Michigan Telecommunications and Technology Law Review

Volume 21 | Issue 2

2015

Voluntary Disclosure of Information as a Proposed Standard for the Fourth Amendment's Third-Party Doctrine

Margaret E. Twomey
University of Michigan Law School

NOTE

VOLUNTARY DISCLOSURE OF INFORMATION AS A PROPOSED STANDARD FOR THE FOURTH AMENDMENT'S THIRD-PARTY DOCTRINE

*Margaret E. Twomey**

Cite as: Margaret E. Twomey, *Voluntary Disclosure of Information as a Proposed Standard for the Fourth Amendment's Third-Party Doctrine*, 21 MICH. TELECOMM. & TECH. L. REV. 401 (2015).
This manuscript may be accessed online at repository.law.umich.edu.

ABSTRACT

The third-party doctrine is a long-standing tenant of Fourth Amendment law that allows law enforcement officers to utilize information that was released to a third party without the probable cause required for a traditional search warrant. This has allowed law enforcement agents to use confidential informants, undercover agents, and access bank records of suspected criminals. However, in a digital age where exponentially more information is shared with Internet Service Providers, e-mail hosts, and social media "friends," the traditional third-party doctrine ideas allow law enforcement officers access to a cache of personal information and data with a standard below probable cause.

This Note explores particular issues that plague the traditional third-party doctrine's interactions with new technology and proposes a standard of voluntary disclosure for courts to use when determining if information falls under the purview of the third-party doctrine. The factors in this proposed standard include the reasonable expectation of privacy of the disclosing person, the frequency with which information is disclosed, the purpose of disclosure, and the degree to which the public can access the information.

* J.D., University of Michigan, 2016 (expected). I am grateful for the assistance of Madison Sharko, KeAndra Barlow, Micah Siegel Wallace, and Lauren Babst, and the support of the entire *MTTLR* Volume 21 editorial staff.

Introduction

"Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions."[1] Justice Brandeis wrote this statement in a dissenting opinion in 1928 for a case involving the wiretapping of bootleggers. While science may not yet allow us to read minds, advances in technology have made it possible to quickly and easily share intimate details of one's life with friends, family, and the world.

Advances in technology are also shaping how law enforcement officers conduct investigations. This intersection of publicly shared information and law enforcement techniques has long been ruled by the third-party doctrine, which generally provides that information released to a third party loses its Fourth Amendment protection, and can be obtained by law enforcement without a search warrant.[2]

A commonly cited statute to support this idea is 18 U.S.C. § 2703, which requires a court order supported by specific and articulable facts—a standard lower than the probable cause required for a warrant[3]—to force disclosure of stored wire and electronic communications.[4] There is a presumption that warrantless searches are unconstitutional, but Fourth Amendment cases have carved out certain exceptions to that rule.[5] The release of information to a third party is one such exception.

Some attorneys and legal scholars now push for the dissolution of this doctrine. They assert the doctrine infringes Fourth Amendment rights given advances in technology that require much more information to be released to

1. Olmstead v. United States, 277 U.S. 438, 474 (1928).

2. *See* Orin Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561, 573–75 (2009).

3. *See* Erin Smith Dennis, Note, *A Mosaic Shield: Maynard, the Fourth Amendment and Privacy Rights in the Digital Age*, 33 Cardozo L. Rev. 737, 757–58 (2011) (noting the different standards for accessing information under various electronic communication statutes); *see also* Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. Pa. L. Rev. 327, 380 (2015).

4. 18 U.S.C. § 2703 (2012).

5. *See* Arizona v. Gant, 556 U.S. 332, 332 (2006) ("Warrantless searches 'are *per se* unreasonable,' 'subject only to a few specifically established and well-delineated exceptions.'") (quoting Katz v. United States, 389 U.S. 347, 356 (1967)).

third parties.[6] However, the doctrine can be amended to both protect rights and allow law enforcement officers to continue to use the valuable investigation tools that stem from this doctrine, including the use of confidential informants and review of suspects' bank records.[7]

The best way to balance these interests is for the doctrine to distinguish information that citizens knowingly and voluntarily convey to third parties from information that citizens may not know or even suspect they convey to a third party but which is obtained by third parties in their normal course of business. This proposed solution incorporates the reasonable expectation of privacy test that has developed in Fourth Amendment jurisprudence,[8] while remaining true to the original third-party doctrine that law enforcement officers have been relying on for decades.[9]

This Note outlines the history and development of the third-party doctrine, highlights incompatibilities between the traditional doctrine and new technology, and proposes a solution using a voluntary disclosure standard. A voluntary disclosure standard would allow law enforcement officers to seek a court order, under statutes like 18 U.S.C. § 2703, only when the information they are seeking was knowingly and voluntarily disclosed to a third party.

