Journal of Criminal Law and Criminology

Volume 103 | Issue 3 Article 9

Summer 2013

Adventures on the Autobahn and Infobahn: United States v. Jones, Mandatory Data Retention, and a More Reasonable "Reasonable Expectation of Privacy"

John A. Stratford

0091-4169/13/10303-0985
THE JOURNAL OF CRIMINAL LAW & CRIMINOLOGY Vol. 103, No. 3

ADVENTURES ON THE AUTOBAHN AND INFOBAHN: *UNITED STATES V. JONES*, MANDATORY DATA RETENTION, AND A MORE REASONABLE "REASONABLE EXPECTATION OF PRIVACY"

John A. Stratford*

I. INTRODUCTION

On July 28, 2011, the House Judiciary Committee voted nineteen to ten in favor of passing H.R. 1981, also known as the Protecting Children from Internet Pornographers Act of 2011.[1] Among other provisions aimed at stamping out child pornography on the Internet, one particular section of the bill stirred up a maelstrom of controversy among privacy and civil liberties advocates. The provision required every Internet service provider (ISP) to retain, for a period of at least eighteen months, certain information about every user of its service in order to allow law enforcement to access records of suspected child pornographers.[2]

Many of the same privacy advocates eagerly awaited last year's decision in *United States v. Jones*.[3] In *Jones*, the Supreme Court considered whether extended warrantless GPS tracking of a vehicle by law enforcement violates the Fourth Amendment.[4]

These two hot-button issues both present concerns about privacy and

* J.D., Northwestern University School of Law, 2013; B.A., University of California, Santa Barbara, 2005. The author thanks Jessica Notebaert, the JCLC editorial staff, and Professor Martha Kanter for invaluable insight and support.

[1] Protecting Children from Internet Pornographers Act of 2011, H.R. 1981, 112th Cong. § 4; H.R. REP. NO. 112–281, pt. 1, at 22–29 (2011); *see also* Rainey Reitman, *House Committee Approves Bill Mandating that Internet Companies Spy on Their Users*, ELECTRONIC FRONTIER FOUND. (July 28, 2011), https://www.eff.org/deeplinks/2011/07/house-committee-approves-bill-mandating-internet. As of this writing, the bill remains in the House of Representatives, scheduled on the Union Calendar.

[2] H.R. 1981; *see also Bipartisan Furor over Data Retention Bill Mars House Judiciary Markup*, WASH. INTERNET DAILY (July 28, 2011), *available at* 2011 WLNR 15187895; Greg Nojeim, *Data Retention Hearing: Opposition from Both Sides*, CTR. FOR DEMOCRACY & TECH. (July 13, 2011), http://www.cdt.org/blogs/greg-nojeim/137data-retention-hearing-opposition-both-sides.

[3] United States v. Jones, 132 S. Ct. 945 (2012).

[4] *Id.*

how courts should regulate interactions between individuals and the government. In this Comment, I argue that these two controversies—one involving surveillance of Internet users on the infobahn and one involving surveillance of drivers on the autobahn—represent and illustrate the same underlying problem with current Fourth Amendment jurisprudence: the "assumption of risk" doctrine first articulated in *Katz v. United States*.[5] I further contend that this doctrine is misguided and has become untenable in modern society. Under a modified *Katz* test, setting aside the assumption of risk doctrine, citizens have a reasonable expectation of privacy both in user data retained by ISPs and in the totality of the movements of their vehicles. The modified *Katz* test proposed here renders both of these regimes presumptively unconstitutional. Such a modified test would at the very least begin the process of bringing the Court's Fourth Amendment jurisprudence back in line with the fundamental principles behind that Amendment.

Part I briefly outlines the history of and controversy surrounding both mandatory data retention and warrantless GPS tracking in the context of the Court's Fourth Amendment jurisprudence. Part II articulates how these two controversies can be understood as symptoms of the same problem: the assumption of risk doctrine. It then explains why the current state of Fourth Amendment jurisprudence does not provide adequate safeguards for individual privacy and presents the normative reasons supporting a change in the doctrine. Finally, Part III offers a modified "reasonable expectation of privacy" framework that excludes the assumption of risk doctrine. This Part concludes that both mandatory data retention and warrantless GPS tracking raise grave constitutional concerns under such a test. It then addresses concerns about potential future applications of *Katz* under this test.

II. BACKGROUND

A. THE FOURTH AMENDMENT AND *KATZ V. UNITED STATES*

The Fourth Amendment provides a short and rather vague statement that acts as almost the sole regulation of conduct between individual citizens and law enforcement officers. It provides:

> 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

[5] 389 U.S. 347 (1967).

seized.[6]

As one commentator notes, "An elaborate regulatory system rests upon this one sentence."[7] The Fourth Amendment regulates a myriad of state–citizen interactions, from more traditional traffic stops, search and frisks, and arrests, to high-tech investigatory actions like wiretaps, Internet surveillance, and GPS vehicle tracking.

A recurring question of interpretation in this regulatory system is what constitutes a "search" or "seizure" for purposes of the Amendment. If a government action against an individual is not a search or seizure, then the Fourth Amendment inquiry ends and there is no further question of whether the action was reasonable or whether a warrant was required under the Amendment.[8] Early Supreme Court decisions focused on whether or not the government was interfering with property interests when deciding what constituted a search.[9] The meaning of a search soon came to be limited to physical intrusions, a doctrine that culminated in the Court's *Olmstead* decision in 1928.[10] In that case, the Court held that law enforcement tapping an individual's telephone was not a search because it did not involve a physical intrusion into the home.[11] This decision was immediately criticized for cutting against the normative principles behind the Fourth Amendment.[12] Was tapping a phone really so unlike invading

---

[6] U.S. CONST. amend. IV.

[7] Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1516 (2010).

[8] The Supreme Court "has created a presumption that a warrant is required, unless infeasible, for a search to be reasonable." United States v. Garcia, 474 F.3d 994, 996 (7th Cir. 2007) (citing cases). But, as Solove points out, "[d]espite the Court's pronouncement in *Katz* in 1967 that there are only 'a few specifically established and well-delineated exceptions' to the warrant requirement, in the decades following *Katz*, the Court has made numerous exceptions." Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy Protection*, 75 S. CAL. L. REV. 1083, 1119 (2002).

[9] *See, e.g.*, Boyd v. United States, 116 U.S. 616, 630 (1886) ("It is not the breaking of [a man's] doors and the rummaging of his drawers that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty, and private property.").

[10] Olmstead v. United States, 277 U.S. 438, 466 (1928).

[11] *Id.* at 466.

[12] Indeed, Justice Brandeis offered an eloquent dissent in *Olmstead*, which now looks prophetic considering *Katz*'s refocusing of the Fourth Amendment on privacy concerns:

> The protection guaranteed by the Amendments [the Fourth and Fifth] is much broader in scope [than the protection of property]. The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men. To protect that right, every unjustifiable intrusion by the Government

physical property? Could the government simply wait until technology afforded them the means to monitor citizens wholesale while the Fourth Amendment stood idly by?

Nevertheless, the Court limited Fourth Amendment "searches" to physical intrusions until its landmark *Katz* decision in 1967.[13] In *Katz*, the FBI attached a listening device to a phone booth in which the defendant was having a conversation about illegal gambling.[14] They recorded the conversation, having obtained no warrant to do so, and then used the recording against him in court.[15] Katz argued that his Fourth Amendment right against unreasonable searches was violated, and the Court agreed.[16] Rejecting their previous doctrine of physical intrusion, the Court stated, "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."[17] The test for exactly what was "constitutionally protected" is now considered embodied in Justice Harlan's oft-quoted concurrence in the case: "My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[18]

As the doctrine now stands, then, a search for the purposes of the Fourth Amendment is a government action that infringes a person's "reasonable expectation of privacy."[19] The test has both subjective (an individual's actual expectation of privacy) and objective (whether society

---

upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment.

Id. at 478–79 (Brandeis, J., dissenting).

[13] Katz v. United States, 389 U.S. 347 (1967).

[14] *Id.* at 348.

[15] *Id.*

[16] *Id.* at 359.

[17] *Id*. at 351.

[18] *Id.* at 361 (Harlan, J., concurring).

