2008.[297] Snowden's leaks included information related to collection under the Patriot Act's "library records" provision and section 702 of the amended FISA that provided broadly for the targeting of non-U.S. persons reasonably believed to be located outside the United States to acquire foreign intelligence information.[298] Under the authority of section 215 of the Patriot Act, "the NSA collects telephone call records or metadata—but not the content of phone conversations—covering the calls of most Americans on an ongoing basis, subject to renewed approvals by the [FISC]."[299] Separately, under section 702 of the FISA, "the government collects the contents of electronic communications, including telephone calls and emails, where the target is reasonably believed to be a non-U.S. person located outside the United States."[300]

A few months after those disclosures, the Justice Department began disclosing to certain criminal defendants instances in which some information derived from warrantless intelligence-driven surveillance led to evidence later used against them in court.[301] Ever since, there

---

> suppress the truth you feel it is your duty to leak it to the opposition. That is something new, and it is not proven. So when you tamper around with the fundamentals of society . . . the effects are in the next, and often after the next, generation.

Adam R. Pearlman, *Vision and Leadership: A Review of 'Lee Kuan Yew: The Grand Master's Insights on China, the United States, and the World, Interviews and Selections*,' 16 ENGAGE 67, 72 n.6 (2015) (quoting LEE KUAN YEW: THE GRAND MASTER'S INSIGHTS ON CHINA, THE UNITED STATES, AND THE WORLD (2013)). We leave it to the reader to opine about how prophetic on this point Lee may have been.

296. Pub. L. 108-458 § 1061.

297. The PCLOB's chairman, its only full-time member, was confirmed by the Senate five days before the first article on the Snowden material began to appear in the press. The other four members, also Senate-confirmed appointees who were confirmed earlier, serve part-time. To be sure, the timing of the confirmation of the Board's chairman is coincidental; the sudden reliance on that body by other parts of the government, however, is not.

298. 50 U.S.C. § 1881a(a).

299. REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT, PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, at *1 (2014), *available at* https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf. Board member Rachel Brand's separate statement analyzing the section 215 program is available at https://www.pclob.gov/library/215-Brand_Statement.pdf; Board Member Elizabeth Collins Cook's separate statement regarding that provision is at https://www.pclob.gov/library/215-Cook_Statement.pdf.

300. REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, at *1 (2014), *available at* https://www.pclob.gov/library/702-Report.pdf.

301. *See Federal Prosecutors, in a Policy Shift, Cite Warrantless Wiretaps as Evidence*, NY TIMES (Oct. 26, 2013), http://www.nytimes.com/2013/10/27/us/federal-prosecutors-in-a-policy-shift-cite-warrantless-wiretaps-as-evidence.html?hp&_r=1&. Dis-

also has been a constant flow of public reporting of official statements, purported leaks, and mere speculation alike that suggest extraordinary technological capabilities, either in operation now or hoped for in the future. This includes collecting information remotely from "connected gadgets,"[302] tracking and analyzing potential threats and uncovering evidence of crimes through social media,[303] monitoring traffic to certain media sites,[304] and the use of facial recognition software to scan websites for pictures of criminal suspects.[305] These reports have been accompanied by an explosion in the proliferation of cameras—both stationary and mobile, including the use of unmanned aerial equipment (i.e., "drones")[306] and camera-equipped street

closure of *the fact* of FISA-derived evidence, however, does not necessarily entitle a defendant access to the underlying materials. *See* U.S. v. Daoud, 755 F.3d 479 (7th Cir. 2014) (reversing district court's granting cleared defense counsel access to FISA application materials).

302. Rob Waugh, *The CIA Wants to Spy on you Through your TV: Agency Director Says Net-Connected Gadgets will 'Transform' Surveillance*, DAILY MAIL (Mar. 16, 2012), http://www.dailymail.co.uk/sciencetech/article-2115871/The-CIA-wants-spy-TV-Agency-director-says-net-connected-gadgets-transform-surveillance.html.

303. Helen A.S. Popkin, *Careful What you Tweet: Police, Schools Tap Social Media to Track Behavior*, NBC NEWS (Oct. 6, 2013), http://www.nbcnews.com/technology/careful-what-you-tweet-police-schools-tap-social-media-track-4B11215908 ("While criminals — or those guilty of ill-placed sarcasm — aren't wising up about social media oversharing, tools for monitoring Americans online are increasingly accessible and affordable to authorities, no NSA-level clearance required."); Gerry Shih, *U.S. Police Behind Most Requests for Twitter Information,* REUTERS (July 2, 2012), http://www.reuters.com/article/2012/07/02/us-twitter-requests-idUSBRE8611EY20120702.

304. Steve Watson, *Group Forces Congressional Hearing on Big Sis' Twitter, Drudge Spying*, INFOWARS (Feb. 9, 2012), http://www.infowars.com/group-forces-congressional-hearing-on-big-sis-twitter-drudge-spying/ (reporting a congressional hearing into alleged DHS tracking of traffic to, *inter alia*, *The Huffington Post* and *The Drudge Report*).

305. Murray Weiss, *High-Tech NYPD Unit Track Criminal Through Facebook and Instagram Photos*, DNAINFO (Mar. 25, 2013), http://www.dnainfo.com/new-york/20130325/new-york-city/high-tech-nypd-unit-tracks-criminals-through-facebook-instragram-photos.

306. For examples of reporting on surveillance camera-equipped drones, see, e.g., Charles Feldman, *FAA to Ease Rules for Police Agencies to Fly Unmanned Drones*, CBS LOS ANGELES (May 15, 2012), http://losangeles.cbslocal.com/2012/05/15/faa-to-ease-rules-for-police-agencies-to-fly-unmanned-drones/; *Is the NYPD Experimenting with Drones Over the City? Evidence Points to Yes*, CBS NEW YORK (Jan. 23, 2012), http://newyork.cbslocal.com/2012/01/23/is-the-nypd-experimenting-with-drones-over-the-city-evidence-points-to-yes/; Brian Bennett, *Police Employ Predator Drone Spy Planes on Home Front*, L.A. TIMES, (Dec. 10, 2011), http://www.latimes.com/news/nationworld/nation/la-na-drone-arrest-20111211,0,324348.story; Steve Watson, *Air Force Document: Drones Can Be Used to Spy on Americans*, INFO WARS (May 11, 2012), http://www.infowars.com/air-force-document-drones-can-be-used-to-spy-on-americans/; Jack Cafferty, *Should Drones Be Used to Spy on Americans?*, CNN (May 15, 2012), http://caffertyfile.blogs.cnn.com/2012/05/15/should-drones-be-used-to-spy-on-americans/?hptHP_t2; Charles Feldman, *The Age of Drones: Military May be Using Drones in U.S. to Help Police*, CBS LOS ANGELES (June 4, 2012), http://losangeles.cbslocal.com/2012/06/04/the-age-of-drones-military-may-be-using-drones-in-us-to-help-police/; Kurt Nimo, *EPA Using Drones to Spy on Cattle Ranchers in Nebraska and Iowa*, INFO WARS (June 4, 2012), http://www.infowars.com/epa-using-

lights[307] that offer multiple platforms for vehicle license plate identification[308] and facial recognition.[309] The ubiquity of smartphones and

drones-to-spy-on-cattle-ranchers-in-nebraska-and-iowa/; Kris Gutierrez, *Drone Gives Texas Law Enforcement Bird's-Eye View on Crime*, FOX NEWS (Nov. 16, 2011), http://www.foxnews.com/us/2011/11/16/drone-gives-texas-law-enforcement-birds-eye-view-on-crime/. Advancements in technology are reportedly allowing for airborne equipment and their cinematographic payloads to be manufactured at ever-smaller scales, making them increasingly difficult to notice or otherwise detect. *See, e.g.*, *Is That Really Just a Fly? Swarms of Cyborg Insect Drones are the Future of Military Surveillance*, DAILY MAIL (June 20, 2012), http://www.dailymail.co.uk/sciencetech/article-2161647/Is-really-just-fly-Swarms-cyborg-insect-drones-future-military-surveillance.html.

307. Paul Joseph Watson, *New Street Lights to Have 'Homeland Security' Applications*, INFOWARS (Oct. 26, 2011), http://www.infowars.com/new-street-lights-to-have-homeland-security-applications/ (discussing street lights designed such that their "primary capabilities" include "energy conservation, homeland security, public safety, traffic control, advertising, video surveillance."); Paul Joseph Watson, *Talking Surveillance Cameras Coming to U.S. Streets*, INFOWARS (May 14, 2012), http://www.infowars.com/talking-surveillance-cameras-coming-to-u-s-streets/ (reporting the units being installed in Chicago, Detroit, and Pittsburg).

