2014

Starting Over: Mass Surveillance and a Factual Approach to the Fourth Amendment

Emily Rucker

Starting Over: Mass Surveillance and a Factual Approach to the Fourth Amendment

by

Emily Rucker

Submitted in partial fulfillment of the requirements of the
King Scholar Program
Michigan State University College of Law
under the direction of
Professor Katz
Spring, 2014

INTRODUCTION

In June of 2013, former National Security Agency contractor Edward Snowden leaked a multitude of classified documents that revealed just how much the government knows about the American people.[1] It knows more than most anyone thought.[2] The revelations started a rigorous debate on how much information the government should gather and the manner in which they gather it,[3] all in the age of smartphones, social media, and data brokers. The Fourth Amendment to the Constitution, which protects Americans against unreasonable searches and seizures, is one of the centers in this debate.[4] The modern Fourth Amendment test centers on the reasonableness of a person's subjective expectations of privacy.[5] The digital age and the amount of personal information shared in today's world, both willingly and unwillingly, puts the usefulness of this test into question.[6] After the Snowden leaks, society at large knows that the government is in on the game on an astonishing scale. The reasonable expectation of privacy test will soon fail to protect a sphere of individual privacy,[7] and the Fourth Amendment test must be reshaped with those concerns in mind. This note suggests an overall factual inquiry independent of privacy

---

[1] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 5, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order/.
[2] *See id.* ("[T]his is the first time significant and top-secret documents have revealed the continuation of the practice on a massive scale under President Obama.").
[3] *See* Spencer Ackerman, *Obama Formally Proposes End to NSA's Bulk Collection of Telephone Data*, THE GUARDIAN (March 27, 2014), http://www.theguardian.com/world/2014/mar/27/obama-proposes-end-nsa-bulk-data-collection. In 2014, debate for reform included proposals from members of Congress, outside privacy advocacy groups, and private communications companies. *Id.*
[4] *See, e.g.*, Conor Friedersdorg, *The Spirit of the Fourth Amendment – and the NSA's Disregard For It*, THE ATLANTIC (Mar. 19, 2014), http://www.theatlantic.com/politics/archive/2014/03/the-spirit-of-the-fourth-amendment-and-the-nsas-disregard-for-it/284498/.
[5] *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 954-55 (2012) (Sotomayor, J., concurring).
[6] *See, e.g.*, JULIA ANGWIN, DRAGNET NATION 30-34 (2014) (detailing who collects data and with whom they share it).
[7] *See infra* Section IV.A.

expectations, as well as an abolishment of the third party doctrine and a strengthening of digital privacy laws.[8]

Part I of this paper discusses Fourth Amendment jurisprudence, including the traditional test, the modern test, the third party doctrine, and recent rulings in cases involving technological surveillance. Part II discusses the scope of the National Security Agency internet metadata and telephone data surveillance programs. Part III provides an overview of recent rulings on the constitutionality of the NSA programs. Part IV suggests possible changes to the Fourth Amendment test, including a shift from subjective expectations of privacy to a factual analysis, and the elimination of the third party doctrine.

I. THE FOURTH AMENDMENT

The text of the Fourth Amendment protects "persons, houses, papers, and effects, against unreasonable searches and seizures" and also requires that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[9] Approaches to the interpretation of the amendment have varied over time, with a shift in the 1960s that gave rise to the modern test.[10] Each Fourth Amendment question requires a two-step analysis: Was the area or interest intruded on by the government protected under the Fourth Amendment, and, if so, was the intrusion reasonable?[11] The search will be reasonable if undertaken pursuant to a warrant supported by probable cause or under certain other exceptional circumstances.[12]

---

[8] *See infra* Section IV.C.
[9] U.S. Const. amend. IV.
[10] *See, e.g.*, Katz v. United States, 389 U.S. 347 (1967); *compare to* Olmstead v. United States, 227 U.S. 438, 464 (1928).
[11] ACLU v. Clapper, No. 13 Civ. 3994, 2013 WL 6819708 (S.D.N.Y. Dec. 27, 2013). It is important to distinguish these two inquiries in the context of mass surveillance. According to one court, "dragnet character doesn't

A. Traditional Test: Spheres of Protection

A brief examination of the history of the Fourth Amendment is worthwhile when discussing traditional Fourth Amendment jurisprudence.[13] Although original intent arguments can be problematic giving the impossibility of ascertaining the actual intent of the Framers, certain fundamental concepts can be drawn from the historical record.[14] In England, the issuance of general warrants was common, authorizing broad ranges of places to be searched, items to be seized, and people to be arrested.[15] Colonies including Pennsylvania and Massachusetts had protections against unreasonable searches and seizures, prohibiting warrantless searches or seizures and requiring individualized suspicion to search.[16] Under the conventional view of the Fourth Amendment, the first clause implies that the people have a general right against government intrusions and invasions of privacy, and the second clause specified when those invasions would be reasonable and permissible.[17] This note is concerned mainly with the issue of what interests and information are protected by the Fourth Amendment rather than when intrusions on those interests are reasonable.

---

automatically turn it into a search." *Id.* If none of the information gathered by the government is protected under the Fourth Amendment, it is essentially public and the government may gather it as they see fit. *See id.*

[12] Spencer S. Cady, *Reconciling Privacy with Progress: Fourth Amendment Protection of E-Mail Stored with and Sent Through A Third-Party Internet Service Provider*, 61 DRAKE L. REV. 225, 230 (2012).

[13] *See generally* Thomas Clancy, *The Role of History*, 7 OHIO ST. J CRIM. L. 811 (2010).

[14] *See id.* at 813-814 (discussing various histories of the Fourth Amendment and their strengths and weaknesses).

[15] *See* Thomas K. Clancy*, The Role of Individualized Suspicion in Assessing the Reasonableness of Searches and Seizures*, 25 U. MEM. L. REV. 483, 509 (1995) (discussing English case in which general warrant was issued for libel and forty-nine people were arrested).

[16] *Id.* at 513-14.

[17] Thomas Clancy, *The Framers' Intent: John Adams, His Era, and the Fourth Amendment*, 86 IND. L.J. 979, 983 (2011) (quoting Jacob W. Landynski, *Search and Seizure and the Supreme Court: A Study in Constitutional Interpretation*, 84 JOHNS HOPKINS U. STUDIES IN HIST. AND POL. SCI. 1, 19 (1966)) ("The first clause—"[t]he right of the people to be secure . . . against unreasonable searches and seizures, shall not be violated"—recognized as already existing a right to freedom from arbitrary governmental invasion of privacy and did not seek to create or confer such a right. It was evidently meant to re-emphasize (and, in some undefined way, strengthen) the requirements for a valid warrant set forth in the second clause. The second clause, in turn, defines and interprets the first, telling us the kind of search that is not "unreasonable," and therefore not forbidden, namely, the one carried out under the safeguards there specified.").

