# The Third Party Exception: Reshaping an Imperfect Doctrine for the Digital Age

*Rebecca Lipman**

It is a chilly night in Cambridge, and you go to Seamless.com to find a restaurant to order dinner from. After placing your order, you decide to kill a little time looking at Facebook. Suddenly in your Facebook newsfeed, there is an advertisement for one of the restaurants you just looked at on Seamless.com. Slightly spooked, you check your e-mail, and on the Gmail sidebar appears a list of advertisements for hotels to stay at in Washington, D.C.—right beside your latest e-mail to your friend mentioning your upcoming trip to D.C. Not only has Google deduced that you are going to D.C., it knows that you do not live there and might need a hotel room.

This experience is increasingly common. As users become more aware that what they do online is seen by others, or at least by complex algorithms,[1] what constitutes a "reasonable expectation of privacy"[2] within the scope of the Fourth Amendment will likely shift. However, third parties can see more than your browsing history and your e-mails. Credit cards and banks track your purchases, cell phones and E-Z Passes track your location, and keycards can track employees' locations at work and keep tabs on how long an employee spends in the break room each day.[3] Your private chats can be stored on a technology company's servers,[4] along with your address books, personal calendars, and a history of your viewing habits.[5]

Online activity is not tracked solely by the individual websites you visit. Many websites allow dozens of outside companies to monitor their

* J.D. Candidate, Harvard Law School, Class of 2015. The author would like to thank her husband Benjamin Feuer for his love and support of all her ambitions, and Professor Phil Heymann and the Harvard Law and Policy Review editorial team for their advice and comments.

[1] Google runs algorithms that scan users' e-mails to determine which ads to display. Dan Mitchell, *Much Like Google, Microsoft Also Scans Your E-mail*, CNN MONEY (Mar. 5, 2013, 4:03 PM), http://tech.fortune.cnn.com/2013/03/05/much-like-google-microsoft-also-scans-your-e-mail/.

[2] *See* Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

[3] Fred H. Cate, *Government Data Mining: The Need for A Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 456 (2008).

[4] Google stores all Gmail chats by default. *See Chatting Off the Record*, GOOGLE, https://support.google.com/talk/answer/29291?hl=en.

[5] While services like Netflix make it obvious that what you watch is being tracked, YouTube will also keep track of all videos you view by default. Matt Elliott, *How to Delete and Pause Your YouTube Watch History*, CNET (Nov. 19, 2013, 3:20 PM), http://howto.cnet.com/8301-11310_39-57612940-285/how-to-delete-and-pause-your-youtube-watch-history/.

users' activity.[6] This can lead to a wealth of information being shared unintentionally, particularly if you believe you are sharing information in a relatively private setting. For example, dating websites routinely ask their users a slew of questions when they sign up,[7] ranging from their educational and work backgrounds to their drinking and recreational drug habits.[8] By filling out such a survey, ostensibly only for the website's use in connecting you with a potential date,[9] you may be simultaneously revealing to other companies that you occasionally engage in illegal drug use.[10]

There are many companies that specialize in aggregating personal data about individuals.[11] They collect information about virtually every individual they can[12] and then sell that information to private companies and government agencies.[13] They sell social security numbers, past addresses, past employers, automobile registrations, professional licenses, criminal records, and names of relatives.[14] When government agencies utilize such information, agency employees are not always aware of the privacy protections that may apply to some of the information.[15]

The range of information that private companies have access to, and the relative ease of processing that data, makes it possible for a third party or government official to put together a more detailed picture of an individual's life than ever before.[16] If the police install a GPS tracker under your car, they can determine where you work and where you live, and draw a number of limited conclusions about you.[17] However, if the police have access to your e-mail and bank accounts, they can determine what your salary is, who your friends are, and what you are likely doing at work or inside your home on a given day.

---

[6] Websites often allow other companies to monitor their users' activity. Daniel Zwerdling, *Your Digital Trail: Private Company Access*, NPR (Oct. 1, 2013, 2:00 PM), http://www.npr.org/blogs/alltechconsidered/2013/10/01/227776072/your-digital-trail-private-company-access.

[7] *See, e.g.*, *29 Dimensions of Compatibility*, eHarmony, http://www.eharmony.com/why/dating-relationship-compatibility/.

[8] Zwerdling, *supra* note 6.

[9] *See, e.g.*, eHarmony, *supra* note 7.

[10] Zwerdling, *supra* note 6.

[11] Cate, *supra* note 3, at 457. LexisNexis is one such aggregator. *Consumer Access*, LexisNexis, https://www.lexisnexis.com/privacy/for-consumers/request-personal-information.aspx.

[12] *See* Bob Sullivan, *ChoicePoint Files Found Riddled with Errors*, NBC News (Mar. 8, 2005, 4:41 PM), http://www.nbcnews.com/id/7118767.

[13] Eric Noe & Paul Eng, *ChoicePoint Fraud Illustrates Identity Threat*, ABC News (Jan. 26, 2006), http://abcnews.go.com/Business/FinancialSecurity/story?id=506031.

[14] *Id.*; Sullivan, *supra* note 12.

[15] *Privacy: Key Challenges Facing Federal Agencies Before the Subcomm. on Commercial and Admin. Law*, 110th Cong. 2–3 (2006) (statement of Linda D. Koontz, Director, Information Management Issues), *available at* http://www.gao.gov/new.items/d06777t.pdf.

[16] *See* Cate, *supra* note 3, at 485.

[17] The D.C. Circuit noted, in the case leading up to *U.S. v. Jones*, that prolonged GPS tracking could lead to "deduc[ing] whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts." United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010).

The government is able to access much of this private information by virtue of the third party exception. The third party exception is a standard developed by the courts that allows the government to access information that individuals share with third parties without a warrant. The modern version of the exception is based on a 1979 Supreme Court case, *Smith v. Maryland*.[18] Given the dramatic technological advancements that have occurred since 1979, the third party exception needs to be reexamined and reigned in to more accurately reflect the privacy protections that Americans expect under the Fourth Amendment.

This article will first look at how the third party exception developed and Congress's statutory responses to it. Part II will examine how the third party exception has been applied recently and how courts have been grappling with changes in technology. Part III will explore potential alternative versions of the third party exception. Part IV will evaluate those alternatives and conclude.