[19] This Comment assumes that *Katz* correctly held that privacy protection is the appropriate and intended purpose of the Fourth Amendment's prohibition on unreasonable searches and seizures. It is outside this Comment's scope to discuss other potential justifications, but some commentators argue that privacy should not be the Fourth Amendment's controlling interest. *See, e.g.*, William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure*, 93 MICH. L. REV. 1016 (1995) (advocating for less focus on privacy and more focus on police violence in criminal procedure); Scott E. Sundby, *"Everyman"'s Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751 (1994) (arguing that the Court's focus on privacy has actually restricted individual rights).

deems that expectation reasonable) components.[20] Crucially relevant to this Comment, however, is what may be seen as *Katz*'s exception to the general "reasonable expectation of privacy" test: "What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[21] In the following sections, I show how this part of *Katz*'s holding and its rigid interpretation by the Court has birthed a series of controversial rules surrounding searches and privacy, using mandatory data retention and warrantless GPS tracking as current examples.

B. MANDATORY DATA RETENTION AND THE THIRD-PARTY DOCTRINE

Times have changed since *Katz* was decided in 1967—it is no secret that we now live in an age where Internet use has become ubiquitous and is arguably a necessity for navigating life in modern society.[22] And while the Internet offers unprecedented opportunities for communication, education, business, and entertainment, it is also the greatest aggregator of personal information in human history.[23] As users navigate the Internet, they leave behind a massive trail of data, including e-mail communication, instant messaging, website browsing data, commercial transaction records, and even information about software, hardware, and geographic location.[24]

It is unsurprising that third parties are increasingly eager to access this virtual treasure trove of personal information. Search engines like Google use it to sell tailored advertising;[25] marketing firms use it to analyze trends in commerce;[26] and, relevant to this Comment, law enforcement uses it to track down criminal suspects.

In the United States today, most ISPs retain some data about each of their users for a limited period of time.[27] This data might include browsing

---

[20] Although the Court has generally considered whether a "reasonable person" would have the subjective expectation of privacy, it is worth noting here that the reasonable person presupposes an *innocent* person. For instance, the Court held in *Rakas v. Illinois* that the Fourth Amendment would not protect a burglar's subjective expectation of privacy in a summer cabin he is attempting to rob. 439 U.S. 128, 143–44 n.12 (1978).

[21] *Katz*, 389 U.S. at 351.

[22] According to one source, there were over two billion Internet users worldwide as of 2011 and over 78% of North Americans were Internet users. INTERNET WORLD STATS, http://www.internetworldstats.com (last visited May 20, 2013).

[23] *See* Solove, *supra* note 8, at 1093; Gavin Skok, *Establishing a Legitimate Expectation of Privacy in Clickstream Data*, 6 MICH. TELECOMM. & TECH. L. REV. 61, 62–70 (2000).

[24] *See* Skok, *supra* note 23, at 64–65.

[25] *See Privacy Policy for Google Ads and Advertising Services*, GOOGLE, http://www.google.com/privacy/ads/privacy-policy.html (last updated July 27, 2012).

[26] *See* Steve Lohr, *The Age of Big Data*, N.Y. TIMES, Feb. 11, 2012, at SR1.

[27] *See Is It Legal?: Internet*, NEWSLETTER ON INTELLECTUAL FREEDOM, Mar. 1, 2011, at 83.

history, records of e-mail communication, and Internet protocol (IP) addresses.[28] After a time, this information is often deleted.[29] Under current data preservation laws, however, law enforcement officials may require ISPs to retain certain data about specific customers suspected of crimes to assist investigations.[30] The government can force ISPs to retain this data for up to 180 days as part of its investigation.[31]

H.R. 1981, introduced by Representative Lamar Smith of Texas, would impose a much more severe regime of "mandatory data retention."[32] Under a mandatory data retention program, ISPs (or other telecommunications providers) are required to retain data about *every* user for a specified period of time. In the case of H.R. 1981, ISPs would have to retain temporarily assigned network addresses of all users for at least one year.[33] Temporarily assigned network addresses are records of IP addresses that the ISP assigns to customers.[34] In combination with other "clickstream" data—like browsing history, commercial transaction records, and communications—these IP addresses would allow law enforcement to effectively identify customers and match them up with a comprehensive record of online activity.[35]

The bill was supported by the Department of Justice and the International Association of Chiefs of Police.[36] It was met with loud opposition from privacy advocates in the media and within the House of Representatives. The Center for Democracy & Technology, for example, "urge[d] Congress to fully investigate questions about child pornography

---

[28] An IP address is a unique number that identifies computers on the Internet. *IP Address*, MERRIAM-WEBSTER.COM, http://www.merriam-webster.com/dictionary//ip%20 address (last visited May 20, 2013).

[29] *See Is It Legal?: Internet*, *supra* note 27.

[30] *See, e.g.*, *Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes: Hearing Before the Subcomm. on Crime, Terrorism, & Homeland Sec. of the H. Comm. on the Judiciary*, 112th Cong. 23–33 (2011) [hereinafter *Data Retention Hearing*] (testimony of Kate Dean, Executive Director, United States Internet Service Provider Association); Kristina Ringland, *The European Union's Data Retention Directive and the United States's Data Preservation Laws: Finding the Better Model*, 5 SHIDLER J.L. COM. & TECH. 13 (2009), *available at* http://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/427/vol5_no3_art13.pdf?sequence=1.

[31] *Data Retention Hearing*, *supra* note 30, at 24 (testimony of Kate Dean).

[32] H.R. 1981, 112th Cong. § 4 (2011).

[33] *Id.*

[34] For an explanation of how data retention works with respect to IP addresses and temporarily assigned network addresses, see *Mandatory Data Retention*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/issues/mandatory-data-retention (last visited May 20, 2013).

[35] *Id.*

[36] *See Is It Legal?: Internet*, *supra* note 27, at 83.

investigations before it consider[ed] imposing burdensome and costly mandates on American industry that, in turn, harm the civil liberties of American citizens."[37] Failed data-retention bills introduced in the past have met similar opposition.[38]

Europe implemented a mandatory data-retention directive in 2006,[39] also in the face of great controversy,[40] and other countries have likewise faced opposition in introducing data-retention laws.[41]

While many opponents of mandatory data retention cite concerns of cost and practicality,[42] privacy advocates are particularly worried that H.R. 1981 will be an irresistible temptation to law enforcement officials who would have access to a vast amount of customer information without the need for a search warrant. As of this writing, the Bill is still on the House of Representatives' Union Calendar.[43]

The data-retention discussion above begs the question: why wouldn't law enforcement officials need a warrant to access this type of online user data? It might follow from a commonsense interpretation of a "reasonable expectation of privacy" that data about Internet usage would be exactly the kind of information that the *Katz* Court, in its rejection of physical limitations on searches, wanted to protect from the prying eyes of the government. But the issue that floats just beneath the surface of the mandatory data-retention controversy is *Katz*'s holding that information "knowingly expose[d]" to public view is not subject to Fourth Amendment protection. In the context of customer data retained by ISPs, the

---

[37] *Data Retention Hearing*, *supra* note 30, at 34–45 (testimony of John Morris, General Counsel, Center for Democracy and Technology).

[38] *See* Leslie Harris, *Internet Safety Act Would Make Us Less Safe*, ABC NEWS (Mar. 12, 2009), http://abcnews.go.com/Technology/AheadoftheCurve/story?id=7060343&page=1#.UVWl5RyPMs5 (criticizing the Internet Safety Act of 2009, a similar data-retention bill).

[39] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006, 2006 O.J. (L 105) 54–56, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF.

[40] *See, e.g.*, *"Monumentous Battle" Said Raging over Telecom Data Storage*, COMM. DAILY, Nov. 4, 2005; Warwick Ashford, *EEF Calls for ISP Data Retention Law to Be Scrapped*, COMPUTER WKLY. (Oct. 26, 2010, 4:58 PM), http://www.computerweekly.com/news/1280094182/EEF-calls-for-ISP-data-retention-law-to-be-scrapped.

[41] *See, e.g.*, John Fotiadis, *Cyber Crime: Big Brother Is Watching*, BANGKOK POST (Aug. 15, 2008), http://www.tilleke.com/sites/default/files/cyber_crime.pdf (detailing new mandatory data-retention laws in Thailand); Sean Parnell, *Canberra Rethinks Retention Regime on ISP Subscriber Records*, AUSTRALIAN (July 26, 2011), http://www.theaustralian.com.au/news/foi/canberra-rethinks-retention-regime-on-isp-subscriber-records/story-fn8r0e18-1226101609674 (discussing plans for an Australian data-retention regime).

[42] *See, e.g.*, *Data Retention Hearing*, *supra* note 30, at 23–33 (testimony of Kate Dean).