Traditionally, the Fourth Amendment was thought to protect certain physical areas, and some significant remnants of that line of thought endure.[18] The home was, and still is, generally entitled to the highest level of protection,[19] while some areas, such as open fields, are entitled to no protection at all.[20] Still others have an intermediate protection, such as the automobile,[21] and the curtilage or area immediately surrounding the home.[22] Significant developments in traditional Fourth Amendment jurisprudence came in the Prohibition-era cases of *Olmstead v. United States*[23] and *Carroll v. United States*.[24] In *Olmstead*, officers used wiretaps to intercept telephone messages, without a warrant, to discover and gather evidence regarding a massive bootlegging operation.[25] The Court found that this kind of wiretapping was not a search under the Fourth Amendment, and emphasized that the Fourth Amendment protects "a man's house, his person, his papers, and his effects" in the physical and material sense only.[26] Since the telephone wires were not part of the defendant's home, the Fourth Amendment could not be extended to protect telephone communications.[27]

Carroll involved technology in a different way – it established the automobile exception to the warrant requirement, based in part on its unique mobility.[28] At the same time, the Court in *Carroll* noted that "The Fourth Amendment is to be construed in the light of what was deemed an unreasonable search and seizure when it was adopted, and in a manner which will conserve

---

[18] *See, e.g.*, Kyllo v. United States. 533 U.S. 27, 31 (2001) (holding that the warrantless use, from outside the home, of an infrared radiation detector to detect the heat of marijuana grow lamps inside the home unconstitutional).
[19] *See* Carroll v. United States, 267 U.S. 132, 162 (1925); *Kyllo*, 533 U.S. at 31.
[20] *See* Oliver v. United States, 466 U.S. 170, 178 (1984) (holding that the open fields doctrine, which dictates that there is no protected Fourth Amendment interest in an open field, was not overruled by *Katz*).
[21] *See Carroll*, 132 U.S. at 162.
[22] *See Oliver*, 466 U.S. at 178.
[23] 277 U.S. 438 (1928).
[24] 267 U.S. 132 (1925).
[25] *Id.* at 456-457.
[26] *Id.* at 464.
[27] *Id.*
[28] Carroll v. United States, 267 U.S. 132, 154 (1925).

public interests as well as the interests and rights of individual citizens."[29] The Court in *Carroll* recognized that when applying Fourth Amendment principles to novel, life-changing technologies such as the automobile, which fundamentally changed the character of everyday life for Americans, the public interest should be considered because the intent of the Framers cannot be determinative when dealing with such novel technology.[30] It also demonstrates the general approach frequently taken by the Court before the formation of the modern test: using historical principles as a general guide without allowing the constraints of history to inhibit adaptation to changes in society.[31]

B. Modern Test: Reasonable Expectation of Privacy

The modern Fourth Amendment test originated in *Katz v. United States*, when the Court held that the use of an eavesdropping and recording device on the exterior of a phone booth was a search within the meaning of the Fourth Amendment.[32] *Katz* marked a fundamental shift in Fourth Amendment jurisprudence.[33] Previously, courts focused on the areas protected by the Fourth Amendment, with a particular emphasis on the home as the epitome of the private sphere.[34] The government argued that since the use of the listening device required no physical intrusion into the phone booth, which may be considered the constitutionally protected area, its

---

[29] *Id.* at 150.
[30] *See, e.g.*, David A. Sklansky, *Back to the Future: Kyllo, Katz, and Common Law*, 72 MISS. L.J. 143, 182 (2002) (discussing the reliance of Justices Scalia on Thomas on the *Carroll* majority opinion.) Sklansky criticizes both Justice Scalia and Justice Thomas for ignoring the portion of the *Carroll* opinion which states that the Fourth Amendment should also protect "public interests as well as the interests and rights of individual citizens." *Id.*
[31] *See id.* at 165. "Before Katz, history was a dominant theme of search-and-seizure jurisprudence generally--but usually history was consulted to shed light on the central concerns of the Fourth Amendment, not to locate its precise commands." *Id.*
[32] Katz v. United States, 389 U.S. 347, 353 (1967).
[33] *See* Mina Ford, *The Whole World Contained: How the Ubiquitous Use of Mobile Phones Undermines Your Right to Be Free from Unreasonable Searches and Seizures*, 39 FLA. ST. U. L. REV. 1077, 1089 (2012).
[34] *Katz*, 389 U.S. at 352-353. *See also id.* at 367 (Black, J., concurring) ("The Fourth Amendment was aimed directly at the abhorred practice of breaking in, ransacking and searching homes and other buildings and seizing people's personal belongings without warrants issued by magistrates.").

use could not be a violation of the Fourth Amendment.[35] The Court responded with the oft-repeated recognition that "the Fourth Amendment protects people, not places."[36]

It was Justice Harlan's concurrence in *Katz*, however, that began to flesh out the conceptual foundation of the new Fourth Amendment test.[37] Harlan's concurrence laid out the reasonable expectation of privacy standard.[38] Under this standard, Fourth Amendment protections will apply when "a person [has] exhibited an actual (subjective) expectation of privacy and, second, [when] the expectation be one that society is prepared to recognize as reasonable."[39] The concurrence contrasted Katz's phone booth with an open field, which the Court had long ago found entitled to no Fourth Amendment protection, noting that there could be no reasonable expectation in privacy in an open field.[40] The "reasonable expectation of privacy" language appeared just one year later in 1967 in *Terry v. Ohio*, another noteworthy Fourth Amendment case which established the legality of a limited weapons search based on a reasonable suspicion of criminal activity.[41]

Katz itself was born out of new technology, although primitive by today's standards. In the late 1970s, the Court again confronted the intersection of a new technology and the Fourth Amendment in *Smith v. Maryland* - this time it was a "pen register," which recorded the numbers dialed from the defendant's telephone.[42] Police installed the pen register at the central office of the telephone company without a warrant, after a woman who had been robbed began receiving

---

[35] *Id.* at 349.
[36] *Id.* at 351.
[37] *See id.* at 360 (Harlan, J., concurring) (discussing Fourth Amendment protections in terms of "reasonable expectation of privacy").
[38] *Id.*
[39] *Katz*, 389 U.S. at 360 (internal quotation omitted).
[40] *Id. See also* Hester v. United States, 265 U.S. 57 (1924).
[41] Terry v. Ohio, 392 U.S 1, 9 (1968).
[42] 442 U.S. 735, 737 (1979).

obscene phone calls.[43] The Court applied the *Katz* reasonable expectation of privacy test, finding that the petitioner had no reasonable expectation of privacy in the numbers dialed from his telephone.[44] The Court noted that pen registers were commonly used in telephone company billing operations and other business purposes along with law enforcement purposes.[45] It also reaffirmed that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," a proposition known as the "third-party doctrine."[46]

In 2011, the Supreme Court considered some of the most advanced and problematic technology yet: Global Positing Systems, which allows law enforcement to pinpoint the location of the device within 50 to 100 feet with minimal cost and effort.[47] In *United States v. Jones*, officers installed a GPS device on a vehicle used by a suspected cocaine distributor and tracked his movements for 28 days.[48] This surveillance generated over 2,000 pages of data on the defendant's whereabouts.[49] Justice Scalia, writing for the majority, analyzed the alleged illegal intrusion not under the *Katz* reasonable expectation of privacy test, but under a property-based theory.[50] In rejecting the government's argument that the GPS device captured only the location of the vehicle on public streets, Justice Scalia focused on the trespass in which the government