308. *Police License Plate Scanners Record Driver's Locations*, AUTOBLOG (June 28, 2013), http://www.autoblog.com/2013/06/28/police-license-plate-scanners-record-drivers-locations/?icid=maing-grid7%257Cmain5%257Cdl2%257Csec1_lnk2%2526pLid%253D338326; *Secret Federal Government Program Tracks Millions of Motorists*, AUTOBLOG (Jan. 28, 2015), http://www.autoblog.com/photos/secret-federal-government-program-tracks-millions-of-motorists; Ellen Nakashima & Josh Hicks, *Homeland Security is Seeking a National License Plate Tracking System*, WASH. POST (Feb. 18, 2014), http://www.washingtonpost.com/world/national-security/homeland-security-is-seeking-a-national-license-plate-tracking-system/2014/02/18/56474ae8-9816-11e3-9616-d367fa6ea99b_story.html (this particular plan was scuttled the day after this report appeared; *see* Ellen Nakashima & Josh Hicks, *Department of Homeland Security Cancels National License-Plate Tracking Plan*, WASH. POST (Feb. 19, 2014), http://www.washingtonpost.com/world/national-security/dhs-cancels-national-license-plate-tracking-plan/2014/02/19/a4c3ef2e-99b4-11e3-b931-0204122c514b_story.html); Allison Klein & Josh White, *License Plate Readers: A Useful Tool for Police Comes with Privacy Concerns*, WASH. POST (Nov. 19, 2011), http://www.washingtonpost.com/local/license-plate-readers-a-useful-tool-for-police-comes-with-privacy-concerns/2011/11/18/gIQAuEApcN_print.html; Larry Copeland, *Not Just Tolls: E-Z Pass Keeping an Eye on Speeders*, USA TODAY (Dec. 20, 2014), http://www.usatoday.com/story/news/nation/2014/12/19/ez-pass-and-speeding/20558251/ (noting that E-Z Pass claims not to pass info to law enforcement for ticketing purposes, such as timestamp data between fixed-distance toll booths, but the capability is there, as is the raw location data); *DEA Chief: US Abandoned Plans to Track Cars Near Gun Shows*, FOX NEWS (Jan. 28, 2015), http://www.foxnews.com/politics/2015/01/28/dea-chief-us-abandoned-plan-to-track-cars-near-gun-shows/?intcmp=latestnews; Chris Halsne *Mysterious Spy Cameras Collecting Data at Post Offices*, FOX 31 DENVER (Mar. 12, 2015), http://kdvr.com/2015/03/11/mysterious-spy-cameras-collecting-data-at-post-offices/ (noting that the Postal Inspection Service was reportedly using cameras to record customers' cars leaving a Denver-area post office parking lot).

309. *See* Allya Sternstein, *FBI to Launch Nationwide Facial Recognition Service*, NEXTGOV (Oct. 7, 2011), http://www.nextgov.com/nextgov/ng_20111007_6100.php?oref=rss (regarding the Next-Generation Identification system); *Massive FBI Facial Recognition Database Poses Threat to Privacy, Group Says*, FOX NEWS (Apr. 16, 2014), http://www.foxnews.com/tech/2014/04/16/massive-fbi-facial-recognition-database-threat-to-privacy-group-says/?intcmp=obnetwork (same).

similar devices allegedly further enables the possibility of real-time tracking nearly anyone, anywhere, at any time.[310]

Internet search giant Google says surveillance is "on the rise"[311] at a rate that could "break the Internet,"[312] even as it performs law enforcement functions itself by scanning not only the text of the emails its account holders send and receive but also the content of associated attachments.[313] The arguable hypocrisy from that company and others does not end there—several reports have surfaced describing web-based companies' psychological experimentation on and social engineering of unwitting subjects: their customer base.[314] The so-called Net-Neutrality debate also became a thinly veiled proxy war for whether Internet Service Providers would gain greater leverage to potentially manipulate consumer behavior by restricting access to certain websites, particularly streaming platforms, in exchange for higher fees.[315] And even while funding studies to buttress its position that users' search results deserve protections under the First Amendment,

310. Paul Joseph Watson, *Mandatory 'Big Brother' Boxes in All New Cars From 2015*, INFOWARS (Apr. 18, 2012), http://www.infowars.com/mandatory-big-brother-black-boxes-in-all-new-cars-from-2015/; Gerry Smith, *Robert Mueller Can't Rule Out FBI Obtained Data From Carrier IQ*, HUFF. POST (Dec. 14, 2011), http://www.huffingtonpost.com/2011/12/14/robert-mueller-fbi-carrier-iq_n_1148700.html; Catherine Crump, *Are the Police Tracking Your Calls?*, CNN (May 22, 2012), http://www.cnn.com/2012/05/22/opinion/crump-cellphone-privacy/index.html?hptHP_t2; *Secret US Spy Program Targeted Americans' Cellphones*, FOX NEWS (Nov. 14, 2014), http://www.foxnews.com/politics/2014/11/14/secret-us-spy-program-targeted-americans-cell-phones/ (USMS program for law enforcement purposes) ; Delvin Barrett, *CIA Aided Program to Spy on U.S. Cellphones*, WALL ST. J. (Mar. 10, 2015), http://www.wsj.com/articles/cia-gave-justice-department-secret-phone-scanning-technology-1426009924; David Sherfinski, *Congress Demands Answers on Feds' Cellphone Tracking by Simulator Towers*, WASH. TIMES (Dec. 31, 2014), http://www.washingtontimes.com/news/2014/dec/31/leahy-grassley-wants-answers-from-doj-dhs-on-cell-/.

311. Jennifer Martinez, *Google: Surveillance 'Is on the Rise*,' THE HILL (Nov. 12, 2012), http://thehill.com/blogs/hillicon-valley/technology/267591-google-us-made-nearly-8000-requests-for-user-data.

312. Trevor Mogg, *Google Chief Fears Surveillance Could 'Break the Internet*,' FOX NEWS (Oct. 9, 2014), http://www.foxnews.com/tech/2014/10/09/google-chief-fears-surveillance-scandal-could-break-internet/?intcmp=features.

313. *See, e.g.*, Martin Evans, *Paedophile Snared as Google Scans Gmail for Images of Child Abuse*, TELEGRAPH (Aug. 4, 2014, 8:10 PM), http://www.telegraph.co.uk/technology/news/11012008/Paedophile-snared-as-Google-scans-Gmail-for-images-of-child-abuse.html; *see also supra* note 254.

314. *See, e.g.*, Micah L. Sifry, *Facebook Wants You to Vote on Tuesday. Here's How It Messed with Your Feed in 2012*, MOTHERJONES (Oct. 31, 2014, 5:00 AM), http://www.motherjones.com/politics/2014/10/can-voting-facebook-button-improve-voter-turnout; Julian Hattem, *Fed-Backed Twitter Study Draws Fire*, THE HILL (Oct. 18, 2014, 2:57 PM), http://thehill.com/policy/technology/221182-fed-backed-twitter-study-draws-fire; Kashmir Hill, *OkCupid Lied to Users About Their Compatibility as an Experiment*, FORBES (July 28, 2014, 5:44 PM), http://www.forbes.com/sites/kashmirhill/2014/07/28/okcupid-experiment-compatibility-deception/.

315. *See also* David Goldman, *Slow Comcast Speeds Were Costing Netflix Customers*, CNN MONEY (Aug. 29, 2014, 10:18 AM), http://money.cnn.com/2014/08/29/technology/netflix-comcast/index.html?hptHP_bn5.

Google was being investigated by Federal Trade Commission staff for manipulating those same results.[316]

There certainly is bona fide pushback on some of the government's uses of technology, however, from both the legislative and judicial branches, and citizens alike. During the drafting and editing of this Article, Congress considered several privacy- and surveillance-related legislative proposals, including the 'USA Freedom' Act and the Email Privacy Act. The Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring (USA FREEDOM) Act of 2015,[317] which became law on June 2, 2015, includes provisions that cabin bulk records collection previously conducted under section 215 of the Patriot Act to collection based on "specific selection terms," prohibits the use of intelligence collected under section 702 of FISA in court proceedings against United States persons if FISC deems the collection procedure to be "deficient," and increases transparency of the FISA litigation process via declassification and amicus provisions.[318] The Email Privacy Act,[319] which (like the original version of the USA Freedom Act) failed to pass during the 113th Congress, intended to alter the provision of the Electronic Communications Privacy Act of 1986 that "extends Fourth Amendment protections against unreasonable search and seizure only to electronic communications sent or received fewer than 180 days" prior to being sought by investigators.[320] As the law now stands, any information (emails, text messages, pictures, documents) stored on remote servers for longer than 180 days are considered abandoned and are subject to administrative subpoenas; they are not deemed protected by the warrant requirement of the Fourth Amendment.