[43] Protecting Children from Internet Pornographers Act of 2011, H.R. 1981, 112th Cong. § 4.

government is allowed access via the third-party doctrine.

The third-party doctrine essentially holds that the Fourth Amendment does not protect from government intrusion any information that an individual willingly offers to a third party.[44]

The doctrine finds its roots in pre-*Katz* cases dealing with government informants. In *Hoffa v. United States*, for example, the Court held that the defendant had no expectation of privacy in conversations with an associate who later turned out to be a government informant.[45] In a precursor to later cases dealing with the assumption of risk doctrine, the Court reasoned that the Fourth Amendment afforded no protection to "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."[46]

After *Katz*, the third-party doctrine was solidified in *United States v. White*.[47] In *White*, the government relied on testimony from law enforcement agents who used a radio transmitter to listen in on conversations between the defendant and a government informant.[48] White argued that the government violated his Fourth Amendment rights and his expectation of privacy in the conversation with the informant. Relying in part on the pre-*Katz* cases involving government informants discussed above,[49] the Court held that White had no reasonable expectation of privacy in the conversation:

> Inescapably, one contemplating illegal activities must realize and risk that his companions may be reporting to the police. If he sufficiently doubts their trustworthiness, the association will very probably end or never materialize. But if he has no doubts, or allays them, or risks what doubt he has, the risk is his.[50]

In essence, anything told to another, no matter what the subjective expectation of privacy in that information, is not private enough to meet the *Katz* "reasonable expectation of privacy" test.

Five years after *White*, the Court significantly expanded the third-party doctrine in *United States v. Miller*, a case more closely analogous to the

---

[44] Many scholars discuss the evolution and meaning of the third-party doctrine in detail that is beyond the scope of this Comment. *See, e.g.*, Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 596–600 (2011).

[45] Hoffa v. United States, 385 U.S. 293, 302–03 (1966).

[46] *Id.*; *see also* Lewis v. United States, 385 U.S. 206, 211 (1966) (holding that the Fourth Amendment was not implicated by sending an undercover agent to the defendant's house to make a purchase of narcotics from the defendant); Lopez v. United States, 373 U.S. 427, 437–39 (1963) (holding that the Fourth Amendment was not implicated by an undercover agent using a recording device to record a conversation with the defendant).

[47] United States v. White, 401 U.S. 745 (1971).

[48] *Id.* at 746–47.

[49] *Id.* at 749 (citing cases).

[50] *Id.* at 752.

issue of data retention by ISPs.[51] Faced with a society of individuals who increasingly exposed more and more of their information to third parties via new technology, and not just in personal conversations, the Court stuck with the logic of the third-party doctrine. *Miller* involved the retention of customer bank records and whether or not it was a Fourth Amendment search for the government to access them. Relying on *White* to reject Miller's claim of Fourth Amendment protection of the records, the Court held, "The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[52] Reaching back to the government-informer cases, the Court further declared:

> [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[53]

Three years after *Miller*, the Court in *Smith v. Maryland* considered the third-party doctrine in the context of a pen register device used by a telephone company to record phone numbers dialed by the defendant.[54] In this third landmark case, the Court held that the defendant had no reasonable expectation of privacy in the phone numbers he dialed: "When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed."[55]

The Court has kept the third-party doctrine alive in the face of advancing technology and a society that increasingly exposes more and more individual information to third parties. In *White*, the protected information was disclosed via word of mouth; in *Miller*, via written records; and in *Smith*, via numbers dialed on a home telephone.[56] What about information disclosed via the Internet? The answer is that although there is

---

[51] United States v. Miller, 425 U.S. 435 (1976).

[52] *Id.* at 443.

[53] *Id.* (citing *White*, 401 U.S. at 751–52). There was already a suggestion of some limitation on the third-party doctrine here, however: the Court also noted that "the checks [were] not confidential communications but negotiable instruments to be used in commercial transactions." *Id.* at 442.

[54] Smith v. Maryland, 442 U.S. 735, 736 (1979).

[55] *Id.* at 744.

[56] *See also* Florida v. Riley, 488 U.S. 445, 449–52 (1989) (holding no reasonable expectation of privacy in a greenhouse with a missing window where a government plane flew above it and discovered marijuana plants inside); California v. Greenwood, 486 U.S. 35, 39–43 (1988) (holding no reasonable expectation of privacy in garbage bags placed on the defendant's curb).

a somewhat complex scheme of statutory protections in place for data transmitted online,[57] law enforcement is still able to access a vast amount of data held by ISPs without the need for a warrant.[58] The controversy over mandatory data retention is simply over which information ISPs must hold and for how long.

C. WARRANTLESS GPS TRACKING

United States v. Jones represents one new frontier in a long-standing battle over the constitutionality of electronic surveillance.[59] In *Jones*, the defendants were suspected of possession and distribution of cocaine. Government agents planted a GPS[60] tracking device on Jones's vehicle and tracked the location of the vehicle every ten seconds for a month.[61] They did so without a warrant.[62] Using location data from the GPS along with cell phone records, the government at trial was able to paint a comprehensive and incriminating picture of Jones's activity. The issue before the Supreme Court was whether this extended warrantless monitoring by GPS was a violation of Jones's Fourth Amendment rights.

The Government argued that under the Court's decision in *United States v. Knotts*, the use of the GPS tracking device was not a "search" for Fourth Amendment purposes because Jones had no reasonable expectation of privacy in the public movements of his vehicle.[63]

In *Knotts*, law enforcement agents in Minnesota attached an electronic "beeper" tracking device to a drum of chloroform that they suspected was going to be used by the defendant for manufacturing illegal drugs.[64] Once the drum was placed in a vehicle, agents used the device to track the vehicle's movements to a cabin, which they then obtained a warrant to

---

[57] For a thorough analysis of the statutory regime of protections regulating government access to third-party records, see Solove, *supra* note 8, at 1138–51. Although there are statutes regulating areas like wiretapping, access to stored communications, financial records, and medical records, Solove concludes that it is inadequate to "fill the void created by the judicial evisceration of the Fourth Amendment." *Id.* at 1150.

[58] *Id.*; *see also* Catherine Crump, *Data Retention: Privacy, Anonymity, and Accountability Online*, 56 STAN. L. REV. 191, 196 (2003).

[59] United States v. Jones, 132 S. Ct. 945 (2012).

[60] The Global Positioning System is a network of U.S.-owned satellites used to pinpoint locations on the surface of Earth. *See GPS Overview*, GPS.GOV, www.gps.gov/systems/gps (last modified Jan. 17, 2013).

[61] United States v. Maynard, 615 F.3d 544, 555 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

[62] *Id.* (explaining that the police had actually obtained a warrant earlier in the investigation, but installed the GPS device after the warrant had expired).

[63] 460 U.S. 276, 280–85 (1983).

[64] *Id.* at 277.

search. They used the evidence found therein to convict Knotts. The Court ruled that there was no expectation of privacy in the movements of a vehicle along public streets—this was essentially information that was "knowingly exposed" to the public. And although Knotts argued that the use of the electronic tracking device was different than a law enforcement officer following him in person, the Court dismissed the beeper as only being of "limited use" and noted that a police officer could have gleaned the same information that the beeper had with the naked eye.[65]

Both the Seventh and Ninth Circuits have relied on *Knotts* to hold that using a GPS device to track and monitor an individual's movements in his vehicle over an extended period of time is not a Fourth Amendment search. In *United States v. Garcia*,[66] police placed a GPS tracking device on the defendant Garcia's vehicle and used it to track him to a field where they found evidence of methamphetamine manufacturing. Prosecutors used this evidence to convict Garcia. Although the court expressed some concern about the potential implications of a GPS surveillance regime on privacy protection,[67] it held that use of the GPS device was not a Fourth Amendment search. The court's justification rested in part on the observation that use of the GPS device was merely a substitute for good old-fashioned police surveillance, which was "unequivocally *not* a search within the meaning of the [Fourth A]mendment."[68]

In *United States v. Pineda-Moreno*, the named defendant was observed purchasing supplies often used in growing marijuana.[69] Federal agents then undertook an extensive investigation of Pineda-Moreno, installing GPS tracking devices on his vehicle on seven different occasions.[70] When the GPS device alerted the agents that Pineda-Moreno was leaving a suspected marijuana growing site, they followed his car, arrested him, and eventually got consent to search his home and trailer, where they found marijuana.[71] The Ninth Circuit, considering the question whether the use of the GPS devices was a Fourth Amendment search, concluded that it was not: "The only information the agents obtained from the tracking devices was a log of

---

[65] *Id.* at 285. The Court also foresaw future difficulties in dealing with advancing technology that might not constitute such a "limited use." But in addressing the question of whether a warrant would be required in a case involving prolonged, round-the-clock surveillance, the Court declined to answer: "[I]f such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable." *Id.* at 283–84.