Part I outlines the history and development of the third-party doctrine up to and including *Katz*. Part II provides background on the expansion of the third-party doctrine post-*Katz* and Part III addresses how the third-party doctrine should apply to new technology. The application of the third-party doctrinal standards to new technology has led to many criticisms of the doctrine, and these criticisms are laid out in Part IV. Finally, Part V argues for a voluntary disclosure standard, wherein law enforcement officers may seek a court order, under statutes like 18 U.S.C. § 2703, only when the information they are seeking was knowingly and voluntarily disclosed to a third party. Access to invasive types of data that citizens do not actively and knowingly

---

6. Richard M. Thompson II, *Cong. Research Serv., R43586, The Fourth Amendment Third-Party Doctrine* 12 (2014) ("While the third-party doctrine has been criticized by Members of Congress, various commentators and others as overly constrictive of Americans' privacy right . . . .").

7. *E.g.*, United States v. Miller, 425 U.S. 435 (1976).

8. *See infra* Parts III and IV (describing the *Katz* case and the progression of cases post-*Katz*).

9. This doctrine has allowed for the use of undercover agents, confidential informants and pen registers—three major investigative tools. As evidence of the effect on third-party electronic service providers now, it is worth noting that Apple and Google, two larger electronic communication providers, publish data on government requests. In 2013, Google received 21,492 user data requests from the U.S. Government. Google, *Google Transparency Report*, http://www.google.com/transparencyreport/userdatarequests/countries/?p=2013-06 (last visited Feb. 18, 2015). In the same year Apple received between 1,638 and 2,638 requests, as they published the first half of 2013 in a range, instead of providing a specific number. Apple, *Reports on Government Information Requests,* https://www.apple.com/privacy/transparency-reports/ (last visited Feb. 17, 2014).

share (e.g., cell site location data, content of messages, and data from a car computer) should require the same standard of probable cause needed to obtain search warrants of houses, offices, and hard drives.[10]

I. Development of the Third-Party Doctrine

The Justice Brandeis quote[11] mentioned above originates in one of the earliest third-party doctrine cases, *Olmstead v. United States*.[12] That case dealt with the wiretapping of suspected large-scale bootleggers. The wiretapping did not require law enforcement to physically trespass on the defendants' property.[13] The majority held that because there was no physical trespass, the law enforcement officers had not conducted a search under the Fourth Amendment, so the defendants' Fourth Amendment claims were invalid.[14] The court in *Olmstead* also reiterated the idea that information or materials that are purposely shared with others, like calls over a telephone wire that connect to a larger network, are not subject to the same protection that one's person or house merits.[15]

Beyond the glamorous profession of bootlegging, the third-party doctrine also developed around cases involving informants and undercover agents.[16] In one seminal case, involving Teamsters boss Jimmy Hoffa, the Supreme Court held that revealing information to an informant (or "false friend") eliminates the expectation of privacy that a person has, and allows that information to be brought before a court.[17]

Courts have additionally held that it is lawful for individuals wearing recording equipment to converse with, or be within earshot of, a suspect. This view stems from the idea that the recording equipment simply provides

---

10. The Container Doctrine applies to hard drives and mandates a search warrant for law enforcement officers. *See* Saby Ghoshray, *Privacy Distortion Rationale for Reinterpreting the Third-Party Doctrine of the Fourth Amendment*, 13 Fla. Costal L. Rev. 33, nn. 260–66 (2011).

11. *See* Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting) ("Advances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions.").

12. *Id.*

13. *Id.*

14. *Id.* at 464–66 (emphasizing that the Fourth Amendment protects the search of material things, like a man's person, house, papers or effects and should not be read so liberally as to include a man's voice that is being projected along public wires).

15. *Id.* at 466 ("The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house and messages while passing over them are not within the protection of the Fourth Amendment.").