---

[43] *Id.*
[44] *Id.* at 742.
[45] *Id.*
[46] *Id.* at 744. The Court also stated that a person who discloses information to a third party assumes the risk that this information will eventually be turned over to the government for law enforcement purposes. *Id.* at 743.
[47] United States v. Jones, 132 S. Ct. 945, 948 (2012). Global Positioning Systems use triangulation between ground-level user devices and 24 orbiting satellites to pinpoint velocity and time as well as location. *See* UNITED STATES AIR FORCE, GLOBAL POSITIONING SYSTEM FACT SHEET (Sepl. 15, 2010), http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104610/global-positioning-system.aspx (last accessed Feb. 26, 2014).
[48] *Jones*, 132 S. Ct. at 948.
[49] *Id.*
[50] *See id.* at 949 ("It is important to be clear about what occurred in this case: The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a "search" within the meaning of the Fourth Amendment when it was adopted.").

engaged by placing the device on the vehicle, and dismissed the *Katz* reasonable expectation of privacy standard as non-exclusive.[51]

Justice Sotomayor's concurrence in *Jones* highlighted the problems with using a trespass framework to analyze technological intrusions on privacy.[52] Justice Sotomayor joined the majority opinion because for her, Justice Scalia's trespass framework constitutes "an irreducible constitutional minimum."[53] The concurrence, however, noted that not all technological surveillance requires trespass – even the same kind of GPS monitoring undertaken in *Jones* could soon be done using smartphones or factory-installed GPS devices, with no physical trespass necessary.[54] The opinion also noted that these helpful but intrusive technologies are fundamentally reshaping societal expectations of privacy.[55] Sotomayor further suggested that perhaps the time has come to abolish the third-party doctrine altogether, because of the great quantity of deeply personal information revealed to third parties through technology on a regular basis.[56]

II. National Security Agency Data Collection Programs

A. Leaks

In June of 2009, The Guardian, a British newspaper, began publishing anonymous reports of bulk data collection programs undertaken by the National Security Agency in the United

---

[51] *See id.* at 952 ("[T]he Katz reasonable-expectation-of-privacy standard has been *added to,* not *substituted for*, the common-law trespassory test." (emphasis in original)).
[52] *See Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring).
[53] *Id.*
[54] *Id.*
[55] *Id.*
[56] *Id.*

States.[57] The newspaper initially revealed that the NSA was collecting phone records from customers of the telecommunications giant Verizon, regardless of any suspicion of wrongdoing or criminal activity.[58] The leaker (or whistleblower) turned out to be Edward Snowden, a contractor who had formerly worked with the National Security Agency.[59] Soon after his identification, Snowden was charged with espionage and is now in Russia, seeking asylum in Europe.[60] Snowden had access to an estimated 1.7 million documents, and months after the revelations it is still unclear which documents he actually downloaded and shared with the media.[61] Snowden clearly has an agenda, as evidenced by his comments in a January 2014 interview:

> Every time you pick up the phone, dial a number, write an e-mail, make a purchase, travel on the bus carrying a cellphone, swipe a card somewhere, you leave a trace and the government has decided that it's a good idea to collect it all, everything, even if you've never been suspected of any crime.[62]

The government eventually acknowledged the existence of the collection programs, although many documents remain classified.[63] The procedure by which the data collection is authorized is as follows: the Federal Bureau of Investigation seeks an order from the Foreign Intelligence Surveillance Court directing, in the case of telephone

---

[57] Scott Neuman, *Newspaper Reveals Source for NSA Surveillance Stories*, THE TWO-WAY, NPR.ORG (June 9, 2013), http://www.npr.org/blogs/thetwo-way/2013/06/09/190121734/newspaper-reveals-source-for-nsa-surveillance-stories.
[58] Greenwald, *supra* note 1.
[59] *Id.*
[60] Eyder Peralta, *Edward Snowden Tells EU Parliament He Wants Asylum in Europe*, NPR.COM (March 7, 2014), http://www.npr.org/blogs/thetwo-way/2014/03/07/287459845/edward-snowden-tells-eu-parliament-he-wants-asylum-in-europe. Snowden was nominated for Nobel Peace Prize in 2014. Bill Chappel, *Edward Snowden Nominated for Nobel Peace Prize* (Jan. 29, 2014), THE TWO-WAY, NPR.COM, http://www.npr.org/blogs/thetwo-way/2014/01/29/268421741/edward-snowden-is-nominated-for-the-nobel-peace-prize.
[61] Walter Pincus, *Critics of Government Surveillance Aren't Backing Off Despite Recent Developments*, FINE PRINT, WASHINGTON POST (February 10, 2014), http://www.washingtonpost.com/world/national-security/critics-of-government-surveillance-arent-backing-off-despite-recent-developments/2014/02/10/04828cf8-8f6b-11e3-b227-12a45d109e03_story.html.
[62] *Id.*
[63] *See* Klayman v. Obama, No. 13–0881, 2013 WL 6598728, *2 & *2 n. 9 (D.D.C. 2013).

data, telecommunications providers to turn over all "telephony metadata" available.[64] In the case of internet metadata, the order is directed at internet communications companies such as Google or Apple.[65]

The legal mechanism that allows for this data collection is also largely secret.[66] The Foreign Intelligence Surveillance Court is an Article III court created in 1978 by the Foreign Intelligence Surveillance Act, which was passed as a response to discoveries that warrantless electronic surveillance was being used (and abused) for national security purposes.[67] After September 11, 2001, the USA PATRIOT Act amended the Foreign Intelligence Surveillance Act to allow the FBI to obtain orders "requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities."[68] The full details of the FISC procedure is outside the scope of this paper, but it is important to note that all petitions, records of proceedings, and orders from the court are to be kept from public view.[69]

B. Telephone metadata

The National Security Agency, beginning in 2006, has conducted a dragnet data collection program in which they collect telephone company records of calls for all land-line and

---

[64] *Id.* at *2.
[65] Spencer Ackerman, *Microsoft, Facebook, Google and Yahoo Release US Surveillance Requests*, THE GUARDIAN (Feb. 3, 2014), http://www.theguardian.com/world/2014/feb/03/microsoft-facebook-google-yahoo-fisa-surveillance-requests.
[66] *See* 50 U.S.C. §§ 1803(c), 1861(f)(4)-(5) (2006 & Supp. 2012).
[67] *See Klayman*, 2013 WL 6598728, *3; 50 U.S.C. §§ 1804(a)(3), 1805(a)(2) (2006 & Supp. 2012). The Foreign Intelligence Surveillance Court acts as the district court of the system, while the Foreign Intelligence Surveillance Court of Review acts as the court of appeals. *See* 50 U.S.C. §§ 1804(a)(2), 1805(a)(2).
[68] 50 U.S.C. 1861(a)(1). 2006 amendments to the act required that the FBI show that "there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation ... to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." *Klayman*, 2013 WL 6598728, at *3 (quoting 50 U.S.C. § 1861(b)(2)).
[69] *See* 50 U.S.C. §§ 1803(c), 1861(f)(4)-(5),

some cellular telephones in the United States.[70] These records reveal the number making the call, the number receiving the call, and the length of the call.[71] The NSA cannot, however, immediately access the data it collects.[72] In order for the NSA to make a query to search for information in its massive collection, it must "[identify] a known telephone number for which, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion that the telephone number is associated with [redacted]."[73] This "reasonable suspicion" language originates from the Court's decision in *Terry v. Ohio*, and is a lesser showing than probable cause.[74] The NSA holds the collected data for five years.[75] The massive domestic telephone metadata program is not the limit of the NSA's technological capacity for data-gathering – in spring of 2014, the Washington Post reported that the NSA has the technological capability to record and store for 30 days all phone traffic (including the content of entire telephone conversations, not just metadata) of an unnamed foreign country.[76]