[66] 474 F.3d 994, 995 (7th Cir. 2007).

[67] *See infra* notes 90 and 102.

[68] *Garcia*, 474 F.3d at 997.

[69] 591 F.3d 1212, 1213 (9th Cir. 2010).

[70] *Id.* at 1213.

[71] *Id.*

the locations where Pineda-Moreno's car traveled, information the agents could have obtained by following the car."[72] Relying on *Garcia* as persuasive authority, the court reasoned that the use of the GPS device was simply a substitute for an activity that was not a search—that is, in-person surveillance by a police officer—and that this substitution did not fundamentally change the fact that Pineda-Moreno's movements were exposed to the public.[73]

However, the lower court decision in *Jones*, *United States v. Maynard*, distinguished *Knotts* in holding that warrantless GPS tracking of the type used in *Jones* was a search for Fourth Amendment purposes.[74] The *Maynard* court invoked the mosaic theory, a central concept in intelligence gathering more often applied in the national security context.[75] The theory holds that individual data points, while perhaps not revealing on their own, can be highly revealing if aggregated and analyzed as a whole.[76] In applying the mosaic theory to GPS tracking, the Court reasoned that "[t]he whole of one's movements over the course of a month is not constructively exposed to the public because, like a rap sheet, the whole reveals far more than the individual movements it comprises . . . no single journey reveals the habits and patterns that mark the distinction between a day in the life and a way of life."[77] Essentially, because GPS tracking revealed a more intimate and detailed picture of Jones's activities, the court found a conceptual difference between this type of surveillance and the use of the beeper in *Knotts*.[78]

In the end, a majority of the U.S. Supreme Court in *Jones* declined to

---

[72] *Id.* at 1216.

[73] *Id.*

[74] *Maynard*, 615 F.3d 544, 555–56 (D.C. Cir. 2009).

[75] For a discussion of the mosaic theory in general and its evolution in the context of the Freedom of Information Act, see generally David E. Pozen, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628 (2005).

[76] *Id.*

[77] *Maynard*, 615 F.3d at 562. The *Maynard* court also noted that the Supreme Court "implicitly recognized the distinction between the whole and the sum of the parts in the Fourth Amendment case of *Smith v. Maryland*," and "considered not just whether a reasonable person expects any given number he dials to be exposed to the phone company but also whether he expects all the numbers he dials to be compiled in a list." *Id.*

[78] *See also* People v. Weaver, 909 N.E.2d 1195 (N.Y. 2009). In *Weaver*, the Court of Appeals of New York similarly distinguished the use of a GPS tracking device from the beeper in *Knotts*:

> One need only consider what the police may learn, practically effortlessly, from planting a single [GPS] device. The whole of a person's progress through the world, into both public and private spatial spheres, can be charted and recorded over lengthy periods possibly limited only by the need to change the transmitting unit's batteries.

Id. at 1199.

frame the issue as one falling under *Katz*'s "reasonable expectation of privacy" test. Instead, the Court held the GPS tracking was a Fourth Amendment search because it was a trespass to place the tracking device on Jones's car—it did not hold that Jones had a reasonable expectation of privacy in the movements of his vehicle.[79] Relying on a *Boyd*-like conception of invasion of property rights as a Fourth Amendment search, the Court noted that *Katz* was viable, but that a reasonable expectation of privacy was not the sole criterion for defining a search.[80]

After the Court's narrow holding in *Jones*,[81] privacy advocates continue to argue that GPS technology, like mandatory data retention, provides the government another "irresistible temptation" to undertake unreasonably broad monitoring of individuals.[82]

III. DISCUSSION

A. THE "ASSUMPTION OF RISK" DOCTRINE

This Part argues that the controversies over mandatory data retention and warrantless GPS tracking are symptoms of the same problem—the assumption of risk doctrine implicit and often explicit in the Court's Fourth Amendment jurisprudence.

The assumption of risk language stems from the Court's consideration of retaining bank records in the *Miller* case: "The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[83] But the central idea of the assumption of risk doctrine is rooted in the language of *Katz*, nineteen years before: "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[84]

On its face, the language seems to echo the "plain view" doctrine used by courts in the Fourth Amendment context. As Justice Harlan noted in his concurrence in *Katz*, "[O]bjects, activities or statements that [an individual] exposes to the 'plain view' of outsiders are not 'protected' because no

---

[79] *See* United States v. Jones, 132 S. Ct. 945, 950 (2012).

[80] *Id.* at 951.

[81] *See, e.g.*, Tom Goldstein, *Why* Jones *Is Still Less of a Pro-Privacy Decision than Most Thought*, SCOTUSBLOG (Jan. 30, 2012, 10:53 AM), http://www.scotusblog.com/2012/01/why-jones-is-still-less-of-a-pro-privacy-decision-than-most-thought/.

[82] *See, e.g.*, Editorial, *Is GPS Tracking Too '1984'?*, L.A. TIMES, Nov. 10, 2011, at A22; *GPS Inventor Joins EFF in Fight Against Warrantless GPS Tracking*, ELECTRONIC FRONTIER FOUND. (Oct. 3, 2011), https://www.eff.org/press/archives/2011/10/03-0; Frank Miniter, *Is the Right to Privacy Dead?*, FORBES (Nov. 17, 2011, 4:09 PM), www.forbes.com/sites/frankminiter/2011/11/17/is-the-right-to-privacy-dead/.

[83] United States v. Miller, 425 U.S. 435, 443 (1976).

[84] Katz v. United States, 389 U.S. 347, 351 (1967).

intention to keep them to himself has been exhibited."[85] If a police officer pulls a vehicle over for a traffic stop and happens to see the passenger carrying drugs through the window, it is not a violation of that passenger's Fourth Amendment rights for the officer to seize the drugs—the contraband was there for anyone to see. Similarly, if a homeowner puts a sign on his front lawn declaring himself a criminal, he has "knowingly exposed" this information to the public and it violates no Fourth Amendment right for the government to use that information against him under the plain view doctrine.

As discussed above, the Court has applied this rationale repeatedly, holding in various contexts that any information disclosed to a third party is no longer "private" and thus is no longer protected by the Fourth Amendment—no matter what actual, subjective expectation of privacy the defendant held. In *White* and the government-informer cases, defendants gave information by word of mouth to another. In *Miller*, the defendant entrusted the bank with checks and deposit slips. In *Smith*, the defendant exposed the phone numbers he dialed to the phone company. But did any of these individuals *actually* expect that they had no privacy interest in their respective information that was "knowingly exposed" to outsiders? Common sense seems to dictate that Mr. Miller should reasonably expect some modicum of privacy in the records kept by his bank, or that Mr. Smith would be allowed some reasonable amount of surprise to find out that every phone number he dialed would be exposed to the government.[86]

The same rationale applies in the line of GPS tracking cases. In *Knotts*, the defendant "knowingly exposed" the movements of his vehicle to the public and thus, the inquiry was over—he could have no "reasonable expectation of privacy" against the tracking of his vehicle by the government. Following *Knotts*, the courts in *Garcia* and *Pineda-Moreno* used the same rationale to allow extensive warrantless GPS tracking of the defendants' vehicles, no matter what the *actual* expectation of privacy was on the part of Garcia or Pineda-Moreno. If one were to ask Mr. Garcia himself, or a reasonable cross section of society,[87] whether or not they would expect the government to be tracking their vehicles' every move for days or weeks at a time, it seems difficult to argue that they would answer in the affirmative.[88]

---

[85] *Id.* at 361 (Harlan, J., concurring).

[86] See *infra* text accompanying notes 125–135 for empirical studies on subjective expectations of privacy.

[87] The author here notes the obvious difficulty of defining such a group, but the argument remains the same—a "commonsense" understanding would be another way to phrase it.