In related judicial developments, the Supreme Court has ruled that police cannot apply a GPS tracking unit to a suspect's vehicle without a warrant[321] and normally cannot search the content of a suspect's cell phone, even as incident to arrest, absent independent magisterial finding of probable cause.[322] An expansive reading of *Jones* could even

316. *Compare* Kim Zetter, *Search Results Protected by First Amendment, Google-Funded Analysis Says*, WIRED (May 9, 2012, 3:47 PM), http://www.wired.com/threatlevel/2012/05/google-first-amendment/, *with* Rolfe Winkler & Brody Mullins, *How Google Skewed Search Results*, WALL ST. J. (Mar. 19, 2015, 7:25 PM), http://www.wsj.com/articles/how-google-skewed-search-results-1426793553.

317. Pub. L. 114-23 (2015).

318. *See also* Jodie Liu, *So What Does the USA Freedom Act Do Anyway?*, LAWFARE (June 3, 2015, 5:29pm), https://www.lawfareblog.com/so-what-does-usa-freedom-act-do-anyway.

319. Email Privacy Act, H.R.1852, 113th Cong. (2013–14).

320. Lindsay Wise, *Government Wonders: What's in Your Old Emails?*, MCCLATCHY DC (Feb. 11, 2015), http://www.mcclatchydc.com/2015/02/11/256304/government-wonders-whats-in-your.html.

321. United States v. Jones, 132 S. Ct. 945, 949 (2012).

322. Riley v. California, 134 S. Ct. 2473, 2495 (2014) (noting that "[T]he fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders

imply that police cannot use technology as a complete replacement for allocating human resources to traditional law enforcement tasks.[323] Multiple states' high courts have ruled a warrant is also required to track phone location data.[324] And some trial courts, too, are requiring more scrutiny of the technological means by which some evidence is procured, to such an extent that prosecutors have felt compelled to offer generous plea deals to avoid discovery and *Brady* challenges.[325]

The public, too, has not merely been vocal about its apprehension regarding the use of surveillance technologies, such as drones[326] and facial recognition,[327] but also is increasingly utilizing encryption techniques to shield the contents of communications from undesired surveillance.[328] Many people have also "unplugged" from social media

---

fought."). For a learned summary of the 2014 *Riley* decision, with context, see Daniel J. Solove, *Does the U.S. Supreme Court's Decision on the 4th Amendment and Cell Phones Signal Future Changes to the Third Party Doctrine?*, LINKEDIN (June 25, 2014), https://www.linkedin.com/pulse/20140625172659-2259773-does-the-u-s-supreme-court-s-decision-on-the-4th-amendment-and-cell-phones-signal-future-changes-to-the-third-party-doctrine.

323. *See also* Kyllo v. United States, 533 U.S. 27, 35 n.2 (2001). This might include, for example, fully automated speed cameras. *See also* text accompanying note 41, *supra*, regarding concrns about "lazy" law enforcement.

324. Debra Cassens Weiss, *Cops Need a Warrant to Track Cellphone Location Data, a Second State High Court Says*, ABA J. (Feb. 19, 2014, 2:21 PM), http://www.abajournal.com/news/article/cops_need_a_warrant_to_track_cellphone_location_data_a_second_state_high_co/?utm_source=maestro&utm_medium=email&utm_campaign=tech_monthly (describing New Jersey and Massachusetts high court rulings finding unreasonable searches and seizures under their respective states' constitutions).

325. *See, e.g.*, Ellen Nakashima, *Secrecy Around Police Surveillance Equipment Proves a Case's Undoing*, WASH. POST (Feb. 22, 2015), http://www.washingtonpost.com/world/national-security/secrecy-around-police-surveillance-equipment-proves-a-cases-undoing/2015/02/22/ce72308a-b7ac-11e4-aa05-1ce812b3fdd2_story.html?hpid=z1 (Florida judge ordered production of StingRay in case against defendant charged with robbery with a deadly weapon, which carried a four-year sentence. Prosecution refused, and cut a deal for six-months of probation. The judge is reported to have asked the prosecution at a pre-trial hearing, "What right does law enforcement have to hide behind the rules and to listen in and take people's information like the NSA?"). The New York Civil Liberties Union has also won a suit to compel disclosure of Stingray capabilities. *See* Kendra Eaglin, *NYCLU Releases Details of EC Sheriff's Cell Phone Spying*, WKBW BUFFALO (Apr. 7, 2015, 7:09 PM), http://www.wkbw.com/news/nyclu-releases-details-of-ec-sheriffs-cell-phone-spying.

326. Gordon Tokumatsu & Jeanne Kuang, *City Hall Protesters Demand "Drone-Free LAPD*," NBC4 S. CAL. (Aug. 21, 2014, 2:03 PM), http://www.nbclosangeles.com/news/local/City-Hall-Protesters-Demand-Drone-Free-LAPD-272202761.html; *Krauthammer on Drones Flying in US: "Stop It Here, Stop It Now*," REAL CLEAR POLITICS (May 14, 2012), http://www.realclearpolitics.com/video/2012/05/14/krauthammer_on_drones_flying_in_us_stop_it_here_stop_it_now.html.

327. John D. Sutter, *How to Hide from Face-Detection Technology*, CNN (Apr. 29, 2012, 10:25 AM), http://whatsnext.blogs.cnn.com/2012/04/29/how-to-hide-from-face-detection-technology/?hptHP_c2.

328. *See, e.g.*, *New Encryption Technology Hits Nerve with DOJ*, FOX NEWS (Nov. 20, 2014), http://www.foxnews.com/tech/2014/11/20/new-encryption-technology-hits-nerve-with-doj/?intcmp=latestnews; Jose Pagliery, *FBI Director: iPhones Shields*[sic] *Pedophiles from Cops*, CNN MONEY (Oct. 14, 2014, 10:17 AM), http://money.cnn

networks (or at least attempted to), citing privacy and lifestyle reasons.[329] Even former Secretary of the Department of Homeland Security Tom Ridge has said he "[doesn't] want the NSA looking at [his] emails."[330]

But the pushback is far from uniform or consistent. Democratically elected representatives and chief executives at all levels of government continue to ensure broad surveillance authorities,[331] and courts have upheld many of the programs and the secrecy surrounding them.[332] Even public opinion indicates greater acceptance of controversial and arguably intrusive technological means to catch

---

.com/2014/10/13/technology/security/fbi-apple/index.html?hptHP_t2; Pamela Brown & Evan Perez, *FBI Tells Apple, Google Their Privacy Efforts Could Hamstring Investigations*, CNN POLITICS (Oct. 12, 2014), http://www.cnn.com/2014/09/25/politics/fbi-apple-google-privacy. For a particularly thoughtful, brief discussion on the increasing use of encryption tools, also known as "going dark," see Carrie Cordero, *Weighing In on the Encryption and "Going Dark" Debate*, LAWFARE (Dec. 4, 2014, 11:30 AM), http://www.lawfareblog.com/2014/12/weighing-in-on-the-encryption-and-going-dark-debate/.

329. Anick Jesdanun, *As Facebook Grows, Millions Say 'No, Thanks*,' FOX NEWS (May 17, 2012), http://www.foxnews.com/scitech/2012/05/17/as-facebook-grows-millions-say-no-thanks/; Jenna Wortham, *Shunning Facebook, and Living to Tell About It*, CNBC (Dec. 13, 2011, 4:34 PM), http://www.cnbc.com/id/45659248 (relaying the stories of several former Facebook accountholders who deactivated their accounts).

330. Mara Siegler, *Ex-Homeland Secretary: 'I Don't Want the NSA Looking at My Emails*,' NYPOST.COM (Oct. 20, 2013, 3:41 AM), http://pagesix.com/2013/10/30/ridge-doesnt-want-the-nsa-looking-at-his-emails/?_ga=1.221059551.619747476.1382834287.