---

[70] Pincus, *supra* note 61; Ellen Nakashima, *NSA is Collecting Less Than 30 Percent of U.S. Call Data, Officials Say*, THE WASHINGTON POST (Feb. 7, 2014), http://www.washingtonpost.com/world/national-security/nsa-is-collecting-less-than-30-percent-of-us-call-data-officials-say/2014/02/07/234a0e9e-8fad-11e3-b46a-5a3d0d2130da_story.html.
[71] *Id. See also* In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted], Order at 2, Docket No. BR 06-05 (F.I.S.C. May 24, 2006), *available at* http://www.dni.gov/files/documents/section/pub_May%2024%202006%20Order%20from%20FISC.pdf (stating that telephony metadata includes "comprehensive communications routing information, including but not limited to session identifying information (*e.g.*, originating and terminating telephone number, communications device identifier, etc.), trunk identifier, and time and duration of call.").
[72] 2 Law of Electronic Surveillance § 9:68.
[73] *Id.* (quoting *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted]*, Order at 5.).
[74] 392 U.S 1, 9.
[75] *Id.*
[76] Barton Gellman and Ashkan Soltani, *NSA Surveillance Program Reaches 'Into the Past' to Retrieve, Replay Phone Calls*, THE WASHINGTON POST (March 18, 2014), http://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html.

C. Internet metadata

Even more troublesome than the NSA's wholesale telephone record collection program is its internet metadata collection program. Internet metadata is information produced when one does almost anything online, from checking email to visiting a social network.[77] This data contains an astonishing amount of detailed information about how we spend our daily lives and our personal characteristics, including highly private aspects of life.[78] For example, whenever an email is sent, the metadata it generates contains name and email of both the sender and recipient, IP address of the sender, date, time, time zone, the subject of the email, and a unique identifier of each email.[79] When Americans use a search engine, which many of us do multiple times per day, the metadata contains the search query, the search results, and the pages visited as a result of the search.[80] Email and search history alone can reveal an incredible detailed picture of how people spend their day, their health, and their personal problems.[81] One commentator noted that internet metadata is "a way of getting inside your head that's in many ways on par with reading your diary."[82] It is worth noting here that this information was being recorded and used by private companies well before it was revealed that the government was also collecting the information.[83]

---

[77] *The Guardian Guide to your Metadata*, THE GUARDIAN (June 12, 2013), http://www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance#meta=1000000.
[78] *See id.*
[79] *Id.* In 2013, the FBI traced the affair of General David Patreus and Paula Broadwell using metadata from the anonymous email account they shared. *Id.* Instead of sending emails, the two saved drafts to communicate – but the government still had enough information from the metadata to connect the dots between them. *Id.*
[80] *Id.*
[81] ANGWIN, *supra* note 6, at 1-20.
[82] Glen Greenwald and Spencer Ackerman, *NSA Collected US Email Records in Bulk for More Than Two Years under Obama*, THE GUARDIAN (June 27, 2013), *available at* http://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama ("The calls you make can reveal a lot, but now that so much of our lives are mediated by the internet, your IP [internet protocol] logs are really a real-time map of your brain . . ." said Julian Sanchez of the Cato Institute.").
[83] For an excellent explanation of data collection and targeted advertising, *see* Elspeth A. Brotherton, *Big Brother Gets A Makeover: Behavioral Targeting and the Third-Party Doctrine*, 61 EMORY L.J. 555, 560-67 (2012).

An entire industry of companies tracks online consumer data and sells it to marketers to use to target marketing to individual consumers based on their internet browsing history.[84]

Updated news on the scope of data collection is reported frequently.[85] For example, as late as February 2014, leaked documents revealed in addition to its domestic surveillance programs, the NSA helped British intelligence agencies capture images from the video calls of ordinary British citizens, including sexually explicit images.[86] The NSA has also worked on circumventing the data encryption system that protects everything from credit card transactions to medical records, going so far as to work with private companies, some of whom insert a "back door" for the government as they develop encryption techniques.[87] The Obama Administration originally asserted that the main NSA internet metadata program was discontinued in 2011,[88] but it was then reported that the NSA's capacity for collecting internet data had actually increased since then.[89]

III. RECENT CHALLENGES TO NSA BULK DATA COLLECTION PROGRAMS

Challenges to NSA dragnet data collection programs began soon after the NSA programs became public knowledge in 2013.[90] Although these cases are still in the early stages of litigation,[91] the district court decisions currently available demonstrate the approaches courts have taken thus far, and shed light on how the Supreme Court may eventually interpret the issue

---

[84] *See* Katy Bachman, *Confessions of a Data Broker: Acxiom's CEO Scott Howe Explains How Self-regulation Can Wor*k, ADWEEK (March 25, 2014), http://www.adweek.com/news/technology/confessions-data-broker-156437.
[85] *See*, *e.g.*, Mark Memmott, *Latest Leak: U.K. Spied On Webchats, Grabbed Millions Of Images*, THE TWO-WAY, NPR.COM, February 27, 2014, http://www.npr.org/blogs/thetwo-way/2014/02/27/283473563/latest-leak-u-k-spied-on-webchats-grabbed-millions-of-images.
[86] *See id.*
[87] Nicole Perlroth, Jeff Larson and Scott Shane, *N.S.A. Able to Foil Basic Privacy Safeguards on Web*, N.Y. TIMES, Sept. 5, 2013, at A1.
[88] Greenwald & Ackerman, *supra* note 82.
[89] Glen Greenwald and Spencer Ackerman, *How the NSA is Still Harvesting Your Online Data*, THE GUARDIAN, June 27, 2013, *available at* http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection.
[90] *See, e.g.*, Klayman v. Obama, No. 13–0881, 2013 WL 6598728 (D.D.C. 2013).
[91] *See, e.g.*, American Civil Liberties Union v. Clapper, No. 13 Civ. 3994, 2013 WL 6819708 (S.D.N.Y. 2013). The initial substantive opinion in *ACLU v. Clapper* was issued on December 27, 2013. *See id.*

of bulk domestic surveillance through technology.[92] In addition to the formal legal challenges in the works, the executive branch is getting into the reform game as well.[93] In March of 2014, President Obama announced his intention to get rid of the current telephone metadata programs and replace it.[94] The designers of any new surveillance program will have to be mindful of the progress of two recent cases in federal court.[95]

A. *American Civil Liberties Union v. Clapper*

In late 2013, one district court drew on cases involving other types of electronic surveillance when it found that the NSA surveillance programs complied with the Fourth Amendment.[96] In *American Civil Liberties Union v.Clapper*, the ACLU and other organizations[97] sought an injunction prohibiting the government from continuing the data collection and a declaratory judgment that the collection was in violation of the Fourth Amendment, the First Amendment, and the Foreign Intelligence Surveillance Act.[98] In late 2013, the district court judge denied the motion, finding that the collection programs comply with Fourth Amendment and the various applicable statutes. [99] In its Fourth Amendment analysis, the court applied the *Katz* reasonable expectation of privacy test.[100] The challengers attempted to distinguish *Smith*, noting that the defendant in *Smith* was the single target of investigation in that