[88] *See infra* text accompanying notes 131–133; *see also* United States v. Jones, 132 S. Ct. 945, 964 (2012) ("[S]ociety's expectation has been that law enforcement agents and others

One only has to look at the public outcry over mandatory data retention and warrantless GPS tracking to see that the assumption of risk doctrine has birthed controversial results in these two areas.[89]

In fact, mandatory data retention can be characterized as the logical extension of the assumption of risk doctrine, which allows warrantless GPS tracking. In both controversies, the assumption of risk doctrine allows the government to access data that has been "voluntarily exposed" by individuals: in one case, Internet usage data exposed to an ISP, and in the other, physical location data exposed to the general public. With respect to the Internet, the court-imposed regime is already far along the path of total surveillance; it has decided that information exposed to ISPs is no longer private. The data-retention controversy is about how much of that data law enforcement agencies will be able to access and the extent to which private companies must assist in that effort. GPS tracking might not be far behind. Judge Posner opined in *Garcia*:

> One can imagine the police affixing GPS tracking devices to thousands of cars at random, recovering the devices, and using digital search techniques to identify suspicious driving patterns. One can even imagine a law requiring all new cars to come equipped with the device so that the government can keep track of all vehicular movement in the United States. It would be premature to rule that such a program of mass surveillance could not possibly raise a question under the Fourth Amendment—that it could not be a search because it would merely be an efficient alternative to hiring another 10 million police officers to tail every vehicle on the nation's roads.[90]

Of course, this strikes a familiar chord with those concerned about mandatory retention of Internet data by ISPs. They fear that the government could similarly use the vast treasure trove of customer data in the Internet context to keep track of all movement in the United States, not along the physical highway, but along the information highway. Another commentator explicitly considers this connection between autobahn and infobahn:

> Hypothetically, if the police used a device to track where one travels in cyberspace, there is no reason to think that the use of such technology would constitute a search under the Fourth Amendment. When one travels along the digital highway, such movements are knowingly exposed to the public and merit no Fourth Amendment protection. The digital web where a user journeys would be considered the functional equivalent of the public streets. A cyber-beeper or pen register would seem to comport with the Court's analysis in *Smith* and *Knotts*.[91]

---

would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period.") (Alito, J., concurring in the judgment).

[89] *See supra* note 2.

[90] United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007).

[91] Brian I. Simon, *The Tangled Web We Weave: The Internet and Standing Under the*

Posner contemplates a regime of wholesale data gathering in the context of GPS tracking. Is mandatory data retention of GPS location data the next step in the *Jones* saga?

Whatever the future may hold, the Court's current Fourth Amendment jurisprudence assumes that *any* information that is not kept completely secret is up for grabs.[92] I now put forward the reasons why this trend is a pernicious one.

B. NORMATIVE JUSTIFICATIONS FOR CHANGES IN FOURTH AMENDMENT DOCTRINE

There are many reasons to fear government surveillance programs allowed by the Court's modern Fourth Amendment jurisprudence. Some critics are reminded of *Nineteen Eighty-Four* and Orwell's vision of totalitarian oversight;[93] others are concerned with more creeping conceptions of bureaucratic encroachment on civil liberties.[94]

In the context of warrantless GPS tracking and mandatory data retention, this Comment proposes that the normative justifications for changing Fourth Amendment doctrine fall into two central categories: particularity and necessity. By particularity, I mean that the Fourth Amendment intends to protect citizens from overly broad government intrusion—that it seeks to make intrusions into private life as narrow and particular as possible. Necessity refers to the idea that disclosure of personal data has become an almost inevitable requirement for participation in modern society.

1. *Particularity*

The Fourth Amendment's protection against unreasonable searches and seizures was largely a response to the English colonial practice of issuing writs of assistance.[95] Arising from the tradition of so-called general warrants issued in England,[96] these writs were used by English customs

---

Fourth Amendment, 21 NOVA L. REV. 941, 967 (1997).

[92] *See Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) ("[W]hatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.").

[93] United States v. Pineda-Moreno, 617 F.3d 1120, 1121 (9th Cir. 2010) (Kozinski, J., dissenting).

[94] *See* Solove, *supra* note 8, at 1101–14.

[95] *See generally* Louis Fisher, *Congress and the Fourth Amendment*, 21 GA. L. REV. 107 (1986).

[96] For a history of the Fourth Amendment and its colonial roots, see NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES

officers as justification for indiscriminate searches for smuggled goods.[97] Future colonial revolutionaries like John Adams spoke out against the writs of assistance as infringing on their rights as individuals.[98] Patrick Henry himself declared, "They may, unless the general government be restrained by a bill of rights, or some similar restrictions, go into your cellars and rooms, and search, ransack, and measure, everything you eat, drink, and wear. They ought to be restrained within proper bounds."[99]

Early state constitutions adopted safeguards against such arbitrary searches and seizures.[100] Eventually, these safeguards became federal law in the Fourth Amendment to the Constitution. Specifically, the language "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" was an explicit prohibition on the issuing of writs of assistance or general warrants.

That the Framers wanted to prevent overly broad or arbitrary government intrusion into individual life is clear. For the purposes of this argument, I will refer to that general principle as the principle of particularity. Behind this principle is the assumption that overbroad searches of private citizens are inherently prone to abuse and arbitrary action by government officials. Indeed, the general writs of assistance were decried by colonial revolutionaries as "the worst instrument of arbitrary power . . . [because they placed] the liberty of every man in the hands of every petty officer."[101] If the power to search is too broad, and if every person and every piece of data is searchable, the discretion of law enforcement officers becomes too powerful. Only by being *particular* in the description of people and places to be searched can law enforcement officers be restrained from exercising arbitrary discretion and using the search power to fulfill personal vendettas or perpetrate other abuses. This is what the Fourth Amendment ensures.

Yet while the Fourth Amendment is the central basis for the system that regulates conduct between individuals and the government, its doctrine

---

CONSTITUTION (1937). Lasson notes that "[t]hese writs, which received their name from the fact that they commanded all officers and subjects of the Crown to assist in their execution, were even more arbitrary in their nature and more open to abuse than the general warrants . . . ." *Id.* at 53–54 (internal citations omitted).

[97] Fisher, *supra* note 95, at 108–109.

[98] *Id.* at 109.

[99] Solove, *supra* note 8, at 1125.

[100] Fisher, *supra* note 95, at 110.

[101] Boyd v. United States, 116 U.S. 616, 625 (1886) (internal quotation marks omitted) (citing THOMAS M. COOLEY, A TREATISE ON THE CONSTITUTIONAL LIMITATIONS WHICH REST UPON THE LEGISLATIVE POWER OF THE STATES OF THE AMERICAN UNION 301–03 (1st ed. 1868)).

has stood essentially unchanged as technology advances and offers the government more broadly invasive and effective tools for individual surveillance. As Chief Justice Warren remarked in *Lopez*:

> [T]he fantastic advances in the field of electronic communication constitute a great danger to the privacy of the individual . . . indiscriminate use of such devices in law enforcement raises grave constitutional questions under the Fourth and Fifth Amendments . . . and these considerations impose a heavier responsibility on this Court in its supervision of the fairness of procedures in the federal court system.[102]

It is this Comment's contention that the Court has not lived up to the responsibility with which Warren felt it was entrusted.

New technology may encroach on the fundamental principle of particularity in two ways. The first is by allowing surveillance of an overbroad *number of individuals* at once. The second is by allowing the government to gather an overbroad *type of information* about the individuals it surveys.

The controversies over mandatory data retention and warrantless GPS tracking are just two current examples of how technological advances implicate these two types of violations of particularity.

i. Overbroad Types of Information

With respect to Internet data, an Internet user whose online activities are tracked is not the same as a bank user whose deposit slips are searched or a telephone user whose dialed numbers are recorded.[103] Activity on the Internet can be, and usually is, much more comprehensive and revealing than banking or dialing phone numbers[104] (which, it may be added, may both now be done online as well), meaning that law enforcement observers may have access to much irrelevant and perhaps personal data. Internet users may undertake a range of private activities online that are unrelated to a law enforcement interest: e-mailing friends and family, checking medical records, e-mailing doctors, participating in political discussion, or exploring sexual proclivities. Accessing customer data from an ISP is not akin to searching a car or a house for drugs or evidence of a specific crime. It is more analogous to following someone, within the home and without, listening in on that person's conversations, reviewing a list of books checked out and purchases made, and, in sum, obtaining a complete picture

---

[102] Lopez v. United States, 373 U.S. 427, 441 (1963).

[103] *See generally* Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976). The *Greenwood* case is another example of a search discovering overly broad types of information, as Justice Brennan pointed out in dissent: "A single bag of trash testifies eloquently to the eating, reading, and recreational habits of the person who produced it." California v. Greenwood, 486 U.S. 35, 50 (1988) (Brennan, J., dissenting).