331. Mark Hosenball, *U.S. Spies Press for Renewal of Broad Electronic Surveillance Law*, REUTERS (Sept. 11, 2012, 6:47 PM), http://www.reuters.com/article/2012/09/11/usa-electronicspying-idUSL1E8KBCW620120911; David Kravets, *Calif. Governor Veto Allows Warrantless Cellphone Searches*, WIRED (Oct. 10, 2011, 11:09 AM), http://www.wired.com/threatlevel/2011/10/warrantless-phone-searches/; *Brown Vetoes Bill Limiting Drone Surveillance*, CBS SACRAMENTO (Sept. 28, 2014, 7:42 PM), http://sacramento.cbslocal.com/2014/09/28/brown-vetoes-bill-limiting-drone-surveillance; *FAA to Ease Rules for Police Agencies to Fly Unmanned Drones*, CBS L.A. (May 15, 2012, 8:16 AM), http://losangeles.cbslocal.com/2012/05/15/faa-to-ease-rules-for-police-agencies-to-fly-unmanned-drones/. There are some instances where it seems clear legislators are passing funding for controversial surveillance equipment for purely political reasons (what political scientists might call "pork barrel"). *See, e.g.*, Katie Drummond, *DHS Doesn't Want Its New Spy Drones*, WIRED (Nov. 1, 2011, 6:39 PM), http://www.wired.com/dangerroom/2011/11/dhs-unwanted-drones/?mbid=ob_ppc_dangerroom.

332. Jason Koebler, *Court Upholds Domestic Drone Use in Arrest of American Citizen*, U.S. NEWS & WORLD REP. (Aug. 2, 2012, 11:32 AM), http://www.usnews.com/news/articles/2012/08/02/court-upholds-domestic-drone-use-in-arrest-of-american-citizen; Dustin Volz, *NSA Spying Wins Another Rubber Stamp*, NAT'L J. (Feb. 27, 2013), http://www.nationaljournal.com/tech/nsa-spying-wins-another-rubber-stamp-20150227; *U.S. Spy Agency Can Keep Mum on Google Ties: Court*, YAHOO! NEWS (May 12, 2012), *available at* https://sg.news.yahoo.com/us-spy-agency-keep-mum-google-ties-court-195145718.html (discussing secrecy of NSA/Google relationship); *Number of Court-Approved Wiretaps Soared in 2010*, FOX NEWS (Aug. 20, 2011), http://www.foxnews.com/politics/2011/08/20/number-court-approved-wiretaps-soared-in-2010/?intcmp=obinsite.

criminals,[333] although it draws the line at other administrative functions of government, like speeding tickets.[334] Shortly after the Snowden leaks, the popular satirical publication The Onion lampooned those expressing outrage over the NSA's purported activities in articles including *Area Man Outraged His Private Information Being Collected By Someone Other Than Advertisers*,[335] and *Terrorist Living In U.S. Gets Why NSA Spying Such A Complicated Issue*.[336]

The acceptance of privacy-sacrificing technologies is also only growing more prevalent with time and is profoundly different across generation gaps, with younger Americans increasingly desensitized to what their parents might have seen as unacceptable intrusions upon their privacy.[337] Even the proposed Email Privacy Act discussed above does not include communications metadata in its increased protections, despite the controversy around the NSA's telephony metadata program studied by the PCLOB. And some scholars have advocated for the easing of bureaucratic restrictions and the higher-than-constitutionally-required burden FISA imposes on the government.[338] This opinion is not merely driven by American technological hegemony;

333. Mary Madden & Lee Rainie, *American's Attitudes About Privacy, Security & Surveillance*, PEW RESEARCH CENTER INTERNET, SCIENCE & TECH (May 20, 2015), http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/ (discussing results of March 2015 Pew study regarding American's attitudes concerning digital life); Dave Helling, *Acceptance of a Semi-Public Digital Life Worries Privacy Advocates*, KANSAS CITY STAR (Mar. 29, 2015), *available at* http://multimedia.thehawkeye.com/story/BC-CPT-ONLINE-PRIVACY-KC————national—1200-words—03-29-071623.

334. *Poll: Catching Criminals Is Fine, But Don't Use Drones for Speeding Tickets, Americans Say*, CNN (June 13, 2012, 2:30 PM), http://news.blogs.cnn.com/2012/06/13/poll-catching-criminals-is-fine-but-dont-use-drones-for-speeding-tickets-americans-say/?hptHP_c1; *see also supra* text accompanying note 332.

335. *Area Man Outraged His Private Information Being Collected by Someone Other Than Advertisers*, THE ONION (June 11, 2013), http://www.theonion.com/articles/area-man-outraged-his-private-information-being-co,32783/.

336. *Terrorist Living in U.S. Gets Why NSA Spying Such a Complicated Issue*, THE ONION (June 11, 2013), http://www.theonion.com/articles/terrorist-living-in-us-gets-why-nsa-spying-such-a,32788/.

337. *See also* Madden & Rainie, *supra* note 333; Heather Kelly, *Survey: Will We Give Up Privacy Without a Fight?*, CNN (Dec. 18, 2014, 10:05 AM), http://www.cnn.com/2014/12/18/tech/innovation/pew-future-of-privacy/index.html?hpt=hp_bn5; Wortham, *supra* note 329 (noting "[society's adoption of] new behaviors and expectations in response to the near-ubiquity of Facebook and other social networks" that increase the pressure to share personal information via social media); Dylan Stableford, *'Who is Rodney King?' 'Who is Dick Clark?' 'The Titanic was Real?!?!' How Death, Major News Events Expose Twitter's Generation Gap*, YAHOO! NEWS (June 19, 2012, 7:08 AM), http://news.yahoo.com/blogs/the-cutline/rodney-king-dick-clark-titanic-real-death-major-110858944.html (discussing the generation gap with respect to both knowledge and expectations); Sarah B. Weir, *10 Things You Don't Know about Teens and Social Networking*, YAHOO! ENT. (Aug. 17, 2011), https://en-maktoob.entertainment.yahoo.com/blogs/parenting/10-things-you-dont-know-about-teens-and-social-networking-2527367.html.

338. *See, e.g.*, Ronald J. Sievert, *Time to Rewrite the Ill-Conceived and Dangerous Foreign Intelligence Surveillance Act of 1978*, 3 NAT. SEC. L.J. 47 (2014).

rather, in many respects, U.S. government surveillance practices are less invasive than those of other democracies.[339]

Considering everything discussed in this Article—private-sector surveillance and data collection capabilities, society's increased reliance on the convenience of communications technology despite those well-publicized practices and known vulnerabilities,[340] the equally well-known demise of the intelligence/law enforcement wall, and inconsistent steps taken by both political actors and private citizens with respect to evincing a desire for greater privacy—it appears that the constitutional reasonable-expectation-of-privacy concept as the Supreme Court thought of it in *Katz* is, empirically speaking, a legal fiction.

Even so, that notion does not end the legal inquiry as the absence of "constitutionally protected area"[341] is not necessarily the *coup de*

339. Although many other countries, including U.S. allies, have cited privacy concerns in complaints of reported U.S. government surveillance practices, many of those countries have robust domestic intelligence agencies with invasive surveillance practices. *See* Sievert, *supra* note 338, at 82–92 (describing authorities in Germany, the United Kingdom, France, Spain, and Italy); Mark H. Gitenstein, *Nine Democracies and the Problems of Detention, Surveillance, and Interrogation*, *in* LEGISLATING THE WAR ON TERROR: AN AGENDA FOR REFORM (Benjamin Wittes, ed. 2009) (describing Australia, France, Germany, India, Israel, Spain, South Africa, and the United Kingdom). The peculiarity of the complaints in light of those counties' own domestic intelligence surveillance powers is heightened by the antitrust actions taken against U.S. tech companies, which suggests the supposed privacy concerns may be driven, at least in part, by competition policy in a field where businesses in those countries fall behind U.S. companies' technological capabilities. *See also* Danny Hakim, *Google is Target of European Backlash on U.S. Tech Dominance*, N.Y. TIMES (Sept. 8, 2014), http://www.nytimes.com/2014/09/09/technology/google-is-target-of-european-backlash-on-us-tech-dominance.html?_r=0. Indeed, even within the United States, concerns over U.S. government surveillance sometimes conflate international opinion with Americans' privacy. These are two independent questions—the former is a foreign policy issue; the latter is one of constitutional law. *See also* Patrick Tucker, *NSA Chief: Yes, We Still Have Friends*, DEFENSE ONE (Sept. 16, 2014), http://www.defenseone.com/politics/2014/09/nsa-chief-yes-we-still-have-friends/94265/ (noting Admiral Rogers' remarks of continued strong foreign partnerships amid growing cyber threats).