## I. The Development of the Third Party Exception: A Mixture of Consent and Minimal Content

### *A.* Smith v. Maryland *and Its Predecessors*

Recent opinions grappling with the third party exception often hearken back to *Smith v. Maryland*[19] for the assertion that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[20] The majority opinion in *Smith* relied on a number of older cases for that statement.[21] The previous cases included *Hoffa v. United States*[22] and *Lopez v. United States*,[23] both of which involved undercover informants.

When Jimmy Hoffa was on trial in 1962 for violating the Taft-Hartley Act, he attempted to bribe several jurors and talked about his jury tampering plans in front of his friend, Edward Partin.[24] Hoffa did not know that Partin was cooperating with federal agents at the time and informing them of Hoffa's activities.[25] In *Lopez*, a bar owner attempted to bribe an Internal Revenue Agent, who reluctantly took the money, reported it to his supervisors, and went back to the bar wearing a wire.[26] In both cases, the Supreme Court held that the government could use the live or recorded testimony of the informants at trial,[27] emphasizing that it was the defendants' choice to

---

[18] 442 U.S. 735 (1979).

[19] *See, e.g.*, *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 612 (5th Cir. 2013).

[20] *Smith*, 442 U.S. at 743–44.

[21] *Id.* at 744.

[22] 385 U.S. 293 (1966).

[23] 373 U.S. 427 (1963).

[24] *Hoffa*, 385 U.S. at 296 n.3.

[25] *Id.* at 298.

[26] 373 U.S. at 430.

[27] *Hoffa*, 385 U.S. at 303; *Lopez*, 373 U.S. at 440.

reveal their illegal activities to the informants. The Court noted that the defendants had a "misplaced confidence"[28] that the informants would not reveal their activities, and that the risk of being overheard or deceived is "the kind of risk we necessarily assume whenever we speak."[29]

The Court's analyses in *Hoffa* and *Lopez* were not concerned with the quantity or sensitivity of the information the defendants revealed, only with the fact that the defendants had voluntarily disclosed the information.[30] A cynical interpretation may be that the Court did not wish to impede law enforcement's use of informants or prosecutors' abilities to fully utilize any information informants could uncover. A fairer interpretation might be that the Court was motivated by the fact that the defendants revealed their private information face to face, to people they had chosen to trust. As Justice Brennan noted, we are all familiar with the risks that come with sharing our private information.[31] Most people learn at a very young age that a secret whispered to one close friend at lunchtime may be common knowledge to the whole school by the end of the day.

This kind of immediately relatable context for the "misplaced confidence"[32] doctrine did not play into *United States v. Miller*,[33] where federal agents sought incriminating information not from individuals but from the defendant's banks. In *Miller*, the Court emphasized that the documents at issue were records belonging to two banks, not the defendant's "private papers."[34] *Hoffa's* "misplaced confidence"[35] doctrine was a bad fit for *Miller*, as individuals have an expectation that any bank they deal with will not act like an untrustworthy friend and reveal their finances to the world at will. It would have been difficult for the Court to call this expectation unreasonable, particularly when the banks in the case had to be compelled to share their records with a subpoena.[36] Instead, the *Miller* Court focused on the nature of the records ("these are the business records of the banks")[37] and on the actual content of the records. The Court said that the defendant could not have had an "expectation of privacy" in the contents of the records, as they were "not confidential communications but negotiable instruments to be used in commercial transactions."[38] This reasoning, combined with the fact that the defendant "voluntarily" shared his information with the banks,[39] led the Court to conclude that the defendant did not have a protected privacy interest in his bank records.[40]

---

[28] *Hoffa*, 385 U.S. at 302.
[29] *Lopez*, 373 U.S. at 465 (Brennan, J., dissenting).
[30] *See Hoffa*, 385 U.S. at 300–03; *Lopez*, 373 U.S. at 437–40.
[31] *Lopez*, 373 U.S. at 465 (Brennan, J., dissenting).
[32] *Hoffa*, 385 U.S. at 302.
[33] 425 U.S. 435 (1976).
[34] *Id.* at 440.
[35] 385 U.S. at 302.
[36] *Miller*, 425 U.S. at 437.
[37] *Id.* at 440.
[38] *Id.* at 442.
[39] *Id.*
[40] *See id.* at 443.

When the *Smith v. Maryland* Court asserted that individuals have no privacy interest in the information they voluntarily reveal to third parties, the Court cited *Miller* alongside *Hoffa* and *Lopez*.[41] As in *Miller*, the *Smith* Court focused on the content of the records at issue—in this case, a list of phone numbers the defendant had dialed.[42] The majority also hearkened back to *Katz v. United States* to ask if the defendant could have had a "reasonable expectation of privacy"[43] in the phone company's records.[44] The Court said, "[I]t is important to begin by specifying precisely the nature of the state activity that is challenged . . . . a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications."[45] The Court went on to say that the defendant's argument "rests upon a claim that he had a 'legitimate expectation of privacy' regarding the numbers he dialed on his phone."[46] With this statement, the Court followed the reasoning present in *Miller* and backed away from the suggestion that *any* information shared with a third party could be utilized by the government. The Court instead formed the narrower conclusion that because the defendant voluntarily shared his dialing information with the phone company, *and* because he could not have had a reasonable expectation of privacy in something as minimal as "the numbers he dialed on his phone,"[47] the police could access the defendant's calling records without a warrant.[48]

### *B. Congressional Reactions to the Third Party Exception*

After *United States v. Miller* and *Smith v. Maryland* Congress passed legislation to provide some protection for consumers' financial records and to regulate law enforcement's use of pen registers.[49] The Pen Register Act was part of The Electronic Communications Privacy Act of 1986 (ECPA), which followed the content versus non-content divide suggested by *Smith.*[50] Title II of the ECPA is the Stored Communications Act (SCA),[51] which is relevant in cases today that deal with the third party exception in the context

---

[41] Smith v. Maryland, 442 U.S. 735, 744 (1979).

[42] *Id*. at 741.

[43] 389 U.S. 347, 360 (1967) (Harlan, J., concurring). In *Katz*, the Court held that the defendant had a reasonable expectation of privacy in the contents of his phone call (despite being in a public phone booth), and the conversation was therefore entitled to protection under the Fourth Amendment. *See id.* at 351.

[44] *Smith*, 442 U.S. at 743.

[45] *Id.* at 741 (emphasis in original). A pen register is a mechanical device used to track the outgoing numbers dialed on a single line. *Id.* at 736 n.1.

[46] *Id.* at 742.

[47] *Id.*

[48] *Id.* at 745–46.