[104] *See* Tokson, supra note 44, at 602–04.

of that person's life. This is the quintessential violation of particularity against which the Framers wanted to protect when they declared that only those warrants could issue that were "particularly describing the place to be searched, and the persons or things to be seized."

The relatively new technology of GPS tracking devices as used on vehicles also implicates particularity in terms of overbroad types of information. As the New York Court of Appeals pointed out in *Weaver*, using a GPS device to track the totality of a vehicle's movements over an extended period of time reveals much more information than does following that person in a car for one discrete trip.[105] Similarly, in *Maynard*, the D.C. Circuit found that the defendant did not have a reasonable expectation of privacy in individual trips taken in public, but *did* have such a reasonable expectation in the totality of his movements, as documented by the GPS device over a month-long period.[106]

When law enforcement attaches a GPS device to a suspect's vehicle, it is true that they might find evidence that the vehicle made stops at suspicious locations, as was the case in *Pineda-Moreno*. But there is nothing in the technology or current Fourth Amendment doctrine that prevents law enforcement from seeing every innocent movement the vehicle makes, as well. This is one of the ironies of the technological erosion of Fourth Amendment privacy protections: that new technologies are advanced enough to provide law enforcement with a way to get the information they need, but not yet advanced enough to self-regulate and exclude all of the private and probably irrelevant data that they do not need. These types of technologies inherently carry the potential to violate the particularity principle by giving law enforcement access to an overbroad set of data.

ii. Overbroad Numbers of Individuals

The outcry over mandatory data-retention laws is largely a response to a violation of particularity in terms of the number of individuals who are surveilled. As an attorney for the Electronic Frontier Foundation warned about H.R. 1981, "[t]he data retention mandate in this bill would treat every Internet user like a criminal and threaten the online privacy and free speech

---

[105] *See* People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009).

[106] *See* United States v. Maynard, 615 F.3d 544, 560 (D.C. Cir. 2009) ("It is one thing for a passerby to observe or even to follow someone during a single journey as he goes to the market or returns home from work. It is another thing entirely for that stranger to pick up the scent again the next day and the day after that, week in and week out, dogging his prey until he has identified all the places, people, amusements, and chores that make up that person's hitherto private routine.").

rights of every American."[107] The technological ability and capacity of ISPs to retain data on every customer now allows a data-retention regime that collects in its net not only those suspected of crimes, but also every person who uses that provider's service. This is in stark contrast to the current regime in the United States, discussed above, which provides for data retention only for those customers who are already the subject of a law enforcement investigation. One does not need a very active mind to imagine widespread government searches of a database of innocent user activity that would root out patterns of "suspicious" Internet use.

And although GPS tracking technology does not implicate this type of particularity quite as explicitly, there is still the potential for the same kind of overbroad searching allowed by data retention. A GPS device does not know who drives a vehicle—it only tracks the vehicle itself. Potentially, then, a GPS device like the one used in *Jones* will track not only the Joneses of the world, but also anyone who associates with the Joneses and rides in or uses that vehicle: girlfriends of the Joneses, brothers of the Joneses, and the children of the Joneses.

These were the kinds of overbroad searches that Madison and the Framers sought to curtail in drafting the Fourth Amendment; much like the hated writs of assistance, they encompass either too many individuals, or too many types of information, or both.

Judge Posner remarked in *Garcia*:

> Technological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive. Whether and what kind of restrictions should, in the name of the Constitution, be placed on such surveillance when used in routine criminal enforcement are momentous issues that fortunately we need not try to resolve in this case.[108]

This Comment contends that the time is ripe for these "momentous issues" to be decided and that these violations of the fundamental constitutional concept of particularity are grave enough to warrant a change in the doctrine.

2. *Necessity in the Internet Age*

The other essential justification for a change in current Fourth Amendment doctrine with respect to new technology falls into the category of what I refer to here as necessity—i.e., that it is becoming increasingly difficult to function in modern society without exposing personal information to others.

The assumption of risk doctrine itself rests on an assumption that the

---

[107] Reitman, *supra* note 1.

[108] United States v. Garcia, 474 F.3d 994, 998 (2007).

giving up of information by an individual is undertaken voluntarily. In this Part, I argue that as new technologies with potential for widespread surveillance have become more prevalent in modern society, it has become increasingly impractical or even impossible to live one's life adhering to more traditional standards of privacy.

The Internet is not a fad. While it might not be discussed in the same breath as human necessities like food, water, and shelter, it may not be far behind. In the United States, individuals are increasingly conducting business online, communicating online, and entertaining themselves online. According to a Nielsen study in 2010, 55% of American adults use the Internet every day.[109] Forty-five percent of American adults use it to communicate every day; 30% use it to get news every day; and 18% use it to bank online every day.[110] New, unconventional uses are arising all the time. Interactive video games like World of Warcraft, social networking giants like Facebook and Twitter, and discussion forums of infinite varieties attract millions of active users worldwide.

The *importance* of the Internet does not simply follow from the fact of its widespread use, but it is increasingly being recognized as an indispensable part of the modern experience. In a recent report, the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, recognized the importance of the Internet. According to La Rue, the Internet is fundamental for the basic human need to give and receive information, to organize, and to express opinions:

> Given that the Internet has become an indispensable tool for realizing a range of human rights, combating inequality, and accelerating development and human progress, ensuring universal access to the Internet should be a priority for all States.[111]

A private study commissioned by Internet giant Cisco in 2011 found that one-third of college students questioned in fourteen different countries agreed that the Internet was as important to them as water, food, air, and shelter.[112]

---

[109] *How the World Spends Its Time Online*, VISUALECONOMICS, http://visualeconomics.creditloan.com/how-the-world-spends-its-time-online_2010-06-16/ (last visited May 20, 2013).

[110] *Id.*

[111] Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *17th Sess. on the Promotion and Prot. of All Human Rights, Civil Political, Economic, Social, and Cultural Rights, Including the Right to Development*, Human Rights Council, U.N. DOC. A/HRC/17/27 (May 16, 2011) (by Frank La Rue).

[112] CISCO, 2011 CISCO CONNECTED WORLD TECHNOLOGY REPORT (2011), *available at* http://www.cisco.com/en/US/solutions/ns341/ns525/ns537/ns705/ns1120/2011-CCWTR-Chapter-3-All-Finding.pdf.

Is it realistic to ask citizens to make the choice between using the Internet and keeping a private life? More importantly, is it right to ask individuals to make that choice? From a standpoint of protecting civil liberties, the answer to these questions must be "no"—but nevertheless it is what the courts require of our citizens today.[113]

We might go further and consider whether we should ask citizens to choose between driving cars and protecting the privacy of their movements over extended periods of time. The potential chilling effect such a choice would have on our constitutionally protected fundamental freedom of movement is obvious.

Consider the future implications: what about an advanced device that combined facial recognition technology with an aggregation of closed circuit commercial video feeds to track individual human movement throughout the day?[114] In deciding that such a regime would not violate a person's Fourth Amendment rights because they had knowingly exposed their public movements to the world, the Court might very well ignore the dilemma facing individuals who had a choice between total government surveillance and never leaving home.

As Justice Warren warned, in a regulatory system based on the vague and simple language of the Fourth Amendment, much of the responsibility for drawing the line in interactions between the citizen and the state falls on the Court.[115] Yet the Court has largely failed to update its Fourth Amendment jurisprudence since *Katz*. Solove declares the Court's more recent Fourth Amendment cases to be the harbingers of a "new *Olmstead*, one that is just as shortsighted and rigid in approach."[116] The Court in *Olmstead* took a narrow formalistic approach to privacy in holding that only physical intrusions were government searches. The Court in *Smith*, *Miller*, and its other assumption of risk cases adopted a similarly severe approach in holding that any information that is "knowingly exposed" cannot be the subject of Fourth Amendment protection.[117] In sum, modern technology

---

[113] *See supra* Part II.A.

[114] One study conducted in London concluded that the city was home to over 500,000 closed-circuit television surveillance cameras—one camera for every fourteen people in the city. Michael McCahill & Clive Norris, *CCTV in London* (Ctr. for Criminology & Crim. Just., Working Paper No. 6, 2002), *available at* http://www.urbaneye.net/results/ue_wp6.pdf.

[115] Lopez v. United States, 373 U.S. 427, 441 (1963).

[116] Solove, *supra* note 8, at 1133.