340. With respect to data vulnerability, noting that there may not be a reasonable expectation of privacy in online communications in part because users cannot control the third-party routing of the information is not to suggest that the legal analysis is simply kowtow to bad actors with profound capabilities, such as criminal hackers. Just because the public either knows of or can imagine certain empirical realities does not mean we are forced to accept them as "reasonable" in the law. That the Fourth Amendment may not reach as far to protect online communications as we might like, in part because of the inherent vulnerability of those communications, is not to simply resign the Constitution in light of seemingly omnipresent and overwhelming criminal or enemy elements. It should never be required of American society to accept as reasonable the malicious acts of people or organizations that aim to pilfer, abuse, or take advantage of the freedoms our Constitution enshrines. But such recognition is important as an empirical baseline, and driving honest debates concerning the myriad of technology-driven challenges to civil liberties.

341. *See* United States v. Knotts 460 U.S. 276, 285–88 (Brennan, J., concurring).

grace to privacy in general.[342] Indeed, much of modern privacy is based on statutory or regulatory regimes that might be said to parallel tort law principles in making certain expectations reasonable per se. A prime example of this concerns medical information, which is considered to be worthy of very stringent privacy protections. The Health Insurance Portability and Accountability Act ("HIPAA"),[343] for example, is partly the result of the general recognition that there is no constitutional right to privacy in third party records, especially ones that must be shared across businesses. Similarly, the Genetic Information Nondiscrimination Act ("GINA")[344] applies HIPPA's privacy standards to genetic information[345] and prohibits health insurance companies from altering premiums and employers from making hiring and firing decisions based upon genetic predispositions.[346]

In passing HIPAA and GINA, Congress has acted to legislate privacy-favoring policies into law, filling gaps left open in constitutional jurisprudence. It stands to reason, then, that Congress can similarly act with respect to privacy in the realm of national security surveillance and data collection. Indeed, privacy advocates' calls upon Congress to "reign in" the NSA also betray an underlying recognition that what that agency is accused of doing may not actually be unconstitutional, even though it is subject to regulation in important respects. Although plenary constitutional powers may limit Congress's ability to curtail national security intelligence *collection* and possibly retention and analysis if those functions are deemed similarly to fall within the President's Article II powers (though Congress would maintain considerable discretion over funding those functions), Congress could ensure that any surveillance or data gathered could only be *used* in certain ways with respect to U.S. persons, including and especially American citizens.[347] If the Fourth Amendment and certain other

342. United States v. Jones, 132 S. Ct. 945, 953 n.8 (2012) ("Fourth Amendment protects against tresspassory searches only with regard to those items ('persons, houses, papers, and effects') that it enumerates."). Thus, not all searches have constitutional implications.

343. Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, 110 Stat. 1936 (1996).

344. Genetic Information Nondiscrimination Act of 2008, Pub. L. 110–233, 122 Stat. 881 (2008).

345. *Id.* § 105.

346. *Id.* §§ 101, 202.

347. Although not explored in depth here, it bears noting the differences in collection, retention, and usage of data, the last of which might include analysis, sharing, or otherwise acting upon. It is fundamental in Fourth Amendment jurisprudence that *seizure* must interfere with possessory rights, which certainly is not true of data collection nor surveillance. *See, e.g.*, *Jones*, 132 S. Ct. at 951 n.5. The specific Fourth Amendment question must thus be geared to what constitutes a *search* for the purposes of that provision, and how that search does or does not violate reasonable expectations of privacy: "obtaining information is not alone a search unless it is achieved by such a trespass or invasion of privacy." *Id.*

provisions of the Bill of Rights (and the exclusionary rule[348]) are understood to be concerned primarily with protecting the liberty interests of American citizens against the coercive powers of government, rules of evidence or procedure can easily be amended to exclude the use of certain information in criminal prosecutions, or even certain civil enforcement actions, without running afoul of any Separation of Powers principles. One example of such a legislative compromise, as well as the generational pendulum of national security policymaking, is already found in the history of FISA—the former "primary purpose" rule that led to the intelligence/law enforcement wall, which the Patriot Act amended to become the "significant purpose" standard.[349]

This implication of liberty interests is, of course, the major distinction between the private-sector capabilities discussed in Part IV and government employment of the same or substantially similar means in the exercise of its security functions. Further, the Fourth Amendment itself was written as protection from government intrusions,[350] and Americans reasonably should be able to expect that our government adhere to our stated values. Nevertheless, the Constitution builds in this balancing test of reasonableness, which is properly analyzed in light of how American society actually operates and how the Ameri-

348. Although the Supreme Court grounded its pronouncement of the exclusionary rule in the Fourth Amendment, *Weeks v. United States*, 232 U.S. 383, 389–99 (1914), Justice Frankfurter later noted the rule "was not derived from the explicit requirements of the Fourth Amendment [nor] based on legislation expressing Congressional policy in the enforcement of the Constitution." Wolf v. Colorado, 338 U.S. 25, 28 (1949), *rev'd on other grounds*, Mapp v. Ohio, 367 U.S. 643 (1961).

349. We recognize the many drawbacks of a privacy regime governed largely by statute and regulation. Beyond the principle of the potentially uncomfortable concept that "reasonable expectation" concept in constitutional law may not fit squarely with today's realities, several prudential downsides include a hyperactive legislature, overreaching or overcomplicated regulations, the potential of slow and inefficient legislative and judicial processes, separation of powers implications, and the potential that classified exceptions may be made to promulgated regulations, including Executive Orders. For further discussion on this last point, see JAMES E. BAKER, IN THE COMMON DEFENSE: NATIONAL SECURITY LAW FOR PERILOUS TIMES 78 (2007). For a discussion of how this concept might apply in another national security-related context, see Pearlman, *Legality of Lethality*, *supra* note 292. To those who think a statutory fix in this regard ignores the Constitution, however, see Steve Vladeck, Professor of Law at Am. Univ. Washington Coll. of Law, Presentation at the *Texas A&M Law Review* Symposium: *New Technology and Old Law Rethinking National Security* (Oct. 17, 2014) (commenting during the question and answer period after the presentation), we unequivocally believe that the Constitution always matters, but so does the manner in which we conduct ourselves in accordance with our values. We note that it is also part of our system of government to have a robust mechanism to impose statutory limits on government activities, which increasingly seem to be the only available means of maintaining the legal fiction of privacy. This Article has argued that, even if Americans are lowering the constitutional bar by our actions, it may still be possible to raise our expectations back up again with mere words through legislation.

350. Bear in mind that the Foreign Intelligence Surveillance Court of Review has recognized an exception for foreign intelligence gathering. *See In re* Directives [redacted text] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008).

can people really behave. As the Supreme Court has held repeatedly since *Katz*, "a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable."[351] The requisite societal recognition must be more than mere vocalization of concern.

Despite the fact that hacking and data breaches are only expected to continue to increase,[352] we regularly "exchange[ ] privacy for convenience,"[353] and further find ourselves in the midst of an explosion in home-based connected technology, including cameras[354] and microphones,[355] with life-like robots reportedly on the horizon,[356] all of which not only can be hacked as individual devices but also leave entire in-home networks vulnerable.[357] If two private citizens can build a drone in their garage that can hack personal WiFi networks and listen to peoples' phone calls for $6,000 using off-the-shelf electronics,[358]

351. Kyllo v. United States, 533 U.S. 27, 33 (2001). In his concurring opinions in Fourth Amendment cases, Justice Alito repeatedly takes note of the peculiar challenges inherent in this standard. In *Jones*, he wrote that expectation of privacy test "involves a degree of circularity and judges are apt to confuse their own expectations of privacy with the hypothetical reasonable person to which the *Katz* test looks." United States v. Jones, 132 S. Ct. 945, 962 (2012) (citing *Kyllo*, 533 U.S. at 34). With respect to *Riley v. California*, he opined that "it would be very unfortunate if privacy protection in the 21st century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment." Riley v. California, 134 S. Ct. 2473, 2497 (2014).

352. *See, e.g.*, Jay Johnson, *If 2014 Was the Year of the Data Breach, Brace for More*, FORBES (Jan. 2, 2015, 4:50 AM), http://www.forbes.com/sites/danielfisher/2015/01/02/if-2014-was-the-year-of-the-data-breach-brace-for-more/?linkId=11477246&utm_channel=Business.

353. Paul Joseph Watson, *New Microchip Knows Your Location to Within Centimeters*, INFORWARS.COM (Apr. 10, 2012), http://www.infowars.com/new-microchip-knows-your-location-to-within-centimeters/ ("people have willingly exchanged their privacy for convenience"); Kelly, *supra* note 337.