[49] Right to Financial Privacy Act, 12 U.S.C. §§ 3401–3422 (2012); Pen Register Act, Pub. L. No. 99–508, § 301(a), 100 Stat. 1848, 1868–72 (1986) (codified as amended at 18 U.S.C. §§ 3121–3127 (2012)).

[50] *See e.g.*, 18 U.S.C. § 2703(b)–(c) (2012).

[51] Stored Communications Act, Pub. L. No. 99–508, § 201, 100 Stat. 1848, 1860–68 (1986) (codified as amended at 18 U.S.C. §§ 2701–2711 (2012)).

of e-mail and other online communications.[52] Unfortunately, since the Act was written before the creation of the modern-day internet, the protections are a bad fit for how individuals currently interact online.[53] While e-mails stored for 180 days or less require a warrant to access,[54] the SCA states that opened e-mails stored for longer than 180 days can be accessed by a government official with an administrative subpoena, a grand jury subpoena, a trial subpoena, or a court order.[55] These all are easier to get than a traditional warrant,[56] with a court order only requiring that an official show "reasonable grounds to believe that the contents . . . are relevant and material to an ongoing criminal investigation."[57] The Act requires the official to give notice to the person being investigated, but this notice can be significantly delayed.[58]

Congress has also provided some additional safeguards for specific types of information held by third parties. The Cable Act of 1984 protects subscribers from government intrusion into their viewing habits.[59] In 2001, Congress specifically authorized rules from the Department of Health and Human Services to protect personal health information.[60] However, these and other legislative protections are relatively limited[61] and have been undone in part by other statutes such as Section 215 of the PATRIOT Act.[62] As courts and legal scholars grapple with the third party exception, *Smith v. Maryland* and related Supreme Court cases continue to provide the relevant framework for the discussion.[63]

## II. Current Application of the Third Party Exception

Law enforcement officers are able to acquire many of the digital breadcrumbs described in the introduction without a warrant. Tech companies routinely hand over e-mail account information, including where a user is

---

[52] *See, e.g.*, Ehling v. Monmouth-Ocean Hospital Service Corp., 961 F. Supp. 2d 659, 664–67 (D.N.J. 2013).

[53] *See id.* at 666.

[54] 18 U.S.C. § 2703(a) (2012).

[55] Cate, *supra* note 3, at 463.

[56] *Id.*

[57] 18 U.S.C. § 2703(d) (2012).

[58] *See* 18 U.S.C. § 2705 (2012). Notification can be delayed by ninety days, with indefinite ninety-day extensions available by court order, as long as notification would seriously jeopardize an investigation or unduly delay a trial. 18 U.S.C. 2705(a); 18 U.S.C. 2705(b)(5) (2012).

[59] 47 U.S.C. § 551(c)(2)(D) (2012).

[60] Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462 (2000) (codified at 45 C.F.R. pt. 164, §§ 164.502, 164.506).

[61] *See* Cate, *supra* note 3, at 468, calling the HHS rules only "facially restrictive" and downplaying the significance of other congressional actions.

[62] Section 215 allows the FBI to acquire court orders compelling the production of "any tangible things" relevant to certain counterterrorism investigations. Michael J. Woods, *Counterintelligence and Access to Transactional Records: A Practical History of USA PATRIOT Act Section 215*, 1 J. Nat'l Security L. & Pol'y 37 (2005).

[63] *See, e.g.*, Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561, 601 (2009).

located and whom she has e-mailed over the years.[64] Courts have differed on the use of cell tower information to locate individuals,[65] but the Fifth Circuit recently confirmed that months of historical cell site location data can be acquired with only a court order,[66] despite the increasing accuracy of the technology.[67] The standard for these orders is the same as the orders for e-mails over 180 days old: an officer must have "reasonable grounds to believe that the contents . . . are relevant and material to an ongoing criminal investigation."[68] Law enforcement officers are able to subpoena consumers' financial records, though the Right to Financial Privacy Act requires the consumer be notified.[69] Recently, a Department of Justice document surfaced suggesting that officers may frequently follow up their subpoenas for financial records with a court order for non-disclosure, thus thwarting the Act's protections.[70]

Not all companies are willing to follow the dictates of the third party exception and the SCA. Google and Yahoo have stated that they require warrants for the contents of any e-mail messages or user documents stored in the cloud.[71] This goes against the provision in the SCA that explicitly allows the government access to opened e-mails over 180 days old, and which could logically be extended to cover documents stored in the cloud for over 180 days. Google has said it believes its position is supported by the Fourth Amendment,[72] and at least one circuit court has agreed. In *United States v. Warshak*, the Sixth Circuit analogized e-mails to letters and internet service providers to post offices.[73] The court stated that "it would defy common sense to afford e-mails lesser Fourth Amendment protection" than traditional letters,[74] and "to the extent that the SCA purports to permit the government to obtain such e-mails warrantlessly, the SCA is unconstitutional."[75] The

---

[64] *See* David Kravets, *Google Tells Cops to Get Warrants for User E-Mail, Cloud Data*, WIRED (Jan. 23, 2013, 5:29 PM), http://www.wired.com/threatlevel/2013/01/google-says-get-a-warrant/.

[65] *See* Michael T.E. Kalis, *Ill Suited to the Digital Age: Fourth Amendment Exceptions and Cell Site Location Information Surveillance*, 13 U. PITT. J. TECH. L. & POL'Y 1, 17 (2013).

[66] *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 609 (5th Cir. 2013).

[67] *See* Kalis, *supra* note 65, at 4–5. Cell phones constantly communicate with cell towers to make sure the phone has the best possible signal. By using information from overlapping towers, cell phone providers can locate a phone with almost the same accuracy as a GPS. *Id.*

[68] 18 U.S.C. § 2703(d) (2012).

[69] 12 U.S.C. § 3405(2) (2012); 12 U.S.C. § 3407(2) (2012).

[70] *See* Tim Chen, *Is the Government Tracking Your Credit Card Purchases?*, FORBES (Jan. 26, 2011, 3:10 PM), http://www.forbes.com/sites/moneybuilder/2011/01/26/is-the-government-tracking-your-credit-card-purchases/.

[71] Kravets, *supra* note 64; David Kravets, *Yahoo, Like Google, Demands Warrants for User E-mail*, WIRED (Jan. 25, 2013, 4:59 PM), http://www.wired.com/threatlevel/2013/01/yahoo-demands-warrants/ [hereinafter *Yahoo, Like Google*].

[72] Kravets, *supra* note 64.

[73] 631 F.3d 266, 286 (6th Cir. 2010).

[74] *Id.* at 285–86.