[117] The Court made some attempt to rectify this in *Kyllo v. United States*, 533 U.S. 27 (2001). In that case, federal agents suspected that Kyllo was growing marijuana inside his suburban home. They used a thermal-imaging device to scan the outside of his home to determine whether the amount of heat emanating from it was consistent with the use of certain types of lamps used in the manufacture of marijuana. The scan showed that the heat emanating from particular areas of Kyllo's home was hotter than the rest of the home, and

has effected a fundamental change in society whereby individuals find disclosure of personal information inevitable to a certain degree. The Court should update Fourth Amendment doctrine to reflect this change.

Even if it were not necessary, or even important, to engage with modern technology and expose information about oneself, the Court's conception of "privacy" expectations is flawed. In the Court's current Fourth Amendment jurisprudence, privacy is an all-or-nothing game: either there is an expectation of total privacy, or there is no expectation of privacy at all. For example, when an individual has trash in his kitchen trash can, that refuse is private, but as soon as the trash is given to the garbage collector, it is fair game for all.[118] Consider bank records: once they are in the hands of a bank, there is no longer *any* expectation of privacy in those records, at least with respect to the government.[119] Is this a valid place to draw the line? It seems that most people who have their trash rifled through on the curb or their bank records exposed to the public would feel that their privacy had been violated to some degree.[120] Judge Kozinski put it succinctly in his *Pineda-Moreno* dissent:

> [T]here are many parts of a person's property that are accessible to strangers for limited purposes: the mailman is entitled to open the gate and deposit mail in the front door slot; the gas man may come into the yard, go into the basement or look under the house to read the meter; the gardener goes all over the property, climbs trees, opens sheds, turns on the sprinkler and taps into the electrical outlets . . . . This doesn't mean that we invite neighbors to use the pool, strangers to camp out on the lawn or police to snoop in the garage.[121]

Essentially, there is no gray area in current Fourth Amendment doctrine. As soon as privacy is given up with respect to one other person, privacy no longer exists with respect to anyone. As Justice Sotomayor pointed out in her concurrence in *Jones*, "[t]his approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[122]

---

substantially hotter than neighboring homes. Based in part on this evidence, agents secured a warrant and convicted Kyllo. *Id.* at 29–30. In holding that the use of the thermal-imaging device was a Fourth Amendment search, the Court noted that the device was so technologically new that it was not in public use and thus that Kyllo could not have expected that such a device would invade his privacy. *Id.* at 40. This case only went so far, however—the fact that it was the interior of Kyllo's home seemed to play an important part in the Court's decision. *Id.* at 34.

[118] *See generally* California v. Greenwood, 486 U.S. 35 (1988).

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

[120] *See infra* text accompanying notes 125–135.

[121] United States v. Pineda-Moreno, 617 F.3d 1120, 1123 (9th Cir. 2010) (Kozinski, J., dissenting).

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

While the Court declined to address these issues in *Jones*, it is likely only a matter of time before they present themselves again. This Part shows that these are fundamental problems that demand a change in Fourth Amendment doctrine.

IV. A MODIFIED "REASONABLE EXPECTATION OF PRIVACY"

In this Part, I present a revised standard of a "reasonable expectation of privacy" that excludes *Katz*'s "knowingly exposed" assumption of risk exception.

Part II of this Comment attempted to show that the assumption of risk doctrine gives us unreasonable and backward results in applying the *Katz* reasonable expectation of privacy test. I now propose that the Court should adopt a more flexible approach to the *Katz* test by eliminating the rigid per se rule that *any* information divulged or "knowingly exposed" in any way is no longer private. The remaining part of *Katz*, Justice Harlan's now famous two-prong inquiry into whether there was an expectation of privacy and whether that expectation was reasonable,[123] would form the new, modified *Katz* test.

Much as *Katz* attempted to bring more flexibility to Fourth Amendment jurisprudence as a response to controversial cases like *Olmstead*, this modified "reasonable expectation of privacy" test should allow courts to accept the commonsense notion that privacy is not an all-or-nothing principle. Some commentators argue as a whole that *Katz* cannot be saved.[124] Although the privacy issues discussed in this Comment do bring the whole structure of *Katz* into question, I contend that in the context of access to Internet user data and warrantless GPS tracking, *Katz* remains a viable guide if modified correctly. In these cases, the *Katz* test should be limited to the two-step inquiry put forward by Justice Harlan, which has the benefit of a detailed jurisprudential history immediately familiar to courts. The "knowingly exposed" exception to that test, which led to the third-party doctrine and warrantless GPS tracking, should be relegated to the dustbin of Fourth Amendment history.

A. APPLICATION TO MANDATORY DATA RETENTION AND WARRANTLESS GPS TRACKING

How would such a modified *Katz* test treat the two controversies considered in this Comment? Absent the "knowingly exposed" assumption of risk exception, the Court would look first to whether there was an actual, subjective expectation of privacy and then to whether society was prepared

---

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

[124] *See, e.g.*, Skok, *supra* note 23, at 82.

to deem that expectation a reasonable one.

Is it reasonable to expect that telling something to a friend, or handing over records to a bank, exposes that information to government agents? Commonsense expectations aside, empirical studies suggest that, for most, the answer is no.[125] The authors of one study asked individuals to rank various investigative police actions on a scale of how intrusive they felt the actions to be. Some of the survey results showed that actual expectations of privacy generally mapped onto the Court's conception of those expectations. For example, searching a bedroom and bugging a phone were both seen by survey respondents as highly intrusive searches, views which the Court's cases would corroborate.[126]

Other results, however, showed a significant disparity in what the Court considers intrusive and what reasonable people consider intrusive. The use of undercover agents, repeatedly held by the Court not to implicate the Fourth Amendment under the assumption of risk doctrine,[127] was seen by survey respondents as very intrusive.[128] Perusing bank records, held not to be a Fourth Amendment search under the third-party doctrine in *Miller*,[129] was similarly seen by respondents as a highly intrusive search.[130] While "using a beeper to track car" was somewhat lower on the intrusiveness rankings,[131] this survey was conducted in the early 1990s and the question was presumably based on the facts of *Knotts*. We might imagine what the result would have been if the question were changed to "using a GPS device to track every movement of car for a month." In fact, in a more recent survey conducted by Zachary Gray of UC Hastings, Gray explicitly considered society's expectations of privacy related to more modern GPS vehicle tracking as in *Jones*.[132] His conclusion was that "[s]ociety overwhelmingly believes that GPS tracking is unjustifiable and violates an individual's privacy rights."[133]

The results of these surveys show that under the modified *Katz* test proposed here, the Court would at the very least be forced to find a serious

---

[125] *See* 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, 739 (1993).

[126] *Id.*

[127] *See supra* Part I.

[128] Slobogin & Schumacher, *supra* note 125, at 740.

[129] United States v. Miller, 425 U.S. 435, 441–43 (1976).

[130] Slobogin & Schumacher, *supra* note 125, at 740.

[131] *Id.* at 737–38.

[132] Zachary Gray, Note, *Herding* Katz*: GPS Tracking and Society's Expectations of Privacy in the 21st Century*, 40 HASTINGS CONST. L.Q. 145, 147–48 (2012).

[133] *Id.* at 166.

constitutional problem with those regimes.[134] Such a test would set courts free to follow the logic of the D.C. Circuit in *Maynard*: "In considering whether something is 'exposed' to the public as that term was used in *Katz* we ask not what another person can physically and may lawfully do but rather what a reasonable person expects another *might actually* do."[135]

This section has attempted to show that a modified *Katz* test rejecting the assumption of risk exception would find serious constitutional problems with both mandatory data retention and warrantless GPS tracking. In the next section, I will address the main counterarguments against this proposed test.

B. FUTURE APPLICATIONS AND CONCERNS

There are viable concerns with this modified *Katz* test. One is the difficulty it might pose for law enforcement, both in terms of requiring complicated decisions by police officers and in hindering efficient searching. A more important concern from the privacy advocate's perspective is that, like current *Katz* jurisprudence, it leaves open the possibility of future erosion of privacy by advancing technology. I address these arguments in turn.

1. *Law Enforcement Concerns*

One criticism of this modified *Katz* test, and indeed of any change to current doctrine that allows for greater privacy protection under the Fourth Amendment, is that it will increase the cost of effective law enforcement and may allow some criminals to go free.[136] Since more law enforcement actions will now be considered searches for Fourth Amendment purposes, officers will be forced to obtain more warrants, thus increasing the cost and decreasing the efficiency of law enforcement. Many also argue that in the wake of September 11, 2001, the government has a greater interest in

---

[134] As the authors of the study point out, the Court has been reluctant to embrace empirical studies in its opinions. This aside, the point still remains that the Court would at least be forced to consider what reasonable expectations of privacy might be if the assumption of risk doctrine were rejected. *See* Slobogin & Schumacher, *supra* note 125, at 742–43.