354. Magic Madzik, *Rent-to-Own Laptops Secretly Photographed Users Having Sex, FTC Says*, WIRED, (Sept. 25, 2012), http://www.wired.com/2012/09/laptop-rental-spyware-scandal/.

355. Heather Kelly, *Why Amazon's Echo is the Computer of the Future*, CNN (Nov. 13, 2014, 11:40 AM), http://www.cnn.com/2014/11/12/tech/innovation/amazon-echo-always-listening/index.html?hpt=hp_t2. Apple's 'Siri' feature introduced on the iPhone 4S in 2011, and Microsoft's XBox One also feature microphones with active listening modes that constantly listen for commands directed at them via a natural language user interface. *Id.*

356. Michael Fitzpatrick, *The Hyper-Real Robots That Will Replace Receptionists, Pop Stars. . . and Even Sex Dolls: Unnervingly Human Androids Coming to a Future Very Near You*, DAILY MAIL (Nov. 20, 2014, 4:47 PM), http://www.dailymail.co.uk/news/article-2841273/The-hyper-real-robots-replace-receptionists-pop-stars-sex-dolls-Unnervingly-human-androids-coming-future-near-you.html.

357. *See, e.g.*, Malia Zimmerman, *Hacking into Your Home: TVs, Refrigerators Could be Portal to Most Sensitive Info*, FOX NEWS (Apr. 18, 2015), http://www.foxnews.com/tech/2015/04/18/hacking-into-your-home-tvs-refrigerators-could-be-portal-to-most-sensitive-info/; *see also* text accompanying note 287, *supra*.

358. *See* Erin Van der Bellen, *Spy Drone Hacks WiFi Networks, Listens to Calls*, WUSA9 (Dec. 12, 2014, 12:42 PM), http://www.wusa9.com/story/news/local/2014/12/11/spy-drone-hacking-cell-phones-text-messages/20214047/.

and private companies boast of having better technology than government agencies,[359] the Supreme Court's opinion in *Kyllo* unambiguously suggests those facts to be relevant in whether it is permissible for law enforcement to use similar equipment or means. Even as people continue to voice concerns about government activities while any gaps between public and private technology capabilities dissipate, it appears likely that the market is going to continue to support increasingly invasive private capabilities.[360]

It is further relevant that the Fourth Amendment's maximum force applies to searches of the home and that a key factor in cases extending the Amendment's protection in instances not implicating a search of the home is the defendant's taking affirmative steps to protect his privacy from eavesdroppers. In *Katz*, for example, the defendant shut the door to the phone booth. In the context of electronic communications, these two themes are often echoed with respect to the use of user passwords to access and protect certain content. Passwords are often compared to door locks and, like the additional step of encryption, are unambiguous steps taken to protect one's information.[361] Further, just because one knows and understands the possibility that the lock to his home might be picked does not mean he loses his reasonable expectation of privacy in his home.[362] But it does strike us that there is something fundamentally different about locking one's door and leaving his property to the small chance that it will be burgled, versus leaving otherwise private information on a server in an unknown location, serviced by unknown persons, and protected by a password that the user also has given to the same third-party caretaker that manages that server. If passwords are like door locks, then those who maintain servers are merely house sitters, and if there can be no *constitutionally* reasonable expectation of privacy against them (though they might nevertheless be subject to criminal or civil liability for theft or damages),[363] then any argument that the government

359. *See, e.g.*, Derrick Harris, *Google: Our New System for Recognizing Faces Is the Best One Ever*, FORTUNE, (Mar. 17, 2015, 5:05 PM), http://fortune.com/2015/03/17/google-facenet-artificial-intelligence/.

360. *See* Kelly, *supra* note 337 (quoting Janna Anderson Elon Imagining the Internet Center, Director "people have proven that they will give away personal information for something as small as a free cup of coffee.").

361. The Eleventh Circuit has even accorded constitutional protection to passwords with respect to the Fifth Amendment right against self-incrimination. *See* In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011, 670 F.3d 1335, 1341–42 (11th Cir. 2012) (holding that compelling a suspect in a child pornography investigation to provide his password to decrypt a hard drive would require him to engage in a testimonial action in violation of his Fifth Amendment's rights).

362. *See also supra* note 340.

363. *Cf.* Everett Rosenfeld, *AT&T Data Breaches Revealed: 280k US Customers Exposed*, CNBC (Apr. 8, 2014, 1:19 PM), http://www.cnbc.com/id/102570147 (describing the Federal Communications Commission's $25 million fine against AT&T for consumer privacy violations, resulting from an investigation in which employees in Mexico, the Philippines, and Colombia accessed over a quarter-million user accounts

would be acting unconstitutionally by executing a lawful court order compelling a relationship with that third-party that does not result in material loss or tangible harm to the user, rings hollow. Put bluntly, the Internet, and especially "the cloud," is not one's home. The closest analogy is valet parking, and it would not seem reasonable to put one's most valuable assets—including documents with personal information—into a vehicle about to be turned over to a valet.[364]

In Judge Keith's district court opinion that the government appealed in the *Keith* case, he wrote, "The great umbrella of personal rights protected by the Fourth Amendment has unfolded slowly, but very deliberately, throughout our legal history."[365] At its core, however, the Fourth Amendment is a prophylactic measure devised to check the uniquely extraordinary and coercive powers of the central government of a post-Westphalian nation-state. From that perspective, it is worth remembering that it did not even apply to the several states until 1961.[366] This Article has demonstrated that, today, the electronic surveillance capabilities of the government are far from "uniquely extraordinary," and that the everyday actions of a significant percentage of Americans include unambiguously relinquishing control of very personal information in public and/or insecure communications that raise serious questions about the very existence of "privacy" as a factual predicate for modern Fourth Amendment analyses. The characterization of the present debate as being about privacy as an independent and monolithic notion may even do a disservice to the probability of achieving a just and sound outcome within our constitutional system. Perhaps, rather, it is best conceptualized in terms of determining the proper role of government and scope of its authorities, as should be the starting point for virtually any domestic policy analysis. If privacy interests were the initial driver for our form of limited government as enshrined in the Constitution, it seems illogical simply to assert any particular government program violates privacy without first taking account of the proper role(s) of government, and its responsibilities to its citizens, in light of the grand bargain that begot the Constitution in the first instance.[367]

---

without authorization, and sold the account information to third-parties), *available at* http://www.cnbc.com/id/102570147.

364. *Cf.* Scott Shane, *Data Storage Could Expand Reach of Surveillance*, N.Y. TIMES (Aug. 14, 2012, 5:50 PM), http://thecaucus.blogs.nytimes.com/2012/08/14/advances-in-data-storage-have-implications-for-government-surveillance/?hp (Blog post on The Caucus).

365. United States v. Sinclair, 321 F. Supp. 1074, 1077 (D. Mich. 1971).

366. *See* Mapp v. Ohio, 367 U.S. 643, 554–55 (1961).

367. *But see* Peggy Noonan, '*A Nation of Sullen Paranoids' Too Much Security Can Produce a Kind of Madness*, WALL ST. J. (Aug. 23, 2013, 6:53 PM), http://www.wsj.com/articles/SB10001424127887324619504579029170678905440.

> There are too many built-in dynamics that make the national-security state want to grow, from legitimate fears of terrorism, to bureaucratic pride, to the flaws in human nature. And there are too many dynamics that will allow it

The reality is that a certain degree of monitoring is, unfortunately, necessary in this technology-driven age. Although the development of technology in the abstract is most often understood to be morally neutral,[368] technical means have been recognized as increasingly important complements to human intelligence collection,[369] and surveil-

> to grow. The aftermath of 9/11 happened to coincide with a new burst in American technological innovation and discovery: The government has the ways and means to do pretty much anything now, and if they can do it they will do it. If the citizens of the United States don't put up a halting hand, the government can't be expected to: It is in the nature of security professionals to always want more, and since their mission is worthy they're less likely to have constitutional qualms, to dwell on such abstractions as abuse of the Fourth Amendment and the impact of that abuse on the First.

Id.