[75] *Id.* at 288.

companies have not been sued by federal agencies for their practices,[76] but rather a Department of Justice official told Congress last year that "[t]here is no principled basis to treat e-mail less than 180 days old differently than e-mail more than 180 days old."[77] Nevertheless, the contents of old e-mails remain officially available to law enforcement without a warrant, as Congress has not yet updated the relevant SCA provisions.[78]

The status of many potentially revealing online activities, such as an individual's web browsing history, have not yet been determined.[79] By one district court's count, the third party exception has been used to support law enforcement's acquisition of: "(1) bank records; (2) credit card statements; (3) kilowatt consumption from electric utility records; (4) motel registration records; (5) cell phone records; and (6) employment records."[80] Notably absent from the list is any content personally created by the individual. Law enforcement officers can access records of an individual's actions as recorded by third parties, but the content versus non-content divide suggested by *Smith v. Maryland* persists.

The most prominent current application of the third party exception is the National Security Agency's (NSA) mass surveillance of phone calls in the United States and abroad.[81] In one declassified opinion from the Foreign Intelligence Surveillance Court (FISC), the judge stated that *Smith v. Maryland* "remains controlling" in regards to government acquisition of non-content telephony metadata,[82] despite the massive scale and duration of the NSA's surveillance.[83]

Not all courts have accepted this reasoning. Recently, in *Klayman v. Obama*,[84] a D.C. district court judge concluded, "I cannot possibly navigate these uncharted Fourth Amendment waters using as my North Star a case that predates the rise of cell phones."[85] Judge Leon reasoned that *Smith* did not control because the quantity of information available today and the gov-

---

[76] Kravets, *Yahoo, Like Google*, *supra* note 71.

[77] Timothy B. Lee, *Eric Holder Endorses Warrants for E-mail. It's About Time*., WASH. POST (May 16, 2013, 4:46 PM), http://www.washingtonpost.com/blogs/wonkblog/wp/2013/05/16/eric-holder-endorses-warrants-for-e-mail-its-about-time/.

[78] Julian Hattem, *Spy Chief Outlines Hopes for Cybersecurity Bill*, THE HILL (Mar. 4, 2014, 3:20 PM), http://thehill.com/blogs/hillicon-valley/technology/199862-spy-chief-outlines-hopes-for-cybersecrity-bill.

[79] Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2110 (2009).

[80] United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156, at *8 (N.D. Ga. Apr. 21, 2008) (citations omitted).

[81] *See* 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.

[82] *See In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [redacted], No. BR 13-158, 5 (FISA Ct. Oct. 11, 2013).

[83] *See id.* at 2.

[84] 957 F. Supp. 2d 1 (D.D.C. 2013).

[85] *Id.* at 37.

ernment's ability to utilize that information have vastly increased.[86] He went on to cite the "mosaic theory" from *United States v. Maynard*[87]: "Records that once would have revealed a few scattered tiles of information about a person now reveal an entire mosaic—a vibrant and constantly updating picture of the person's life."[88] The mosaic theory posits that if the government has acquired and analyzed so much legally obtainable data about an individual that the information creates a comprehensive "mosaic" of that person's life, then that individual's Fourth Amendment rights have been violated.[89] The theory is attractive in many ways but potentially difficult to implement, as will be explored later in Part III.

## III. Pursuing Alternatives to the Current Third Party Exception

### *A. Problems with the Current Version of the Exception*

The holding of *Smith v. Maryland* is often simplified down to the single line: "[t]his Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[90] This reading ignores the work the Court did in *Smith* and *Miller* in minimizing the significance of the records attained by law enforcement.[91] Content was not left out incidentally—the Court went out of its way to distinguish the phone numbers at issue in *Smith* from the recorded conversation in *Katz*.[92] The *Smith* Court was likely attracted to the content versus non-content divide in part because it aligned nicely with the existing jurisprudence on letters.[93] Additionally, the amount of information the government could glean from non-content information was minimal compared to how

---

[86] *See id.* at 36.

[87] 615 F.3d 544, 561–62 (D.C. Cir. 2010). *Maynard* later became the Supreme Court case United States v. Jones, 132 S. Ct. 945 (2012). Both cases focused on police using a GPS tracker on the defendant's car for thirty days without a valid warrant. 615 F.3d at 555; 132 S. Ct. at 948.

[88] *Klayman*, 957 F. Supp. 2d at 36.

[89] *Maynard*, 615 F.3d at 562–63.

[90] Smith v. Maryland, 442 U.S. 735, 743–44 (1979). Justice Sotomayor did this in her otherwise powerful concurrence in *Jones*, stating "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

[91] *See Smith*, 442 U.S. at 741–43; United States v. Miller, 425 U.S. 435, 440–42 (1976).

[92] The Court emphasized why the two cases were different: "a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications." *Smith*, 442 U.S. at 741 (emphasis in the original). The Court made the divide clear again two pages later: "[a]lthough petitioner's conduct may have been calculated to keep the *contents* of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed." *Id.* at 743 (emphasis in original).

[93] *Ex parte Jackson* held that there was no privacy interest in the routing information on an envelope, but there was a privacy interest in the letter inside the envelope. 96 U.S. 727, 733 (1877).

the data might be analyzed today.[94] Lastly, the divide partially defined the vague "reasonable expectation of privacy" standard established in *Katz*.[95]

The modern applications of the third party exception are troubling to the extent that they ignore the content versus non-content divide and thereby potentially broaden the third party exception.[96] Even when courts are mindful of the divide, it is increasingly insufficient for determining what a reasonable expectation of privacy might be. Americans were shocked by the NSA scandal because they did not expect that the sum of their calling records could be legally collected by a federal agency.[97] Was their expectation unreasonable, given the holding in *Smith*? The FISC opinion authorizing the NSA's collection activities suggests that it was.[98] However, when *Smith* was decided, it was against the background of 1970s policing and telecommunications technology. Today, law enforcement pushes on the limits of the third party exception by collecting millions of pieces of telephony metadata each day[99] and putting in over a million requests a year for cell site location information (CSLI).[100] This scale of collection, as well as what analysts and law enforcement officers can do with the data,[101] could not have been imagined in 1979. The difference between where technology stood in 1979 and where it stands today may simply be too much for the standard to bear.[102]

*Smith* and its related preceding cases relied on the fact that the defendants "voluntarily" turned over their information to a third party.[103] However, as Justice Marshall noted in his *Smith* dissent, there was little "voluntary" about the defendant's actions. If the defendant wanted to call someone, he would necessarily have to share the phone number with the phone company. Justice Marshall saw this fact as undercutting the "voluntary" nature of the defendant's actions: "It is idle to speak of 'assuming'

---

[94] For an example of what the government can do with metadata, see, for example Kashmir Hill, *Here's a Tool to See What Your Metadata Reveals About You*, FORBES (July 10, 2013), http://www.forbes.com/sites/kashmirhill/2013/07/10/heres-a-tool-to-see-what-your-e-mail-metadata-reveals-about-you/.