16. *See, e.g.*, United States v. White, 401 U.S. 745 (1971); Lewis v. United States, 385 U.S. 206 (1966); Lopez v. United States, 373 U.S. 427 (1963); On Lee v. United States, 343 U.S. 747 (1952).

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

a better record of what someone could overhear.[18] In many of these opinions, the Supreme Court stressed that the concept of privacy corresponded to the idea of physical trespass.[19] The Court reasoned that informants or "false friends" were not intruding on the suspect,[20] and held that law enforcement methods that intrude on suspects' personal space, such as homes, offices, and hotel rooms, are illegal.[21]

This line of cases was not without its critics on the bench, who pushed for a broader interpretation of Fourth Amendment protection—one that held the right to privacy protected more than just a person's unshared thoughts. Justice Brandeis's dissent in *Olmstead* supported a more liberal interpretation of the Fourth Amendment—one adaptive to the changing technology that law enforcement used to gather information.[22] Brandeis opined that the Fourth Amendment should be read to protect "the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."[23] Justice Frankfurter's dissent in *On Lee* made reference to Justice Brandeis' *Olmstead* dissent to express Frankfurter's concerns about the technological advances that allow for amplified government intrusion in citizens' lives.[24] Justice Brennan's dissent in *Lopez* asserted that while it is not an undue burden for citizens "to make damaging disclosures only to persons whose character and motives may be trusted," it is unreasonable to use an inescapable third party (such as an agent or a recording device) that cannot be

18. *See On Lee*, 343 U.S. at 753–54 (holding that it was lawful and not a trespass for a customer of the suspect to enter the suspect's business with the consent of the suspect and engage the suspect in a conversation that was being recorded and listened to by a Bureau of Narcotics agent, as "[p]etitioner was talking confidentially and indiscreetly with one he trusted, and he was overheard. This was due to aid from a transmitter and receiver, to be sure, but with the same effect on his privacy as if agent Lee had been eavesdropping outside an open window."); *see also*, *Lopez*, 373 U.S. at 439 ("[the device] neither saw nor heard more than the agent itself."). *But c.f. Lopez*, 373 U.S. at 438 ("The Court has in the past sustained instances of 'electronic eavesdropping' . . . when devices have been used to enable government agents to overhear conversations which would have been beyond the reach of the human ear").

19. *See* United States v. Jones, 132 S. Ct. 945, 958–60 (2012) (describing the historical jurisprudence as centered on a "trespass-based rule.").

20. *See On Lee*, 343 U.S. at 751–52 (the wired informant "entered a place of business with the consent, if not by the implied invitation of the petitioner.").

21. *See Hoffa*, 385 U.S. at 301 ("A hotel room can clearly be the object of Fourth Amendment protection as much as a home or an office." (internal citation omitted)); *see also*, Silverman v. United States, 365 U.S. 505, 509–11 (1961) (holding that the unauthorized physical invasion of a "spike mike" into the exterior of a defendant's house did constitute an illegal intrusion).

22. *See* Olmstead v. United States, 277 U.S. 438, 473 (1928) (Brandeis, J., dissenting) (stating that at the time the Fourth Amendment was ratified, force and violence were the only known means by which the Government could force self-incrimination).

23. *Id.* at 478 (also stating that it is immaterial where the connections to the telephone wires were made, and whether a physical trespass occurred). This idea was also suggested in an 1890 article penned by Warren and Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

24. *On Lee*, 343 U.S. at 759.

shut out of a conversation the same way that a suspect and a trusted confidant could simply walk away from a potential eavesdropper.[25] Justice Brennan additionally opined, "I believe that there is a grave danger of chilling all private, free, and unconstrained communication," and asserted that one aspect of a free society is that people should not have to watch every word as carefully as these cases would require.[26]

Justice Brennan's idea—that a person has the right to seek out a space to have a private conversation with a trusted confidant without government interference or recording—came to a head four years later in a case involving an eavesdropping device placed outside of a phone booth.[27] The Court in *Katz* acknowledged that the trespass doctrine used in *Olmstead* and *Goldman v. United States*[28] had been so eroded by subsequent decisions, that it was no longer sound footing for controlling law.[29] The majority dismissed the idea that the Fourth Amendment protects a general right to privacy.[30] However, the majority departed from its previous characterization of the Fourth Amendment as only protecting physical locations (like houses and offices),[31] by holding that "the Fourth Amendment protects people, not places."[32] Intangible interests, as well as tangible property, could be protected under the Fourth Amendment.