368. *See* Albert C. Lin, *Technology Assessment 2.0: Revamping our Approach to Emerging Technologies*, 76 BROOKLYN L. REV. 1309, 1338–39 (2011) ("The predominant model of technology development, however, is for scientists and engineers to conceive of technology instrumentally; that is, as value free and neutral, not based on morals." (citations omitted)). *But see also* Edward S. Dove, *Back to Blood: The Sociopolitics and Law of Compulsory DNA Testing of Refugees*, 8 U. MASS. L. REV. 466, 500–01 (2013) (citing scholars who disagree with the supposed moral neutrality of technology). In this vein, it is important to be mindful of the threats technological proliferation may pose to governments, as well. For one, as illustrated above with respect to the ACLU's FOIA litigation about alleged targeted killings, technology is proving repeatedly to be a tool for undermining government secrecy. *See also* Robert Chesney, *The Shadow War Is Not Very Shadowy*, LAWFARE (June 14, 2012, 3:06 PM), http://www.lawfareblog.com/shadow-war-not-very-shadowy. It has even been said that the Internet "keeps the government honest." *See* Shantanu Chauhan, *Internet Keeps Government Honest: Google Chief,* CYBER TECHNOLOGY NEWS (Nov. 13, 2011), http://cybertechnologynews.in/internet-keeps-government-honest-google-chief/. On the local level, interactions with police officers are now routinely video-recorded. Similar real-time exposure extends all the way to the realm of global affairs, as perhaps best illustrated by Sohaib Athar's live-tweeting of the Special Forces operation that resulted in the death of Osama bin Laden. And, of course, technology continues to be used in abjectly nefarious ways against the government, from denial of service attacks to hacking for sensitive data, to targeting personnel. *See, e.g.*, Ryan Lovelace, *Drones in Our Future*, NAT'L REVIEW (Feb. 4, 2015, 5:54 PM), http://www.nationalreview.com/article/397930/drones-our-future-ryan-lovelace (describing law enforcement concerns about Mexican drug cartels using drones not just to transport drugs, but to surveil officers. "The biggest concerns about cartel-operated drones, [Drug Enforcement Administration Special Agent Matt] Barden says, have nothing to do with the actual movements of drugs. 'Is it a good way to get some dope out of the woods or out of the jungle to a waiting car or vehicle? Yeah,'" Barden says. 'Better yet, to me personally, is it a better way to perform surveillance on law enforcement? Absolutely. That scares me a whole lot more than does the smuggling aspect of it.'"); Con Coughlin & Ben Farmer, *Intelligence Agencies in 'Technology Arms Race,'* THE TELEGRAPH (Mar. 30, 2015), http://www.telegraph.co.uk/news/uknews/defence/11504702/Intelligence-agencies-in-technology-arms-race.html (noting that "modern technology had been a boon for spy craft, but had also increased the risks to spies and agents"). Even individual legislators have felt their privacy imposed upon by technology. Alex Isenstadt, *Lawmakers: Candidates Almost Being Stalked*, POLITICO (Aug. 3, 2012, 10:39 AM), http://www.politico.com/news/stories/0812/79328.html.

369. *See also* Greg Miller, *CIA Looks to Expand Its Cyber Espionage Capabilities*, WASH. POST (Feb. 23, 2015), http://www.washingtonpost.com/world/national-security/cia-looks-to-expand-its-cyber-espionage-capabilities/2015/02/23/a028e80c-b94d-11e4-9423-f3d0a1ec335c_story.html (noting Director Brennan sees *cyber/tech as increas-*

lance-derived information has been credited with helping to prevent numerous terrorist attacks.[370] Another critical function of monitoring Internet traffic in particular is cybersecurity—it would be impossible to defend against cyber-attacks effectively if the intelligence agencies are not allowed to leverage any capability that might have the potential to touch upon otherwise presumptively private communications.[371]

If privacy is to be a legal fiction, it is one best maintained through the vigilance of not only those charged with writing our laws and otherwise actively protecting our security but also ourselves through the conscious choices we make in how we interact with each other on both social and commercial levels. The importance of the debate includes the need to be frank about the scope of permissible surveillance targets, especially in counterterrorism scenarios.[372] Further, as recog-

---

ingly intertwined with the human collection process, and describing what amounts to Goldwater-Nichols-type reforms within the agency, using the directorates as talent development mechanisms to farm personnel out to fusion/joint/hybrid centers that blend the disciplines in effective ways, a la NCTC, which, of course, he used to direct).

370. *See, e.g.*, Joseph Weber, *Boehner Credits US Surveillance in Catching Capitol Bomb Plot*, FOX NEWS (Jan. 15, 2015), http://www.foxnews.com/politics/2015/01/15/boehner-credits-us-surveillance-in-catching-capitol-bombing-plot/?intcmp=latestnews. One report by the Heritage Foundation counts sixty-four attempted terrorist attacks against the U.S. homeland since the September 11, 2001, attacks, and predicts the rate of such plots to increase. *See* Malia Zimmerman, *Think Tank Tallies 64 Terror Plots Targeting American Homeland Since 9/11*, FOX NEWS (Apr. 1, 2015), http://www.foxnews.com/us/2015/03/31/think-tank-tallies-64-terror-plots-targeting-american-homeland-since-11/.

371. *See also* Kim Zetter, *McCain: Cybersecurity Bill Ineffective Without NSA Monitoring the Net*, WIRED (Feb. 16, 2012, 7:21 PM), http://www.wired.com/threatlevel/2012/02/cybersecurity-act-of-2012/. For a brief unclassified summary of the status of U.S. cybersecurity initiatives and proposals before the Snowden disclosures, including the Comprehensive National Cybersecurity Initiative, see Adam R. Pearlman, *Federal Cybersecurity Programs*, NEW FED. INITIATIVES PROJ., *available at* http://ssrn.com/abstract=1655105.

372. Determining the scope of permissible targets for counterterrorism surveillance requires a clear notion of what "terrorism" is, and who is likely to participate in it. It is therefore notable that, there is no single, unified definition of "terrorism" in the United States Code. Coming to a consensus on the legal contours of that term has been so elusive, even a volume dedicated to recommending legislative changes to various aspects of counterterrorism law that included chapters by some of the preeminent scholars in national security law, lacked a proposal to do so. *See* Adam R. Pearlman, *Institutionalizing Counterterrorism: A Review of Legislating the War on Terror: An Agenda for Reform*, ENGAGE, Dec. 2010, at 107 (Benjamin Wittes, ed.), *available at* http://www.fed-soc.org/publications/detail/institutionalizing-counterterrorism-a-review-of-legislating-the-war-on-terror-an-agenda-for-reform-edited-by-benjamin-wittes/ ("Although the conspicuous absence of a proffered single definition of terrorism may simply indicate a common acceptance that we are in a fight with enemies incapable of a one-size-fits-all legislative definition, its absence leaves open the possibility of uneven, indeed perhaps even arbitrary, applications of the term. Common colloquial usage does not sound policy make. Rather, its greatest potential is to feed the divisive fervor of political rhetoric used by those in ofice to justify extraordinary uses of power by themselves, and leads to charges of fear-mongering by those who are not. Several authors in this book point out that dictators often begin their

nized repeatedly in Supreme Court jurisprudence, there are fundamental differences between measures used in protecting those interests that might be considered "domestic security"[373] versus those with a foreign nexus. And the lone wolf dilemma will continue to loom large, especially as copycats and those inspired by overseas elements increasingly pose real threats inside the United States.[374]

From Internet companies like Google[375] and Facebook[376] to cellular service providers, cell phone "app" programmers, and vehicle manu-

---

tyranny by labeling dissenters as "terrorists," and argue that the distinction between liberty and security is a false one. And in recalling the lessons of our own history, perhaps best highlighted by the disdain with which we associate McCarthy-era blacklists, we are reminded of the effect that labeling peoples and behaviors can have on national political and policy priorities, and how they impact our well-being as a nation under the rule of law. . . .").

373. *See, e.g.*, *Keith*, 407 U.S. 297 (1972). On a related note, it is important to remember that, "for all the very important focus on national-level domestic intelligence law and policy, on account of federal legal, political, and resource predominance, note that there remains a lot of heterogeneity and local variation because most policing in the United States is conducted and controlled at the local level." Matthew Waxman, *More on NYPD and Local Counterterrorism Intelligence*, LAWFARE (May 25, 2012, 10:22 AM), http://www.lawfareblog.com/more-nypd-and-local-counterterrorism-intelligence. This remains true even if local police forces receive federal assistance in resourcing their departments. *See, e.g.*, Jack Gillum & Eileen Sullivan, *U.S. Pushing Local Cops to Stay Mum on Surveillance*, YAHOO (June 12, 2014, 4:32 PM), http://news.yahoo.com/us-pushing-local-cops-stay-174613067.html.