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

[96] *See*, *e.g.*, *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 620 (5th Cir. 2013).

[97] *See*, *e.g.*, Timothy B. Lee, *Everything You Need to Know About the NSA's Phone Records Scandal*, WASH. POST (June 6, 2013, 3:45 PM), http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/06/everything-you-need-to-know-about-the-nsa-scandal/.

[98] *See In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [redacted], No. BR 13-158, 5 (FISA Ct. Oct. 11, 2013).

[99] Greenwald, *supra* note 81.

[100] Kalis, *supra* note 65, at 5.

[101] For example, police often request CSLI for a particular tower, acquiring the number of every user who communicated with a tower at a particular time, in order to do "dragnet surveillance" to figure out who in the area might have been involved with a crime. *Id.* at 7.

[102] *See* Klayman v. Obama, 957 F. Supp. 2d 1, 31 (D.D.C. 2013) (concluding that the differences between a pen register and the NSA's Bulk Telephony Metadata Program are too large to continue using *Smith v. Maryland*).

[103] Smith v. Maryland, 442 U.S. 735, 744 (1979); *see also* United States v. Miller 425 U.S. 435, 442 (1976); Hoffa v. United States, 385 U.S. 293, 413 (1966).

risks in contexts where, as a practical matter, individuals have no realistic alternative."[104]

The question of what we voluntarily share has grown murkier over time. The defendant in *Smith* was at least aware that he was punching in numbers so that the phone company could connect his call. The average person browsing the web may not be aware that she possesses an IP address, much less that she is "voluntarily" sharing her IP address with each website she visits,[105] or that law enforcement officers could trace her IP address back to her exact physical location.[106] Courts have debated this question in relation to CSLI, with the Third Circuit concluding, "A cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way."[107] The Fifth Circuit disagreed, noting that all cell phone customers know they need to connect to a cell tower to make a call, and their terms of service agreements mention that providers save customers' location information.[108] This explanation strains the meaning of the word "voluntary." As technology advances, the gap will grow larger between the information that a third party can acquire and the information that individuals are actually cognizant of sharing.[109]

Given Congress' recent lack of productivity,[110] it seems unlikely that the legislative branch will step in to reshape the third party exception any time soon. At the same time, consumers are doing an increasing amount of business online,[111] making more information available to third parties than ever before.[112] Particularly as companies and individuals increasingly turn to cloud computing,[113] putting even more information into the hands of third parties, the judiciary should revisit the third party exception sooner rather than later.

---

[104] *Smith*, 442 U.S. at 750 (Marshall, J., dissenting).

[105] *See* Michael Horowitz, *What Does Your IP Address Say About You?*, CNET (Sept. 15, 2008, 6:31 PM), http://news.cnet.com/8301-13554_3-10042206-33.html.

[106] *Id.*

[107] *In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317 (3d Cir. 2010).

[108] *See In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 613 (5th Cir. 2013).

[109] *See, e.g.*, Alyssa Newcomb, *Facebook Users Unwittingly Share More Personal Information, Study Finds*, ABC WORLD NEWS (Mar. 6, 2013), http://abcnews.go.com/Technology/facebook-lead-users-reveal-personal-information-study-finds/story?id=18667855.

[110] *See, e.g.*, Matt Viser, *This Congress Going Down as Least Productive*, BOSTON GLOBE (Dec. 4, 2013), http://www.bostonglobe.com/news/politics/2013/12/04/congress-course-make-history-least-productive/kGAVEBskUeqCB0htOUG9GI/story.html.

[111] *See* Betsy Morris, *More Consumers Prefer Online Shopping*, WALL ST. J. (June 3, 2013), http://online.wsj.com/news/articles/SB10001424127887324063304578523112193480212.

[112] Consumers happily receive deals based on their location information and transaction history. *Id.* They also are increasingly making in-person purchases with debit and credit cards instead of cash, providing their credit card companies with a more complete purchasing history than ever before. *See* JAVELIN STRATEGY & RESEARCH, RETAIL POINT OF SALE FORECAST 2012–2017 (June 2012) https://www.javelinstrategy.com/brochure/251.

[113] *See* Quentin Hardy, *Google Joins a Heavyweight Competition in Cloud Computing*, N.Y. TIMES, Dec. 3, 2013, at B1.

### *B. Underlying Considerations for Updating the Third Party Exception*

Justice Sotomayor stated in *United States v. Jones* that she would not assume "all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."[114] She quoted Justice Marshall's dissent in *Smith*, where he expressed the same sentiments: "Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."[115]

Justice Marshall's and Justice Sotomayor's opinions point to a need for a zone of information that is not "secret" but is still considered "private" and therefore protected under the Fourth Amendment. This zone should not exclusively consist of information that is easily identifiable as "content," as the content versus non-content divide in *Smith* suggests. What "content" is can be unclear, given the existence of data like URL addresses, which are ostensibly non-content routing information but can easily expose the content an individual is viewing, e.g., http://www.meetup.com/bostonsocialists/messages/boards/. What exactly the "private but not secret" zone should include will be a defining feature for any alternative version of the third party exception.

Another important consideration in reshaping the exception is how we treat the "reasonable expectation of privacy" test introduced in *Katz*.[116] The Court has explained over time what expectations of privacy our society considers "reasonable," largely on a case-by-case basis.[117] Research indicates that the Court's estimations may be a poor corollary to what information Americans actually expect to be private.[118] Our expectations of privacy will likely continually change with technology—we may not like seeing ads that reflect the content of our e-mails, but at this point we cannot say that we expect our e-mail contents to be private, at least as far as Google's algorithms are concerned. In reshaping the third party exception, we must consider whether we prefer a static standard based on our current beliefs about privacy, or a dynamic standard like *Katz's* "reasonable expectation of privacy"[119] that can adjust over time to society's evolving expectations.

---

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

[115] *Id.* (quoting Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting)).

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

[117] *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, 732–33 (1993).