---

[92] *See id.* at *21.
[93] Stewart Baker, *The New Phone Metadata Program*, THE VOLOKH CONSPIRACY, THE WASHINGTON POST (March 25, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/03/25/the-new-phone, -metadata-program/.
[94] *Id.*
[95] *See generally Clapper*, 2013 WL 6819708; Klayman v. Obama, No. 13–0881, 2013 WL 6598728 (D.D.C. 2013).
[96] *Id.* at *20-21.
[97] Challengers include The American Civil Liberties Foundation, The New York Civil Liberties Union, and the New York Civil Liberties Foundation. *Id.* at *1.
[98] ACLU v. Clapper, No. 13 Civ. 3994, 2013 WL 6819708, at *6 (S.D.N.Y. Dec. 27, 2013).
[99] *Id.* at *1. The order began with a narrative about how metadata collection might have prevented the 9/11 attacks by tracking one of the hijacker's phone calls from San Diego to Yemen. *Id.* at *1.
[100] *Id.* at *20.

case.[101] Since the Court in *Smith* found there is no privacy interest in the telephone numbers themselves, the ALCU argued that the information that can be gleaned from the telephone numbers, such as political association, religion, or personal vices, is entitled to protection.[102] The district court rejected those arguments, endorsing the procedural safeguards employed by the government.[103] It found that the data collection was not transformed into a Fourth Amendment "search" because of its dragnet character.[104]

The court acknowledged that the way people use their phones is much different than the way they used them when *Smith* was decided, but noted that the way calls are placed – by sending information to telecommunications providers – has not changed.[105] Notably, the parties appeared to be proceeding under the assumption that the programs included all landline and cell phone records, although since it has been revealed that the NSA has been unable to keep pace with increased cell phone use and collects only some cell records.[106] Since the telephone metadata challenge still involves the phones' use as phones, not as mobile datebooks, small computers, or any of the myriad things for which we now use our phones, *Smith* controlled,

---

[101] *Id.*
[102] *Id.* at *21.
[103] ACLU v. Clapper, No. 13 Civ. 3994, 2013 WL 6819708, at *21 (S.D.N.Y. Dec. 27, 2013) ("First, without additional legal justification – subject to rigorous minimization procedures – the NSA itself cannot even query the telephony metadata database. Second, when it makes a query, it only learns the telephony metadata within three 'hops' of the 'seed.' Third, without resort to additional techniques, the Government does not know who any of the telephone numbers belong to.").
[104] *Id.* at *22.
[105] *Id.* at *22.
[106] *Id.* at *22; Nakashima, *supra* note 70. The NSA is still trying to keep pace with technological developments and collects more call records, however. *Id.* ("The NSA is preparing to seek court orders to compel wireless companies that currently do not hand over records to the government to do so, said the current and former officials, who spoke on the condition of anonymity to discuss internal deliberations.").

according to the court.[107] The court also explicitly rejected the ACLU's argument based on the *Jones* concurring opinions.[108]

B. *Klayman v. Obama*

The district court for the District of Columbia reached the opposite result in *Klayman v. Obama*, where five individual plaintiffs sought a preliminary injunction barring the government from collecting their phone records or querying the government's data collection using their phone numbers, and asking the government to destroy all information collected about to the plaintiffs thus far.[109] The court granted the preliminary injunction based on the plaintiff's constitutional claims, but stayed the order pending appeal because of "the significant national security interests at stake . . . and the novelty of the constitutional issues . . . ."[110] Interestingly, in *Klayman*, the court stated that violations of the Fourth Amendment occur either when the government commits a physical intrusion, citing *Jones*, or if the government violates the individual's reasonable expectation of privacy, citing *Katz*, although the court dismissed the idea that there was a physical intrusion in the collection of metadata.[111] The court started, predictably, with a citation to *Smith v. Maryland*, but soon made the case that it is no longer useful:

> When do present-day circumstances—the evolutions in the Government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies—become so thoroughly unlike those considered by the Supreme Court thirty-four years ago that a precedent like Smith simply does not apply? The answer, unfortunately for the Government, is now.[112]

The court drew on the part of the *Jones* majority opinion that distinguished the earlier *United States v. Knotts*, by finding that the type of long-term comprehensive surveillance

[107] ACLU v. Clapper, No. 13 Civ. 3994, 2013 WL 6819708, at *21 (S.D.N.Y. Dec. 27, 2013).
[108] *Id.* at *22.
[109] *Id.*
[110] *Id.* at *2.
[111] *Id.* at *17.
[112] *Id.* at *18.

undertaken by the police through GPS monitoring was vastly different from a short-term and short-range "beeper" device.[113] The main differences, according to the court, include (1) the telephone metadata program contains 5 years' worth of information as opposed to just a few days' worth in *Smith*,[114] the program collected data indiscriminately, creating an unofficial joint private-public intelligence program,[115] and (3) the technology used to undertake the program was unimaginable in 1979 when *Smith* was decided.[116] The court further emphasized the ubiquity of cell phones, which is exponentially greater now than in the 1970s or 1980s.[117] In *Klayman*, the Court went on to hold that the plaintiffs showed a substantial likelihood that the challenged programs were unreasonable.[118]

C. *Katz* and the NSA

The early decisions of the District Courts for the Southern District of New York and the District of Columbia act as a preview of how courts will rule on the NSA programs, especially since more information is being revealed continually.[119] Both cases considered only the telephone metadata program,[120] so it worthwhile exploring how the *Katz* test may apply to the internet metadata program.

---

[113] ACLU v. Clapper, No. 13 Civ. 3994, 2013 WL 6819708, at *18 (S.D.N.Y. Dec. 27, 2013).
[114] Klayman v. Obama, No. 13–0881, 2013 WL 6598728, at *19 (D.D.C. 2013).
[115] *Id.* ("It's one thing to say that people expect phone companies to occasionally provide information to law enforcement; it is quite another to suggest that our citizens expect all phone companies to operate what is effectively a joint intelligence-gathering operation with the Government.").
[116] *Id.* at *19.
[117] *Id.*
[118] *Id.*
[119] *See* Memmott, *supra* note 85.
[120] *See* Klayman v. Obama, No. 13–0881, 2013 WL 6598728, at *20 (D.D.C. 2013); ACLU v. Clapper, No. 13 Civ. 3994, 2013 WL 6819708, at *21 (S.D.N.Y. Dec. 27, 2013).

1. *Phone records*

The application of *Smith v. Maryland*, which is based on the *Katz* standard, to the NSA collection of phone records seems fairly straightforward.[121] Today's phone metadata contains mostly the same information as the pen register captured in *Smith*,[122] and the metadata is revealed to the third party of the phone company so that the call can go through, much like it was in the past.[123] There are some key differences in today's phone metadata and the information recorded by *Smith's* pen register – the information is stored indefinitely as opposed to being used for a limited criminal investigation.[124] The other key distinction between *Smith* and the current NSA measures is the nature of the collection. In *Smith*, the pen register was collected from one person who was suspected of committing a crime, although there was still no warrant.[125] The NSA programs are en mass, without suspicion, and also stored for years unlike the limited use the information was put to in *Smith*.[126] Although these factors most directly relate to whether the purported search is reasonable and not whether the information is protected, they are important to consider in an overall factual inquiry.[127] The information that can be gleaned from mass data collection is qualitatively different than individualized data collection because of the connections that can be drawn between the records of different people.[128]

---

[121] *See, e.g.*, *Clapper*, 2013 WL 6819708, at *21.
[122] *See supra* Section II.B.
[123] ACLU v. Clapper, No. 13 Civ. 3994, 2013 WL 6819708, at *21 (S.D.N.Y. Dec. 27, 2013).
[124] *See Klayman*, 2013 WL 6598728, at *20.
[125] *See* Smith v. Maryland, 442 U.S. 735, 737 (1979).
[126] *Id.*
[127] *See* Jim Harper, *Reforming Fourth Amendment Privacy Doctrine*, 57 AM. U. L. REV. 1381, 1398-99 (2008).
[128] See Klayman, 2013 WL 6598728, at *17.