While the *Katz* opinion ushered the third-party doctrine into a new jurisprudential framework, *Katz* is often cited for the test developed by Justice Harlan in his concurrence.[33] It is worth noting that Justice Harlan reads the majority opinion not as doing away with the idea of "constitutionally protected areas"[34] (such as houses and offices), but instead as adding to the list of such protected areas.[35] The two-part test, as stated by Harlan, determines if a suspect is in a situation that warrants such constitutional protection.[36] The test looks at (1) whether the suspect has demonstrated an actual (subjec-

25. Lopez v. United States, 373 U.S. 427, 450 (1963). Brennan also cited Warren and Brandeis' article "The Right to Privacy," *supra* note 23, in his dissent.

26. *Lopez*, 373 U.S. at 452.

27. Katz v. United States, 389 U.S. 347 (1967). It is worth noting that in *Katz*, Brennan joined with Justice Douglas' concurrence expressing concern about the unchecked power of the executive branch to conduct warrantless eavesdropping in matters of national security. *See id.* at 359–60

28. 316 U.S. 129 (1942).

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

30. *Id.* at 350 (stating that this protection is an area largely left to state law).

31. *See, e.g.*, Hoffa v. United States, 385 U.S. 293, 301 (1966); Silverman v. United States, 365 U.S. 505, 509–11 (1961).

32. *Katz*, 389 U.S. at 351.

33. A LexisAdvance search for "*Katz* reasonable expectation of privacy test" returns over 200 federal court opinions since the decision first came down.

34. This phrase is seen in *Hoffa*, 385 U.S. at 301.

35. *Katz*, 389 U.S. at 360 (Harlan, J., concurring) (likening the phone booth to a home, instead of a field, and adding places like closed phone booths, where there is an expectation of privacy, to the list).

36. *Id.* at 361.

tive) expectation of privacy and (2) whether society would deem that expectation of privacy reasonable.[37]

This second prong of the *Katz* test has had the most influence on later cases, so much so that it is often referred to in later decisions as the "*Katz* reasonable expectation of privacy" test.[38] However, the *Katz* majority and the Harlan concurrence clearly established that a person has no reasonable expectation of privacy when information is knowingly disclosed to the public.[39] For example, a man in his office who knowingly projects information to the public by yelling out a window has no reasonable expectation of privacy in that information and can expect the government to acquire it. Contrast that example with a man in a public telephone booth who has taken care to shut the door and shield his conversation from others. The latter person is entitled to the assumption that his conversation remains private.

From this logic, one might think that people have a reasonable expectation of privacy when conversing with a trusted acquaintance. However, after the *Katz* decision, the Court in *United States v. White*[40] continued the logic found in the earlier line of cases[41] which held that people have no constitutionally protected expectation that the person they are conversing with will not share that information with law enforcement. So while the *Katz* decision is significant to Fourth Amendment cases in general, and marks the Court's acceptance of a possible "right to privacy," the third-party doctrine jurisprudence did not immediately change in response to it.

II. Expansion of the Third-Party Doctrine

In 1976, the third-party doctrine reached beyond conversations and voice recordings by opening up documents to government acquisition in *United States v. Miller*.[42] In that case, the government investigated Miller for his possible involvement in an illegal whiskey distillery and subpoenaed his bank records, including checks, deposit slips and account statements kept in the bank's ordinary course of business.[43] Miller argued that he had a reasonable expectation that his bank documents were being kept and maintained

37. *Id.*

38. *See supra* note 33. And while this prong is where much of the action takes place, the first prong has developed the "abandonment theory," when a defendant abandons a reasonable expectation of privacy in their property. *See, e.g.*, United States v. Harrison, 689 F.3d 301, 306–07 (3d Cir. 2012) (discussing that law enforcement can search an abandoned house that is essentially open to the public and frequently vandalized).

39. Katz, 389 U.S. at 351; *see also id.* at 361 (Harlan, J., concurring) ("objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited.").

40. 401 U.S. 745, 754 (1971).

41. *See, e.g.*, On Lee v. United States, 343 U.S. 747 (1952); Hoffa v. United States, 385 U.S. 293 (1966); Lewis v. United States 385 U.S. 206 (1966).

42. 425 U.S. 435, 444 (1976).