[118] *See id.* at 732. The authors did a study of what law enforcement practices Americans believe to be the most and least intrusive. Survey participants believed the use of informants to be on a par with warrantless (illegal) searches of their cars, and tended to draw no distinction between a police dog sniffing them (not considered a legal search) and a policeman frisking them (a search). *See id.* at 740–41.

[119] 389 U.S. at 360 (Harlan, J., concurring).

### *C. Alternative Versions of the Third Party Exception*

The subsections below offer alternatives to the content versus non-content divide in *Smith*.[120] In all alternatives, any information that does not require a warrant would at minimum require an administrative subpoena, preserving the historical standard from the SCA that was enacted in response to *Smith*.[121] Not including such a requirement would allow for unchecked police power that is out of step with current statutory protections.[122]

#### 1. *Information from Private Accounts Stays Private*

In *Ehling v. Monmouth-Ocean Hospital Services*, the court held that information on a Facebook wall was private because of the privacy settings the defendant had selected.[123] This arguably comports with most Americans' view of privacy—if an individual sets a password or selects a privacy setting for her account, then she expects the information in that account to stay private. *Katz* implicitly endorsed the view that private transactions can lead to a reasonable expectation of privacy when it explained how phone booths were used: "One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[124] It is the physically protected element of the phone booth, as well as paying the phone company for the privilege of making a call, that led to the reasonable expectation of privacy in a phone booth. Similarly, an individual who signs up for a private account, and then uses that account to patronize the company, can reasonably expect that any information she exposes to the company will remain private.

This version of the third party exception would obviously upset a number of statutes and existing law enforcement practices.[125] Police could still pursue their own monitoring of individuals via GPS or other means and utilize individual informants, but they could not rely on third party companies as they do now without first acquiring a warrant.

This standard would benefit individuals by making their privacy rights clearer.[126] It would also likely disproportionately benefit educated individuals and criminals who were diligent about altering privacy settings for any

---

[120] 442 U.S. at 741.

[121] 18 U.S.C. § 2703(d) (2012).

[122] *See* Cate, *supra* note 3, at 462–68.

[123] 961 F. Supp. 2d 659, 662–63 (D.N.J. 2013). The court relied on the applicable portions of the SCA, and on how Facebook accounts are set up, with different privacy options available for users to choose from. *Id.* The defendant had chosen to make her Facebook wall visible only to her Facebook friends. *Id.*

[124] 389 U.S. at 352.

[125] *See*, *e.g.*, 18 U.S.C. § 2703 (2012); 18 U.S.C. § 3123 (2012).

[126] By contrast, right now if an individual wants to know if the government can potentially read one of her e-mails, she has to see where she stored the e-mail, how long it has been stored there, and if she opened it already or not. *See* 18 U.S.C. § 2703(a) (2009).

accounts that might otherwise publicly share information by default.[127] Nevertheless, the protections would be broad enough to capture a wide variety of activities engaged in by people across the economic spectrum.[128] This alternative would also have the advantage of being somewhat flexible as society's conception of a "reasonable expectation of privacy"[129] continues to evolve.

One problem with this standard is that it would be disproportionately affected by how companies set up their business models. Financial accounts would obviously create privacy protections for consumers, but what about a rewards card from a supermarket, or situations where a business sells customer information to other companies? Privacy protections could vary from business to business, with the profit motive driving the privacy determination, rather than the courts driving the standard on society's behalf.

Some information would fall into a gray area under this model, notably an individual's web browsing history. Your internet service provider (e.g., Comcast, Verizon) logs what websites you connect to,[130] but to what extent is your account private? Does it hinge on whether your provider asks you questions to verify your identity when you call it for technical support? If a law enforcement officer wants to ask Google about searches conducted from a particular IP address, will the privacy of those searches hinge on whether the person happened to be searching while logged into their Gmail account or not?

While these questions would provide a challenge for the courts to answer, it is a more relevant range of questions than is created by the unwieldy content versus non-content divide in the current version of the third party exception. Except in the most obvious cases (e.g., the contents of a sealed letter vs. the address on the envelope), individuals' privacy expectations are not based on the content versus non-content categorization of the information they are revealing. Americans' expectations of privacy derive from the circumstances under which they reveal information, such as what type of individual or company they are sharing information with and if they have selected any privacy settings. "What makes a private account private?" is therefore a more useful question for courts to answer than the increasingly unclear question, "What is content?"[131]

---

[127] *FAQs About Vine*, TWITTER, http://support.twitter.com/articles/20170317-faqs-about-vine (last visited Apr. 13, 2013).

[128] For example, worldwide, 85% of people have e-mail accounts and 62% use social media. Patricia Reaney, *Most of World Interconnected Through E-mail, Social Media*, REUTERS (Mar. 27, 2012), http://www.reuters.com/article/2012/03/27/net-us-socialmedia-online-poll-idUSBRE82Q0C420120327.

[129] *Katz*, 389 U.S. at 360 (Harlan, J., concurring).

[130] Lincoln Spector, *Is Your ISP Spying on You*?, PC World (Sept. 3, 2012, 7:42 AM), http://www.pcworld.com/article/261752/is_your_isp_spying_on_you_.html.

[131] *See supra* text accompanying notes 114–116.

### 2. *Unknowingly Shared Information Stays Private*

Professor Orin Kerr argues that the third party exception should not be understood as an application of the "reasonable expectation of privacy" standard from *Katz*[132] but rather as a form of consent.[133] As noted above in Section A, an individual can easily "voluntarily" share information with a third party today without actually being aware she has chosen to share something. The third party exception could be reshaped to focus on the consent element and only protect information an individual was unaware she was sharing.

This alternative has the advantage of preventing a certain amount of unfair surprise. The police could not use cell site location data against an individual when she did not know she was sharing her location information with her cell phone service provider. Additionally, this alternative aligns with the "caveat emptor" mentality that has been part of American culture for a long time.[134] If someone has knowingly shared information with a third party, it is arguably reasonable for her to assume that party may share her information with someone else.[135] This alternative also has the benefit of being flexible to technological advances (no matter how much our devices quietly report about us, we will remain protected),[136] and it is adjustable according to what society determines to be a reasonable expectation of privacy. The courts could utilize a "reasonable person" standard when weighing a defendant's claim that she was unaware of sharing a given piece of information, so that a defendant could not claim to be ignorant of every aspect of modern technology. For many types of data, broad rules could be applied—for example, it is hard to imagine a person who is unaware that her credit card company tracks her purchases. For many other types of data, such as IP addresses, the standard would create an increased administrative burden, as courts would need to determine if a particular person realized she was sharing a more obscure type of data or not.