2. *Internet metadata*

The courts in the two cases above considered mainly the NSA telephone data collection programs,[129] but some conclusions can be drawn regarding internet metadata as well. Internet metadata can also be considered to be "voluntarily" revealed to a third party, but it can be incredibly more revealing than phone metadata. Instead of just the numbers dialed and length of the call, internet metadata reveals the interactions we have with the internet and the information that can be accessed by it.[130] Even though the information revealed is exponentially more revealing about us, the basics are the same as with the phone metadata: when writing an email, we enter information that a third party, our communications company, sends to a server to be processed so that we can visit the web page we are seeking to visit.[131]

Unlike our telephone use, our internet use is regularly tracked for the use of private companies, which use the information to target advertisements that often seem to follow us around to different web sites.[132] Web sites track user's web information by the use of a cookie, a small piece of code that is downloaded onto one's browser when one visits a website.[133] This information is used to remember you, as the unique user, when you return to the web site, and used to track your movements throughout the site.[134] It is also regularly shared with data brokers and other outside parties and subsequently sold to marketing companies in order to target advertising to individual consumers.[135]

---

[129] *See generally Clapper*, 20130 WL 6819708; *Klayman*, 2013 WL 6598728.
[130] *See The Guardian Guide to Your Metadata*, *supra* note 77.
[131] *See* ACLU v. Clapper, No. 13 Civ. 3994 , 2013 WL 6819708, at *21 (S.D.N.Y. Dec. 27, 2013).
[132] *See* Joanna Geary, *Tracking the Trackers: What Are Cookies? An Introduction to Web Tracking*, THE GUARDIAN (April 23, 2012), http://www.theguardian.com/technology/2012/apr/23/cookies-and-web-tracking-intro.
[133] *Id.*
[134] *Id.*
[135] *Id.*

This tracking, although it may be more extensive than most people think, is common knowledge, so it would seem that no expectations of privacy on the internet could be reasonable, except perhaps when under special secure types of connections.[136] The disclosure of our Internet history is also voluntary in a strict sense – it is possible to opt out of these tracking devices to various degrees, and it is also possible to avoid behavioral tracking altogether by not using the Internet.[137] *Katz* and the third party doctrine would therefore seem to prevent this information from being protected under the Fourth Amendment.

IV. STARTING OVER: ELIMINATING *KATZ* FOR ELECTRONIC COMMUNICATIONS

The NSA leaks have made clear that the American government is watching and listening closely.[138] Considering the extent to which Americans rely on electronic communications to complete daily tasks and the dragnet nature of the NSA data collection, few expectations of privacy can be reasonable.[139] Since the bell of secret government data collection cannot be unrung, the Fourth Amendment test should shift from one based on subjective expectations of privacy to a factual analysis of the purported search, including the way in which the information may have been disclosed and for what purpose.[140]

---

[136] *See* Perlroth et. al, *supra* note 87.
[137] *See, e.g.,* Jonathan Mayer and Arvind Narayanan, *Do Not Track: Universal Web Tracking Opt Out*, donottrack.us. Google Chrome offers "incognito mode" where the browser does not save information on browsing history; however, it does not affect the tracking of other websites. *Incognito Mode (Browse in Private)*, Google Chrome Help, https://support.google.com/chrome/answer/95464?hl=en.
[138] *See, e.g.*, Adrian Croft, *Obama Says U.S. Needs to Win Back Trust After NSA Spying*, REUTERS.COM (March 25, 2014), http://www.reuters.com/article/2014/03/25/us-usa-security-obama-spying-idUSBREA2O18T20140325.
[139] *See infra* Section IV.A.
[140] *See infra* Section IV.B.

A. Katz No Longer Effectively Protects Privacy Interests Because Few Expectations of Privacy Can Be Reasonable

Katz's continued usefulness is questionable in light of the fundamental societal changes in the last two decades.[141] In 2013, ninety-five percent of Americans under 45 and ninety-one percent of all Americans owned a cell phone;[142] many of those cell phones are smartphones that constantly transmit a vast array of information to third parties.[143] Revealing a great amount of personal information to take part in "mundane tasks" has become part of everyday life for most people.[144] One must go to great lengths and spend a great deal of time and money to avoid being tracked by private companies throughout daily life.[145] As it becomes more difficult to keep private information from private companies, a general sense of hopelessness prevails[146] and societal expectations of privacy become eroded.[147] Although some believe that these technologies actually increase expectations of privacy,[148] others, including Justice Alito, have opined that they result in an "inevitable" diminution in privacy.[149]

---

[141] *See* Jesse Wegman, *Cell Phones and the Expectation of Privacy*, TAKING NOTE: THE EDITORIAL OPINION EDITOR'S BLOG, N.Y. TIMES, Aug. 1, 2013 (last accessed March 18, 2013), http://takingnote.blogs.nytimes.com/2013/08/01/cell-phones-and-the-expectation-of privacy/?_php=true&_type=blogs&_r=0. Wegman argues that the third-party doctrine, as applied to cell phones, "rests on questionable assumptions about the 'voluntariness' with which we provide our personal information to third parties." *Id.*

[142] *Id.*

[143] *See id.*

[144] *See* United States v. Jones, 132 S. Ct. 945, 957 (Sotomayor, J., concurring).

[145] *See If You Think You're Anonymous Online, Think Again*, ALL TECH CONSIDERED, NPR.COM (February 24, 2014), http://www.npr.org/blogs/alltechconsidered/2014/02/24/282061990/if-you-think-youre-anonymous-online-think-again. Julia Angwin, author of the book Dragnet Nation, went on a quest to reduce the amount of data collected about her and in the process purchased a personal wifi device to avoid being tracked in public places that offer free wifi. *Id.* She noted, "privacy has become a luxury good." *Id.*

[146] *Id.*

[147] *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

[148] Klayman v. Obama, No. 13–0881, 2013 WL 6598728, at *19 (D.D.C. 2013).

[149] United States v. Jones, 132 S. Ct. at 162 (Alito, J., concurring).

Scholars were suggesting that the *Katz* test was a failure long before the NSA revelations began.[150] One scholar described the court's Fourth Amendment jurisprudence as "focusing too much on the secrecy of information and failing to account for the fact that in today's Information Age, so little of our data is secret."[151] A 1993 empirical study confirmed that the Supreme Court's conception of reasonable expectations of privacy do not line up with the expectations of the American people.[152] This study predates widespread use of the internet, data tracking, and mobile phones, so it is likely that societal expectations of privacy have changed a great deal since then.[153]

President Obama recently said that "there is a process that is taking place where we have to win back the trust, not just of governments, but more importantly of ordinary citizens, and that is not going to happen overnight."[154] The *Katz* test is circular because it depends on subjective expectations of privacy.[155] If the people's right is continuously violated by, for example, the NSA violating court orders by querying databases without justification,[156] their expectations become less and less reasonable. The NSA leaks, in addition to putting debate about privacy in the forefront, also shook the American people's faith in their government.[157] Americans are already being tracked by private companies almost every minute of the day, but now they know that at least some of this information is being handed over to the government and subsequently

---

[150] Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. Rev. 1511, 1519 (2010).
[151] *Id.* at 1520-21.
[152] Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society,* 42 DUKE L.J. 727, 732 (1993).
[153] Solove, *supra* note 150, at 1524 ("[T]echnology would gradually erode what people expected to be private, and this erosion would allow the government to engage in ever more invasive searches.").
[154] *See* Croft, *supra* note 138.
[155] Harper, *supra* note 127 at 1398-99.
[156] Spencer Ackerman, *Fisa Court Documents Reveal Extent of NSA Disregard for Privacy Restrictions*, THE GUARDIAN (Nov. 19, 2013), http://www.theguardian.com/world/2013/nov/19/fisa-court-documents-nsa-violations-privacy.
[157] *See* Croft, *supra* note 138.

stored for years.[158] The combination of private data tracking and government cooperation with those companies seriously erodes any reasonableness of Americans' expectations of privacy that might have been left.