374. *See US Intelligence to Keep Tabs on Americans with No Ties to Terror*, FOX NEWS (Mar. 22, 2012), http://www.foxnews.com/politics/2012/03/22/us-intelligence-to-keep-tabs-on-americans-with-no-ties-to-terror/; Laura Koran, *Threat of Lone Wolf Attacks Worries Homeland Security Chief*, CNN (Nov. 16, 2014, 10:19 PM), http://www.cnn.com/2014/11/16/politics/homeland-security-lone-wolf/index.html?hptHP_t2 (quoting Homeland Security Secretary Jeh Johnson discussing social media activity as an inspiration for people with no other connections to terrorist organizations, "The new phenomenon that I see that I'm very concerned about . . . is somebody who has never met another member of that terrorist organization, never trained at one of the camps, who is simply inspired by the social media—the literature, the propaganda, the message—to commit an act of violence in this country." The article continues, "Johnson added that, while the U.S. government has largely been successful in disrupting plots hatched by terrorist cells abroad, catching individuals who are not formally connected requires them to take a different tactic—relying heavily on state and local law enforcement.") A recent Heritage Foundation report found that, of the sixty-four terrorist plots against the U.S. homeland that it counted between September 11, 2001, and March 2015, fifty-three of them "were plotted or perpetrated by homegrown extremists. *See* Zimmerman, *supra* note 370.

375. Richard Feloni, *Google is Testing a Program that Tracks You Everywhere You Go*, BUS. INSIDER (Nov. 7, 2013, 3:29 AM), http://www.businessinsider.com.au/google-testing-retail-tracking-program-2013-11; Liam Spradlin, *Exclusive: Google Will Soon Introduce 'Nearby' to Let Other 'People, Places, and Things' Know When You're Around*, ANDROID POLICE (June 6, 2014), http://www.androidpolice.com/2014/06/06/exclusive-google-will-soon-introduce-nearby-to-let-other-people-places-and-things-know-when-youre-around/.

376. Julian Hattem, *Facebook Claims 'a Bug' Made It Track Nonusers*, THE HILL (Apr. 9, 2015, 6:18 PM), http://thehill.com/policy/technology/238399-facebook-claims-a-bug-made-it-track-people-not-on-facebook.

facturers[377] monitoring consumers, to employers monitoring employees,[378] remote electronic tracking has become a fact of modern American life. In addition to consumers' tacit consent to such tracking by continuing to use the goods and services that track them, individuals also increasingly sacrifice not just their own privacy, but that of others (including their children) with countless posts of pictures and videos that have created a narcissistic culture of exploitation for entertainment purposes, exposing them and their antics to voyeuristic strangers constantly and desensitizing themselves and others (especially in younger generations) to the importance of keeping certain things private. Although, as the Bill of Rights recognizes, unwarranted government intrusions can be threats in and of themselves, the U.S. government is not a unique operator in the realm of surveillance and data collection; it does, however, have a unique purpose, which is to protect the American public.[379]

Such a bold statement means nothing, however, if there is no credibility in the system—including both the architecture and the people operating it. In the American constitutional system of limited government, the burden of building and maintaining that credibility is indeed with the government. Although two presidents of different parties, multiple congresses of different compositions, and many federal judges have all given constitutional blessing to these programs that have caused such controversy, perceived missteps, like Director of National Intelligence James Clapper's open Senate testimony about NSA collection on Americans, have led many to be skeptical about the na-

377. Joan Lowy, *Carmakers Unite Around Privacy Protections*, ASSOCIATED PRESS (Nov. 13, 2014, 12:31 AM), http://www.apnewsarchive.com/2014/Carmakers-sign-on-to-principles-to-protect-motorists'-privacy-in-an-era-of-computerized-cars/id-8b512b438b3b41be98bf5d9bfecfc249 ("[C]omputerized cars pass along more information about their drivers than many motorists realize.").

378. *See, e.g.*, Adam Jones, *The Spies in the Cellar Are Now Sidling Up to Your Desk*, FINANCIAL TIMES (Dec. 28, 2014, 1:33 PM), http://www.ft.com/intl/cms/s/0/9412d776-89b4-11e4-8daa-00144feabdc0.html#axzz3NGBqipIS (describing workplace monitoring tools, including sensors in name tags, and desk occupancy sensors). Some employers even have tried demanding employees provide to their (i.e., the employees') passwords for their social media accounts. Rob Manker, *Facebook Joins Fight to Ban Employers from Requiring Workers' Passwords*, CHI. TRIB. (Mar. 23, 2012), http://www.chicagotribune.com/news/local/ct-talk-facebook-passwords-folo-0324-20120324,0,4697740.story; *Senators Call for Federal Probe Over Employers Asking for Facebook Passwords*, FOX NEWS (Mar. 25, 2012), http://www.foxnews.com/politics/2012/03/25/senators-call-for-federal-probe-over-employers-asking-for-facebook-passwords/; David L. Hudson, Jr., *Site Unseen: Schools, Bosses Barred from Eyeing Students', Workers' Social Media*, A.B.A. J. (Nov. 1, 2012 8:10 AM), http://www.abajournal.com/magazine/article/site_unseen_schools_bosses_barred_from_eyeing_students_workers_social_media/.

379. *See, e.g.*, George W. Bush, President Discusses Creation of Military Commissions to Try Suspected Terrorists (Sept. 6, 2006) (noting the President's job is to "protect the American people") (transcript available at http://georgewbush-whitehouse.archives.gov/news/releases/2006/09/20060906-3.html).

ture and value of reported government surveillance programs.[380] Lawfare contributor Jane Chong explains, "To gain the trust of the American people, the intelligence community must be understood as being governed by hard, intelligible jurisdictional constraints. And in the post-9/11, post-Wikileaks and post-Snowden era, it will be harder than ever to persuade Americans that such hard constraints exist."[381] Nevertheless, as seen after the September 11, 2001, attacks, Americans also demand the intelligence community to be effective, and they hold it accountable when tragedy strikes. That in mind, being honest and level-headed about how Americans treat privacy in all aspects of their lives, and how everyday behavior and desire for convenience might enable devastating attacks,[382] is critical to resolving a national security policy dispute for which existing Fourth Amendment precedent has limited applicability.[383]

---

380. *See, e.g.*, Glenn Kessler, *James Clapper's 'Least Untruthful' Statement to the Senate*, WASH. POST (Jun. 12, 2013), http://www.washingtonpost.com/blogs/fact-checker/post/james-clappers-least-untruthful-statement-to-the-senate/2013/06/11/e50677a8-d2d8-11e2-a73e-826d299ff459_blog.html. Notwithstanding arguments that Director Clapper never should have been made to answer certain questions about classified programs during an unclassified hearing, the potential harm from such statements is not merely moral but also economic. *See also* Joseph Menn, *Russian Researchers Expose Breakthrough U.S. Spying Program*, YAHOO NEWS (Feb. 16, 2015, 5:10 PM), http://news.yahoo.com/russian-researchers-expose-breakthrough-u-spying-program-194217480—sector.html (noting potential economic consequences if consumers and trade partners question the integrity of the supply chain of technological products that could have built-in vulnerabilities). In theory, manufacturers of physical technology-sector goods might be subject to the same standards as technology service providers. Note, however, that a complete assessment of the potential economic cost requires weighing the potential economic losses from concerns about supply chain integrity against the costs of unattributable cyberattacks that might be more likely to occur without such tools. *Cf.* Barry Ritholtz, *Cybercrime Is Your Worry, Too*, WASH. POST, Apr. 12, 2015, at F1 (noting that cybercrime costs the United States $100 billion annually, out of a total estimated $575 billion cost to the global economy).

381. Jane Chong, *Why Americans Don't Trust the Intelligence Community*, LAWFARE (Mar. 3, 2015, 10:30 AM), http://www.lawfareblog.com/2015/03/on-why-americans-dont-trust-the-intelligence-community/.

382. *See* Malia Zimmerman, *Security Expert Pulled Off Flight by FBI After Exposing Airline Tech Vulnerabilities*, FOX NEWS (Apr. 17, 2015), http://www.foxnews.com/us/2015/04/16/security-expert-pulled-off-flight-by-fbi-after-exposing-airline-tech/ (describing a report by the Government Accountability Office discussing the possibility that a commercial airliner's in-flight entertainment system may be vulnerable to a hack that could shut off the engines of the plane).

383. *Cf. In re* Directives [redacted text] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008) ("[W]e hold that a foreign intelligence exception to the Fourth Amendment's warrant requirement exists when surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States.").