This version of the third party exception has the substantial disadvantage of eliminating some current privacy protections. It would be hard for a

---

[132] 389 U.S. at 360 (Harlan, J., concurring).

[133] Kerr, *supra* note 63, at 588. Orin Kerr is a leading expert in privacy and technology. *See* Library of Cong., *Orin Kerr Named Scholar in Residence at Law Library of Cong.* (June 6, 2012), http://www.loc.gov/today/pr/2012/12-119.html.

[134] *See* CAPITALISM, CULTURE, AND ECONOMIC REGULATION 67–70 (Leigh Hancher & Michael Moran eds., 1989).

[135] This thinking comports with the simplified version of *Smith*'s holding that there is "no legitimate expectation of privacy in information he voluntarily turns over to third parties." Smith v. Maryland, 442 U.S. 735, 743–44 (1979). It also reflects the statement from *Katz*: "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." 389 U.S. at 351.

[136] Apple requests all new iPhone users "help improve the iOS" by setting their phones to automatically "occasionally provid[e] diagnostic and usage information." *iOS: Providing Apple with Diagnostics and Usage Information*, APPLE (Apr. 11, 2012), http://support.apple.com/kb/HT4305. Apple does not specify what exact information it collects, though it purports to collect the information anonymously. *Id.*

defendant today to argue that she was unaware she was sharing her e-mails with Google, particularly in the face of targeted advertising based on her e-mail content.[137] Without the content versus non-content divide, all e-mail content could therefore be immediately accessible to law enforcement (setting aside Google's and Yahoo's current flouting of the SCA).[138] Any other types of future communication that are clearly stored on a company's servers would similarly be immediately vulnerable to a subpoena or a court order, though the contents of phone calls would likely still be protected, since telecommunications providers cannot routinely tap phone conversations.[139]

Law enforcement would benefit from this immediate access to content, and their use of informants would be unaffected. However, officers would lose access to information the public is largely unaware of, such as the location information embedded in smart phone photos.[140] Additionally, law enforcement officers might frequently feel pressured to go the safer route of getting a warrant, in case a defendant could successfully argue in court that she was unaware she had shared some type of semi-obscure data. Lastly, this standard could create a perverse incentive for law enforcement to advertise what information individuals are regularly sharing with third parties (perhaps in the guise of a cyber-safety campaign) in order to maximize the amount of information they can argue individuals had "voluntarily" shared.

3. *The Mosaic Theory*

The mosaic theory was presented in the D.C. Circuit case *United States v. Maynard*, the case that later became *United States v. Jones* before the Supreme Court. The D.C. Circuit observed that the "privacy interest in a whole" could be greater than the privacy interest in individual pieces of information, if the whole created "an intimate picture" of a defendant's life.[141] The court described how this picture could be formed solely based on prolonged GPS monitoring: "A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts."[142] Based on this reasoning, the

---

[137] *See* Mitchell, *supra* note 1.

[138] *See supra* text accompanying notes 71–78.

[139] The Wiretap Act requires a "super" search warrant to record live phone conversations. *See* Cate, *supra* note 3, at 464.

[140] Many smartphones are automatically set to record location information and embed it in photos. *See* Melissa Ulbricht, *How to Remove Location Information from Mobile Photos*, PBS (Feb. 28, 2011), http://www.pbs.org/idealab/2011/02/how-to-remove-location-information-from-mobile-photos055/.

[141] United States v. Maynard, 615 F.3d 544, 561–62 (D.C. Cir. 2010), *rev'd sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

[142] *Id.* at 562.

*Maynard* court held that the continuous month-long GPS monitoring at issue was a Fourth Amendment search.[143]

*United States v. Jones* was decided on much narrower grounds,[144] but the five concurring justices in *Jones* indicated that they may be interested in signing on to the mosaic theory in future Fourth Amendment cases.[145] Professor Kerr has noted that this is a fundamentally different way of approaching the Fourth Amendment.[146] Courts have traditionally determined whether an unlawful search[147] has occurred by looking at each individual step in a police action.[148] It is a major change to examine an officer's actions as a "collective sequence"[149] rather than as multiple discrete steps. Professor Kerr notes that the mosaic theory would result in certain law enforcement methods sometimes being counted as a search, sometimes not.[150] The approach raises the questions: "What test determines when a mosaic has been created? Which surveillance methods prompt a mosaic approach? Should courts group across surveillance methods? If so, how? What is the half-life of a mosaic search?"[151]

Professor Christopher Slobogin tried to answer some of these questions by formulating a statutory version of the mosaic theory.[152] Professor Slobogin proposed a time-based approach, following Justice Alito's sense in *Jones* that at some point in time, an acceptable law enforcement technique can become unacceptable without a search warrant.[153] For data searches, Professor Slobogin proposed that a warrant should be required for any search of a third party's data that reveals an individual's activities over a period longer than forty-eight hours.[154] While this approach would greatly enhance privacy protections for certain types of data, there are many types of sensitive information about a person that are not tied to a specific time period, e.g., sexual orientation, political affiliation, marital status, etc.

The mosaic theory is appealing because it allows judges to exercise some control over technology. We would not need to worry about courts or the legislature setting a technological standard that would soon become obsolete—judges could intuitively decide when too much information had been revealed. The theory has not yet been applied in any fleshed-out form,

---

[143] *Id.* at 568.
[144] *Jones*, 132 S. Ct. at 949 (2012).
[145] *See id.* at 955 (Sotomayor, J., concurring); *see also id.* at 964 (Alito, J., concurring).
[146] Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313 (2012).
[147] The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." *See* U.S. CONST. amend. IV.
[148] Kerr, *supra* note 146, at 312.
[149] *Id.* at 313.
[150] *Id.* at 344.
[151] *Id.* at 329.
[152] Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y 1, 17–32 (2012).
[153] United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring).
[154] Slobogin, *supra* note 152, at 28.

although lower courts have already echoed the sentiments of the *Jones* concurrences.[155]

The mosaic theory is inherently problematic as a basis for revising the third party exception. It does not outline what third-party-held information is private, or what information is accessible to law enforcement officers without a warrant. It is inherently contextual—you could have two very large pieces of information about a person's life, and not form a mosaic. Alternatively, you could employ a data aggregator to collect only the most public pieces of that person's life and gain a very clear picture of their connections and activities.[156] Therefore, any attempt to further define the theory runs into significant difficulties.