B. Information Transmitted Through Electronic Communications Should Be Protected

The character of the information collected and stored through phone and internet metadata can be incredibly revealing.[159] Phone metadata can reveal religious and political associations and contact with health providers.[160] More importantly, internet metadata can build an incredibly detailed picture of a person's thoughts and curiosities, health problems, and family situation, among countless other bits and pieces of personal information.[161] Under *Katz* and the third party doctrine, this information is revealed to third parties, so there is no reasonable expectation of privacy, so the information is not protected.[162] This result means that a huge amount of personal information is not protected under the Fourth Amendment, a result which, judging by the public outcry resulting from the revelation of the NSA surveillance programs,[163] is not acceptable to American society.

It is scarcely imaginable that the Framers of the Fourth Amendment could have intended that such a wealth of personal details, regardless of their method of transmission, would be

---

[158] Justice Sotomayor noted the possibility of the government taking this course of action with regard to GPS monitoring data in her Jones concurrence. United States v. Jones, 132 S. Ct. 945, 957 (Sotomayor, J., concurring).
[159] *See The Guardian Guide to Your Metadata*, *supra* note 77.
[160] Alex Hern, *Phone Call Metadata Does Betray Sensitive Details About Your Life – study*, THE GUARDIAN (March 13, 2014) http://www.theguardian.com/technology/2014/mar/13/phone-call-metadata-does-betray-sensitive-details-about-your-life-study. In 2014, researchers at Stanford University successfully identified a marijuana grower, a visitor to an abortion clinic, and someone who suffers from multiple sclerosis from their phone metadata. *Id.*
[161] Glen Greenwald and Spencer Ackerman, *NSA Collected US Email Records in Bulk for More Than Two Years under Obama* (June 27, 2013), *available at* http://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama
[162] *See* ACLU v. Clapper, No. 13 Civ. 3994, 2013 WL 6819708, at *21 (S.D.N.Y. Dec. 27, 2013).
[163] *See, e.g.*, Ann Marie Cox, *Who Should We Fear More with Our Data: The Government or Companies?* THE GUARDIAN (Jan. 20, 2014), http://www.theguardian.com/commentisfree/2014/jan/20/obama-nsa-reform-companies-spying-data.

without protection from government intrusion.[164] Justice Brandeis predicted in his *Olmstead* dissent that "Ways may some day be developed by which the government, without removing papers from 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."[165] That day has come because of the Internet.[166]

Several bases for the protection of electronic communications, particularly on the internet, have been proposed.[167] One scholar has suggested that social network communications should be protected under the umbrella of interpersonal privacy, which has been recognized and granted protection in the Court's substantive due process decisions.[168] Another has suggested that the two forms of privacy protections are intertwined, especially when it comes to technology, because an internet user should have interpersonal privacy freedom of choice when making decisions on what parts of the internet to access, which is partially dependent on the knowledge that their actions are not being followed.[169]

C. A New Approach to the Fourth Amendment: Factual Analysis

If *Katz* is no longer viable as a test that adequately protects rights under the Fourth Amendment,[170] a new test must be fashioned, one that takes into account the massive

---

[164] Many of the details available from phone and internet metadata would have been available only in the home in the past. The home has almost always enjoyed enhanced Fourth Amendment protection. *See supra* Section I.A.
[165] Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).
[166] See Saby Ghoshray, *Privacy Distortion Rationale for Reinterpreting the Third-Party Doctrine of the Fourth Amendment*, 13 FLA. COASTAL L. REV. 33, 34 (2011).
[167] *See* Monu Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply*, 54 B.C. L. REV. 1, 42 (2013).
[168] *Id.* ("The two aforementioned notions of privacy--interpersonal privacy under due process and First Amendment principles and privacy under the Fourth Amendment-- seek to protect two different interests. The former protects interpersonal autonomy whereas the latter focuses on a reasonable expectation of privacy. Both can still be seen as protecting against intrusions by the government.").
[169] Brotherton, *supra* note 83, at 584.
[170] *See infra* IV.A-B.

technological changes of the past few decades. One commentator has suggested that the reasonable expectation of privacy test should be replaced with a test that protects information when the government collection of that information would present "problems of reasonable significance," whether people expect the information to be private or not.[171] These problems of reasonable significance include burdens on free speech, free association, lack of accountability, or lack of police discretion.[172] The basic premise of this approach is practical, but there should be some relationship to the reality of how information is shared. If the test calls for the government being prohibited from collecting truly public information, the test would be unworkable.

Another scholar has suggested that, in lieu of the *Katz* reasonable expectations test, the Court instead endorse a fact-intensive inquiry of whether the information gained by the government was actually private as a matter of fact and law combined, as the Court actually did in *Katz* when it considered the character of the telephone booth conversation.[173] The author gives the example of a pill in a man's coat pocket, which will remain hidden unless someone commits a battery.[174] This approach is useful and can simplify the confusing law in the area, even if it does require a more fact-intensive inquiry than the *Katz* test.[175] In order for this test to offer meaningful Fourth Amendment protection, the third party doctrine must be abolished and digital privacy laws must be strengthened.

To make the factual approach workable in the context of electronic communications, another question must be asked in order to protect data: If the information was not in fact private, to whom was the information transmitted and for what purpose? A distinction should be drawn between information purposely, as opposed to voluntarily, disclosed to third parties and

---

[171] Solove, *supra* note 150 at 1528.
[172] Solove, *supra* note 150 at 1528.
[173] Harper, *supra* note 127, at 1398-99.
[174] *Id.*
[175] *See id.* at 1399-1400.

information voluntarily disclosed to third parties for a limited purpose, namely transmitting the information or another purely administrative purpose. One scholar suggested that courts should recognize a concept of "shared privacy," in which they recognize that some information is neither strictly private nor public, but held by third parties who are expected to keep the information.[176] If courts consider this concept as one component of a factual approach, particularly when looking at electronic communications, the people would enjoy greater protection of electronic communications that are held by technology companies.