43. *Id.* at 437–38.

for a specific purpose, and would be protected as if they were copies of his personal records, made available to the bank for this limited purpose.[44] However, Justice Powell distinguished the documents kept in the bank's normal course of business from "private papers" that would merit protection under the trespass theory of protection, as the defendant neither owned nor possessed the business records.[45]

In his second argument, Justice Powell drew from the third-party doctrine[46] and the *Katz* reasonable expectation of privacy test to assert that Miller lost protection under the Fourth Amendment when he knowingly exposed information to the public by doing business with the bank and voluntarily conveying the checks and deposit slips to the bank.[47] Like the informants and agents in earlier cases, the bank was a party to these transactions and its customers had no expectation that it would not share this information with the government.[48] Justice Powell pointed to the Bank Secrecy Act, which requires bank records to be maintained because of their usefulness (especially in criminal matters), as proof that bank customers have no legitimate expectation of privacy.[49]

After *Miller*, the Court affirmed this logic in *Couch*[50] and *Smith*.[51] The former case dealt with documents in the possession of an accountant, and held that there was no expectation of privacy in those documents.[52] In the latter case, a phone company placed a pen register on a customer's phone, at the request of police. This practice was also upheld under the third-party doctrine.[53] The Court began by distinguishing the lists of phone numbers received in *Smith* from electronic eavesdropping on actual conversation in *Katz*, and made an important content/non-content distinction that continues in the third-party doctrine cases today.[54] Writing for the majority in *Smith*, Justice Blackmun observed that phone companies notify customers that they

---

44. *Id.* at 442.

45. *Id.* at 440. It is worth noting that Harlan's concurrence in *Katz* is not the end of the physical trespass concept of the Fourth Amendment. In fact, Justice Scalia in a later case states explicitly that the *Katz* test serves to supplement the trespass theory—not replace it. *See* United States v. Jones, 132 S. Ct. 945, 952 (2012).

46. *Miller*, 425 U.S. at 443 (citing *Hoffa*, 385 U.S. 293, and Lopez v. United States, 373 U.S. 427 (1963)).

47. *Id.* at 441–43 ("The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.").

48. *Id.* at 440–41.

49. *Id.* 442–43.

50. Couch v. United States, 409 U.S. 322 (1973) (holding that there is no expectation of privacy when documents are given to accountants).

51. Smith v. Maryland, 442 U.S. 735 (1979) (holding that a pen register, placed by the phone company, identifying phone numbers was protected by the third-party doctrine).

52. *Couch*, 409 U.S. 322.

53. *Smith*, 442 U.S. 735.

54. *Id.* at 741 (reiterating that a pen register does not record a call or even hear a call, but rather discloses the number dialed); *see also* THOMPSON II, *supra* note 6, at 12. (the old 51)

can report harassing or annoying callers.[55] This, the Court argued, makes it too much to believe that any reasonable subscriber would consider the numbers he dialed to remain a secret.[56] Even if the customer had a subjective expectation of privacy (the first prong of the *Katz* test), it was not a reasonable expectation.[57] Like in the *Miller* case, the *Smith* court held that widely known company practices shape what may reasonably be expected to be private.[58]

The *Smith* Court also made an automation argument that recurs in later third-party doctrine cases and academic writings.[59] Justice Powell wrote that the switching equipment used by phone companies is simply a modern version of an operator—a third party capable of sharing information with the government, like a bank teller.[60] Powell also noted that customers (or depositors in the case of *Miller*) "assum[e] the risk of disclosure."[61] This "assumption of risk" argument is also frequently cited to support the third-party doctrine.[62] That argument supports the use of voluntary disclosure as the standard, since the assumption of risk argument is based on individuals assuming the risk of exposure when they release information of one's own volition. The argument is laden with several assumptions: that customers (1) know information is being released, (2) realize there is a risk of it being revealed, and (3) are willing to take that risk because of the benefit they get from releasing the information.

III. Applying the Third-Party Doctrine to New Technology

In 1986, Congress passed the Electronic Communications Protection Act (ECPA), which was designed to prohibit government access to certain electronic communications.[63] However, the Act ended up creating major ex-

55. *Smith*, 442 U.S. at 742–43.

56. *Id.* at 743–44.

57. *Id.* at 742 ("First, we doubt that people in general entertain any actual expectation of privacy in the numbers they dial.").