[135] United States v. Maynard, 615 F.3d 544, 559 (D.C. Cir. 2010) (emphasis added). For a convincing argument that people may reasonably expect that digital information is being reviewed by automated systems, but not by actual human beings or government agents, see Tokson, *supra* note 44, at 581.

[136] *See* United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007) ("Of course the [Fourth] amendment cannot sensibly be read to mean that police shall be no more efficient in the twenty-first century than they were in the eighteenth. There is a tradeoff between security and privacy, and often it favors security.").

obtaining personal information.[137] While this may be true, this Comment has attempted to show that the consequences of the assumption of risk doctrine have resulted in regimes of government investigation that are broadly invasive and that ignore that changing technology has made it almost a necessity to expose personal information in the course of everyday life.[138] Efficient law enforcement is a legitimate and important government interest, but it must be balanced against competing interests of privacy.[139]

While this balancing of interests does require a complicated normative assessment, the current regime seems to resolve each question in favor of law enforcement interests at the expense of privacy interests.[140] The discussion of particularity and necessity above attempts to show that the privacy rights abrogated under current Fourth Amendment doctrine are fundamental and require more weight in this test.

A similar argument may be made that police officers should not be required to make difficult decisions on the ground about what activity is permitted and what activity is not. It is true that the modified *Katz* test proposed here, which eliminates the "knowingly exposed" exception, would redefine some law enforcement actions as searches which previously were not. This has the potential for engendering uncertainty as law enforcement agencies struggle to define what is a search under the new test. Simplicity, though, is not the essential aim of the modified *Katz* test proposed here—rather, the principal aim is privacy protection. Moreover, complexity is nothing new for law enforcement in this area: Fourth Amendment doctrine is already a notoriously tangled web of exceptions to the warrant requirement.[141] Law enforcement officers will still need to make difficult decisions about what constitutes a search, but no more than they need to today.

The activities with which this Comment is concerned, furthermore, are not the types of activities that require heat-of-the-moment decisions, such as stops and frisks, vehicle stops, or the appropriate use of force. Data retention and GPS tracking are methodical surveillance techniques that require advance planning. Therefore, law enforcement would not be unduly

---

[137] *See* Solove, *supra* note 8, at 1097–98.

[138] *See supra* Part II.B.

[139] Michigan v. Summers, 452 U.S. 692, 706 (1981) (referring to the "general rule that the Fourth Amendment . . . perform[s] the constitutional balance between police objectives and personal privacy") (Stewart, J., dissenting).

[140] *See supra* Part I.

[141] *See, e.g.*, Note, *The Fourth Amendment's Third Way*, 120 HARV. L. REV. 1627, 1628 (2007) (referring to the Court's Fourth Amendment *Katz* doctrine as a "vast maze" consisting of "a multitude of exceptions and exemptions" to the warrant requirement and "doctrinal nooks and crannies").

hindered by having to acquire a warrant or make difficult decisions before conducting these types of technology-heavy activities.

2. *Future Privacy Erosion and Other Possible Alternatives to* Katz

Another criticism of *Katz* in general is that, by depending in part on an individual's subjective expectation of privacy, it allows for the gradual erosion of those expectations as the government uses more invasive means of investigation.[142] For example, what if the government took out a television advertisement during the Super Bowl and announced that it would begin tapping all phone conversations or that it would read all personal e-mails? Individuals might then have lost their subjective expectation of privacy under *Katz*—even the modified *Katz* test proposed here—and those e-mails or phone conversations would no longer be protected by the Fourth Amendment. Although a comprehensive response to this general criticism of *Katz* is somewhat outside the scope of this Comment, until such drastic action occurs, we have not yet reached the point where we need to resolve this problem. As I argued in the preceding Part, there exists today a subjective and reasonable expectation of privacy in both warrantless GPS tracking and Internet usage data that is circumvented only by the assumption of risk exception. Absent that loophole, courts would be forced to consider whether there was a subjective and reasonable expectation of privacy in those activities and they would likely conclude that there is.[143]

Some commentators, in looking for an immediate answer to future erosion of privacy, have proposed that *Katz* be completely discarded.[144] Skok, for instance, proposes that *Katz* be overturned and advocates instead for the Court to undertake the normative inquiry it used previously in *Smith v. Maryland*.[145] Under this test, the Court would ignore the two-part inquiry of *Katz* and ask instead: "should an individual in a free and open society be forced to assume the risk that the government will monitor her as she engages in the activity at issue?"[146] Skok argues that the Court would answer this central question by looking to constitutional principles and to what the Framers intended to protect.[147]

This test has the benefit of hitching the Fourth Amendment to something that appears concrete—the original intent of the Framers. This

---

[142] *See* Kyllo v. United States, 533 U.S. 27, 34 (2001) ("The *Katz* test . . . has often been criticized as circular, and hence subjective and unpredictable.").

[143] *See supra* Part III.A.

[144] *See, e.g.*, Skok, *supra* note 23, at 82.

[145] *See id.*

[146] *Id.*

[147] *Id.* at 82–83.

alleviates the concern that as new technology arises, subjective expectations of privacy will simply be eroded over time. Its drawback, ironically, is this very detachment from changing expectations of privacy in modern society. There are privacy questions today that simply do not allow for easy comparisons to the issues of the colonial era. Modern police forces were not contemplated in the late eighteenth century.[148] We do not know what the Framers would have thought of GPS tracking of vehicles. While personal papers and letters to friends may have been sacred to the Framers,[149] we do not know how they would have felt about Facebook posts or Web histories, and there is no way to ask them.

We have a much better idea, however, of how people feel about modern privacy issues today. If we want more data to determine how people feel about various invasions of privacy in the modern world, we have the tools and the opportunity to collect it.[150] Retaining the part of *Katz* that anchors it to current societal expectations of privacy avoids asking the Court to make guesses about original intent.

In a response specific to the third-party doctrine, Professor Stephen Henderson sets forth four factors to consider in determining the expectation of privacy of a transferor of information to a third party. They are: the necessity of transferring the information to meaningful participation in society; the extent to which the information is personal; the extent to which the information is accessible to nongovernment persons outside of the transferee; and the extent to which existing law restricts or allows access to the information.[151] Although this test is rather complex, Henderson notes that there are few easy answers in the Fourth Amendment/privacy protection debate.[152]

Henderson's test may be a significant step in the right direction in terms of the third-party doctrine. Indeed, it overlaps somewhat with the argument presented here. However, as this Comment has argued, the underlying problem with the third-party doctrine is the assumption of risk exception to *Katz*, which leaves information unprotected even if it is not exposed to a particular third-party institution. As in the case of GPS tracking, the information may simply be exposed to the public at large.[153]

---

[148] *See* Lawrence Rosenthal, *Pragmatism, Originalism, Race, and the Case Against* Terry v. Ohio, 43 TEX. TECH L. REV. 299, 341–46 (2010).

[149] *See* Boyd v. United States, 116 U.S. 616, 641 (1886).

[150] *See supra* Part III.A.

[151] *See* Stephen Henderson, *Real-Time and Historic Location Surveillance After* United States v. Jones*: An Administrable, Mildly Mosaic Approach*, 103 J. CRIM. L. & CRIMINOLOGY 803, 815–17.

[152] *Id.* at 823–24.

[153] *See supra* Part II.A.

My proposed modified *Katz* test thus addresses a somewhat broader concern than does Henderson's four-factor solution.

V. CONCLUSION

This Comment has argued that the current controversies over mandatory data retention and warrantless GPS tracking are symptoms of the same problem: *Katz*'s assumption of risk doctrine. It further argued that changing technology and a static interpretation of the Fourth Amendment have allowed for a regime in which searches are overbroad both with respect to people searched and information obtained. The rationale that information "voluntarily exposed" is no longer private must now be considered obsolete in an age where exposing some amount of personal information is necessary to navigate society.

Under a new conception of the two-part *Katz* test which excludes the "knowingly exposed" exception to the "reasonable expectation of privacy" analysis, both mandatory data retention and warrantless GPS tracking would pose serious constitutional questions—which they should. *Katz*'s rigid assumption of risk rule must be changed to keep up with the times.