As suggested by Justice Sotomayor in her concurrence in *Jones*, the third-party doctrine should be abolished, at very least where technological devices are concerned.[177] Privacy is not equal to secrecy today.[178] One scholar noted that with the advent of cloud computing, in which users store data on remote servers managed by a third party, basically all files have been sent to a third party voluntarily.[179] The Court presented dual rationales for the third-party doctrine in *Smith*, both that the numbers are voluntarily revealed to the phone company and that the content of the communication was not revealed with the use of the pen register.[180] The distinction between content and non-content information breaks down in the context of internet metadata, when the pages visited can reveal a great deal of content, not just logistical information.[181] Further, many courts applying the test consider only what information is revealed, not how the information is used, which runs contrary to the suggested part of the factual inquiry above.[182] The revelation of the metadata that occurs when an email is sent is very different from the

---

[176] Brandon T. Crowther, *(Un)reasonable Expectation of Digital Privacy*, 2012 B.Y.U. L. REV. 343, 367 (2012).
[177] United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.")
[178] *Id.* ("But whatever the societal expectations, [web activity] can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy.").
[179] Khizar A. Sheikh, *I Always Feel Like Somebody's Watching Me*, 280 N.J. LAW 11, 14 (2013).
[180] Solove, *supra* note 150, at 5132.
[181] *See infra* Section II.B.
[182] *See* ACLU v. Clapper, No. 13 Civ. 3994, 2013 WL 6819708, at *20 (S.D.N.Y. Dec. 27, 2013).

revelation of information that occurs when someone publishes something on a social networking site, and should be treated differently for Fourth Amendment purposes.[183]

The other question raised by the continued use of the third-party doctrine is what constitutes a voluntary disclosure when data tracking is as pervasive as it is. In one recent example, a reporter spent two years trying to keep as much of her personal data from others as she could and still take advantage of modern conveniences.[184] Even though she went to great lengths and incurred many inconveniences on this endeavor, the author estimated that she blocked about 50 percent of the data available about her.[185] The third party doctrine eviscerates the Fourth Amendment when applied to electronic communications because in order to keep personal communications protected, one must opt out of taking advantage of modern conveniences.

In the context of *Katz*, much of the data revealed to third parties by phone and internet use is shared and used – mostly not by the government but by private parties looking to target marketing to the tastes of the individual consumer.[186]

Because of the problems with less-than-voluntary data revelations, stronger privacy laws regarding electronic communications will be necessary for the factual inquiry to effectively protect privacy interests.[187] The pushback from dragnet data collection has already begun, so it is not outlandish to think that these strengthened privacy laws are on the horizon.[188] For example, the Federal Trade Commission has proposed a national Do Not Track list to allow Internet users

---

[183] *The Guardian Guide to your Metadata*, *supra* note 77; Peter Eckersly, *How Online Tracking Companies Know Most of What You Do Online (and What Social Networks Are Doing to Help Them)*, ELECTRONIC FRONTIER FOUNDATION (September 21, 2009), https://www.eff.org/deeplinks/2009/09/online-trackers-and-social-networks.
[184] *See* ANGWIN, *supra* note 6, at 112-166.
[185] *See If You Think You're Anonymous Online, Think Again*, *supra* note 145.
[186] *See* Bachman, *supra* note 84.
[187] *See infra* Section IV.A-B.
[188] *See* American Civil Liberties Union, *Modernizing the Electronic Communications Privacy Act*, (last visited Apr. 21, 2014) https://www.aclu.org/technology-and-liberty/modernizing-electronic-communications-privacy-act-ecpa.

to opt out of data tracking,[189] and a non-governmental group has established a Do Not Track code that some companies have pledged to honor.[190] These laws will help ensure that data subject to "shared privacy" remains free from disclosure to the public at large.

1. *Phone Metadata*

When it comes to the mass data collection undertaken by the NSA, the factual approach would help protect some of the information collected. Phone records are generally accessible to three parties: the caller, the receiver of the call, and the phone company.[191] The phone company has the information in order to connect the call and bill the customer for his or her usage.[192] Otherwise, the information is kept private and is not generally accessible to the public.[193] Since the purpose for which the phone company has the information is limited and the disclosure is ordinarily limited to the phone company and not to other parties, this information should be protected as subject to share privacy.[194] This approach would, of course, require reversal of *Smith* and the third party doctrine as well as *Katz*. It would restore a more basic measure of privacy considering the ubiquity of cell phones and other electronic communications devices in today's society.[195]

2. *Internet Metadata*

When it comes to internet metadata, the application of the factual inquiry becomes slightly more complex. Internet metadata is accessible to the internet service provider, but other

---

[189] Brotherton, *supra* note 83, at 568.
[190] *See generally* Jonathan Mayer and Arvind Narayanan, *Do Not Track: Universal Web Tracking Opt Out*, donottrack.us.
[191] *See supra* Section II.C.
[192] *See supra* Subsection on IV.C.1.
[193] Harper, *supra* note 127, at 1398-99.
[194] *See supra* Section IV.B.
[195] *See supra* Section II.B.

information is easily collected through the use of cookies.[196] The information gathered can then be collected and sold to a third party.[197] The collected information, however, is not then accessible to the general public, but made available for sale as a package, aggregated with the data of many other individuals.[198] Because of all this tracking, it is hard to say that internet metadata is actually private under a factual inquiry, but it is also hard to say that it is entirely public. People cannot just go get the data that has been aggregated on themselves, or another person: the companies hold the information closely, and much of it is not personally identifiable without piecing together the information.[199] The question of the actual privacy of internet tracking is still in flux, especially because of the rapid changes in technology.[200] The data would likely fit into the "shared privacy" concept in which a third party holds the information but generally cannot disseminate it to the general public.[201] A strengthening of internet privacy laws would greater ensure that the third parties can only share the information within certain bounds and help ensure that the information does not become generally available to the public. Either way, the actual privacy of internet activity is still a better yardstick than the expectations of privacy, which have been thrown into a tailspin by the NSA revelations.

---

[196] *See infra* Section II.C.
[197] *See* Joanna Geary, *supra* note 132; Bachman, *supra* note 84.
[198] *See id.* Acxiom, one of the leading data broker companies, has a new program that allows people to request their own data. *See generally* AbouttheData.com. However, if the website cannot immediately identify the person requesting the data, the program requires that the person requesting their data send a copy or photo of their government issued identification or recent utility bill to prove identity.
[199] *See* Geary, *supra* note 197; ANGWIN, *supra* note 6, at 1-20. (2014).
[200] Elizabeth Dwoskin, *Web Giants Threaten to End Cookie Tracking*, THE WALL STREET JOURNAL (Oct. 28, 2013), http://online.wsj.com/news/articles/SB10001424052702304682504579157780178992984. Since Microsoft, Google, and Apple all control web browsers *and* mobile devices, they are considering doing their own tracking to aggregate information across all platforms in order to charge other companies for it. *Id.*
[201] *See* Crowther, *supra* note 176, at 367.

CONCLUSION

Using a factual inquiry is of course only a start to reinvigorating the Fourth Amendment in the technological age. Legislation has been introduced to regulate the manner in which private data brokers use consumer information,[202] which could potentially enhance the actual privacy of information over the phone and internet, which in turn would enhance Fourth Amendment protections. Eliminating the subjection, expectation-based *Katz* test and the third-party doctrine could be a beginning to protecting electronic communications.

[202] Electronic Privacy Information Center, *Senators Rockefeller and Markey Propose Data Broker Legislation*, EPIC.ORG (Feb. 13, 2014), http://epic.org/2014/02/senators-rockefeller-and-marke.html ("Under the DATA Act, consumers would be able to access their personal information, make corrections, and opt out of marketing schemes. The DATA Act would empower the FTC to impose civil penalties on violators, and would prohibit data brokers from collecting consumer data in deceptive ways.").