58. *Id.* at 743.

59. *See, eg.*, Matthew Tokson, *Automation and the Fourth Amendment*, 96 Iowa L. Rev. 581 (2011); *see also infra* notes 136–37.

60. *Smith*, 442 U.S. at 744–45.

61. *Id.* at 744.

62. *See* Thompson II, *supra* note 6, at 19; *see also* United States v. Miller, 425 U.S. 435, 443 (1976); *but cf.*, *Smith*, 442 U.S. at 750 (Marshall, J., dissenting) (criticizing this idea, suggesting that people cannot assume the risk when they have no practical alternatives).

63. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in various sections of 18 U.S.C.); *see also Electronic Communications Privacy Act: Hearing on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice of the H. Comm. on the Judiciary,* 99th Cong. 1–2 (1986) (statement of Rep. Robert W. Kastenmeier, Chairman, S. Comm. on Courts, Civil Liberties, and the Administration of Justice) ("Congress needs to act to ensure that the new technological equivalents of telephone calls, telegrams and mail are afforded the same protection provided to conventional communications.").

emptions, prompting calls for change in the third-party doctrine.[64] Three parts of ECPA are most directly implicated in third-party cases: The Wiretap Act[65] expanded restrictions on government wiretaps on phones to electronic computer transmissions;[66] the Stored Communications Act (SCA) was intended to protect communications stored electronically, such as e-mails on Internet Service Provider (ISP) servers;[67] and the Pen Register statute created the requirement of a court order for the disclosure of pen registers to law enforcement, and limited the ability of the government to access the content of such communications.[68]

As discussed in the above-section, the content/non-content distinction first arose in third-party cases.[69] ECPA went on to codify that distinction, making it permanent and influential on the development of later cases. With the SCA and pen register statutes, Congress intended to protect individuals' electronic information, and it intended to do so in a broad manner that would allow the statute to adapt to quickly changing technology.[70] One way Congress did this was by requiring a court order with a standard of "specific and articulable facts"[71] for information that had previously required no such order. However, the "specific and articulable facts" standard is lower than the probable cause standard required to support a search warrant.[72] This lower standard has caused much of the pushback against the third-party doctrine, especially as more and more information is released to third parties (especially ISPs) on a daily basis.[73]

However, despite being relatively newly enacted by Congress, these statutes do not specifically address many of the new technologies that have emerged in recent years. For example, wireless service providers record when a cell phone connects with specific phone towers—essentially pinpointing the travel of the phone holder. Courts are split on whether law enforcement officers can obtain these records from wireless providers without

64. *See* Evan Peters, *The Technology We Exalt Today Is Everyman's Master*, 44 WASH. U. J.L. & POL'Y 103, 120–22 (2014); *see also* Dennis, *supra* note 3, at 754–59.

65. Peters, *supra* note 64, at 132; *see also* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

66. *See Jones*, 132 S. Ct. at 963 (Alito, J., concurring).

67. 18 U.S.C. §§ 2701-12 (2014); *see also*, Alexander Scolnik, *Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment*, 78 FORDHAM L. REV. 349, 375 (2009).

68. *See* Dennis, *supra* note 3, at 757–58; *see also*, Ghoshray, *supra* note 10, at n.22.

69. *See* Smith v. Maryland, 442 U.S. 735, 741 (1979).

70. *See* Scolnik, *supra* note 67, at 374 (citing to 132 CONG. REC. 14,885 (1986)).

71. *See* 18 U.S.C. § 2703 (2012).

72. *See* Scolnik, *supra* note 67, at 375–77.

73. *See* Dennis, *supra* note 3, at 755–56 (noting that information that law enforcement can monitor in real time under the Pen Register Statute includes all information in e-mail headers, including e-mail addresses, timestamps, and IP addresses.).

a warrant.[74] Cell site location data is one of the most hotly contested areas of the third-party doctrine right now.