The theory may best be utilized as an alternative to *Katz's* "reasonable expectation of privacy" standard.[157] Just as the Court has fleshed out which types of third-party-held information retain a privacy interest under *Katz*,[158] the Court could explore what types of investigative practices can violate an individual's Fourth Amendment rights by creating a mosaic of her life. For example, physically tailing a suspect could be allowed indefinitely, since it is naturally limited by the cost and resources involved, but cheap GPS monitoring longer than two weeks could be banned. This approach would prove undesirable if the number of investigative techniques outnumbered the different types of data held by third parties, in which case *Katz* would provide the more useful standard. This application of the mosaic theory would also tend to tie law enforcement to older, less efficient investigative techniques that provide a smaller amount of information about suspects. Lastly, there would likely be separation of powers and federalism concerns if the federal courts took an active role in instructing state officers in precisely how they are permitted to carry out their investigative duties.

4. *Information Shared at Home Stays Private*

This alternative would be firmly grounded in the Fourth Amendment,[159] and it would follow Supreme Court cases like *Kyllo*[160] by drawing a clear privacy line at the defendant's front door. However, this option would be virtually impossible to implement today. Internet service providers (ISPs) can identify a subscriber's home connection,[161] but school-wide networks where a student may have the same IP address in her dorm room and in her

---

[155] *See*, *e.g.*, Montana State Fund v. Sims, 270 P.3d 64, 70 (Mont. 2012) (Nelson, J., specially concurring) (stating that the government cannot use hidden cameras to track individuals' every move throughout the day for an extended period of time).

[156] *See supra* text accompanying notes 11–18.

[157] Katz v. United States, 389 U.S. 347, 360 (Harlan J., concurring).

[158] *See* Slobogin, *supra* note 117, at 732.

[159] The home is the one location specified in the Fourth Amendment: "[t]he right of the people to be secure in their persons, houses, papers, and effects." U.S. CONST. amend. IV.

[160] Kyllo v. United States, 533 U.S. 27, 40 (2001) (using devices "not in general public use" like thermal imaging to look inside the home constitutes a Fourth Amendment search).

[161] *IP 101: The Basics of IP Addresses*, WHATISMYIPADDRESS.COM, http://whatismyipaddress.com/ip-basics (last visited April 14, 2014).

classroom would pose difficulties. Credit card companies may be able to tell an online purchase from an in-store purchase, but they would then need to coordinate with ISPs to determine if the online purchase was made from home or from a public location, before separating out which records they could provide to law enforcement.

If technology advanced to the point where all activities could be easily tracked to a precise location, this standard could provide enhanced privacy protections to individuals. All content and non-content information shared at home would require a warrant, and the standard could readily apply to all new technologies, as long as a third party company was capable of acting as a gatekeeper for government requests. It would be an easy standard for individuals to understand, and it would align with the Fourth Amendment's singling out of the home as the one location individuals are most protected from warrantless searches.[162] There is also already a public awareness that online activities performed at work or on a public wireless network may not be as private as internet activity at home.[163]

Unlike the other alternatives explored above, this standard would not allow for any shifting of what constitutes a reasonable expectation of privacy. Law enforcement would have a clear line for what they could access without a warrant, although unfortunately that line could also be readily exploited by criminals. The sheer amount of criminal activity that could be conducted remotely from an individual's home is enough to make this standard undesirable. Additionally, innocent individuals would lose many of their current privacy protections any time they stepped outside their homes. This sharp divide does not reflect how individuals share information today (that is to say, on their phones, everywhere they go), making a purely location-based privacy standard impracticable going forward.

## IV. Conclusion

The above alternatives all contain different determinations of how far the protections of the Fourth Amendment should extend. It would be disingenuous to choose one alternative as the "best" option going forward, when all of them represent different policy judgments. They also all contain their own administrative challenges, with the implementation problems inherent to the mosaic theory appearing the most daunting in the long run.

The first alternative, "Information from Private Accounts Stays Private," strikes the strongest balance in favor of greater privacy protections. If you have an account with a third party, whether that account contains thousands of pages of your most intimate thoughts, or just a short list of

---

[162] U.S. Const. amend. IV.

[163] *See* Allison Linn, *Big Brother May Not Be Watching, but Your Employer Probably Is*, CNBC (May 16, 2013, 12:56 PM), http://www.cnbc.com/id/100743693; *see also Dangers of Free Public Wifi*, CBS News (July 8, 2010, 10:29 AM), http://www.cbsnews.com/news/dangers-of-free-public-wifi/.

phone numbers, the first alternative prevents access to that information without a warrant. This approach reflects the average American's reasonable expectations of privacy in dealing with private companies.[164] Large corporations should not be treated as legally equivalent to an untrustworthy friend; we simply do not approach friends and corporations with remotely similar expectations. There is reason to be concerned about the amount of power this alternative puts into the hands of private companies, as they largely define the parameters of their customer relationships, but the risk inherent to the standard is arguably preferable to the less protective version of the third party exception currently in effect.

It is important not to minimize the importance of the third party exception to law enforcement. Learning the names of a criminal's associates from her e-mail or telecommunications provider is a valuable tool for uncovering criminal networks. Professor Kerr makes a compelling argument that the third party exception is a necessary tool to prevent criminals from substituting the public aspects of their crimes with private transactions.[165] However, we have always had to strike a balance between privacy and security.[166] *Smith v. Maryland* struck a balance for where things stood in 1979. Given all the technological developments since then, that balance has been disrupted.[167] As Justice Brandeis observed in his dissent in *Olmstead v. United States*, we must read our constitutional protections as having a "capacity of adaptation to a changing world."[168] The third party exception must be updated both to accurately reflect the "reasonable expectation of privacy"[169] standard set in *Katz* and the original purposes of the Fourth Amendment.[170]

---

[164] *See* Slobogin, *supra* note 117, at 737–40. A survey of Americans revealed that they felt perusal of their bank records in particular was a serious privacy invasion. *See id.* at 738.

[165] Kerr, *supra* note 63, at 573.

[166] *See id.* at 564.

[167] Judge Leon forcefully makes this argument in Klayman v. Obama, 957 F. Supp. 2d 1, 31–36 (D.D.C. 2013).

[168] 277 U.S. 438, 472 (1928) (Brandeis, J., dissenting).

[169] Katz v. United States, 389 U.S. 347, 360 (Harlan J., concurring).

[170] Justice Brandeis concluded in *Olmstead* that "the Fourth Amendment safeguards against all evils that are like and equivalent to those embraced within the ordinary meaning of its words." 277 U.S. at 488.