While grappling with adapting precedent to new technology, courts have used some creative solutions—like the automation rationale previously mentioned—to either fit new technology into old standards, or develop new tests to determine the reasonable expectation standard of *Katz*. The D.C. Circuit's decision in *United States v. Maynard*[75] gives courts a unique basis upon which to strike down the intensive monitoring seen in earlier cases, *Karo* and *Knotts,*[76] without using the automation rationale. In *Maynard*,[77] the court adapted the mosaic theory—an idea that originated in Freedom of Information Act cases—and applied it to the Fourth Amendment.[78] Mosaic theory posits that while one discrete piece of information, like a car's location in a public place at one particular time, is not a search under the Fourth Amendment, a GPS tracker identifying a car's location in public over the span of weeks creates a picture far more revealing and intimate than what could be drawn from basic, warrantless surveillance techniques.[79] Patterns and more personal information can be identified from the combination of such extensive information revealing such personal details as frequently visited houses of religion, multiple trips to the headquarters of a political party, or regular visits to a lover's house—information the court held should be protected by a warrant.[80]

The Supreme Court granted a writ of certiorari for *Maynard* in *United States v. Jones*, a 2012 case dealing with a GPS tracker placed on a car.[81] While the justices returned a unanimous decision affirming the D.C. Circuit, they were split on the logic. Justice Scalia authored the opinion (joined by Justices Roberts, Kennedy, and Thomas), Justice Sotomayor wrote an independent concurrence, and Justice Alito (joined by Justices Ginsburg, Breyer and Kagan) also authored a concurrence. The plurality's opinion, written by Justice Scalia, is premised on the older, pre-*Katz* idea of trespass on the

74. *See* In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't., 620 F.3d 304 (3d Cir. 2010); *see also* In re Application of U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013); *but c.f.* Davis v. United States, 754 F.3d 1205 (11th Cir. 2014).

75. United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010).

76. *See* United States v. Karo, 468 U.S. 705 (1984); *see also* United States v. Knotts, 460 U.S. 276 (1983). Both cases dealt with tracking devices that their respective Courts held became unconstitutional once government agents began reviewing the tracking information, similar to the human observation/automation distinction mentioned. So while the placement of the device was constitutional, actually using the tracking device for its intended purpose—to track—caused law enforcement officers' actions to run afoul of the constitution.

77. *Maynard*, 615 F.3d at 562.

78. *See* Dennis, *supra* note 3, at 737, 754–59.

79. *Maynard*, 615 F.3d at 544.

80. *Id.* at 562.

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

defendant's vehicle.[82] Law enforcement agents installed the GPS tracker one calendar day after the warrant's established timeframe, and the tracker was installed while the car was in Maryland—not the District of Columbia, as specified in the warrant.[83] The majority of justices decided the case based on the warrantless physical intrusion of the tracker.[84] Scalia addressed the argument that the *Katz* reasonable expectation of privacy test ended the previous line of physical trespass cases, and instead clarified that the *Katz* test simply expanded the common law trespass test to accommodate for technology that could invade formerly private conversations.[85]

Just as Justice Harlan's concurrence is the most famous opinion from *Katz*,[86] a concurring opinion in *Jones* has prompted additional dialogue about the third-party doctrine. Justice Sotomayor agrees with the plurality that there was a trespass on the defendant's car, and based her holding on that principle.[87] However, she also discusses the two lines of privacy doctrine that exist today: the historical trespass reasoning (which the majority used in *Jones* to maintain the doctrine of constitutional avoidance[88]), and the *Katz* idea of a reasonable expectation of privacy that contributed to the development of the mosaic theory as a tool to determine that expectation.[89] Sotomayor's concurrence, while not proposing a solution to the third-party doctrine's applicability to a modern era, reinforces the concern that widespread, available, and cheap electronic surveillance could chill "associational and expressive freedoms" by revealing large amounts of data about those under surveillance.[90]

Another concurring opinion, authored by Justice Alito, focuses solely on the reasonable expectation of privacy test, and even goes as far as to assert that the majority is "hard-pressed to find support in post-*Katz* cases for its trespass-based theory."[91] Justice Alito's concurrence highlights the inconsistency of the trespass theory, noting that under such a theory, briefly tracking a car using GPS surveillance would not be allowed under the Fourth Amendment, but following that same car for weeks using unmarked law enforce-

82. *Id.* at 954 ("It may be that achieving the same result [as traditional surveillance] through electronic means, *without an accompanying trespass*, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question.") (emphasis added).

83. *Id.* at 948.

84. *See id.* at 949; *see also*, *id.* at 955 (Sotomayor, J., concurring).

85. *Id.* at 952 ("But as we have discussed, the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.").

86. *See supra* note 33.

87. *Jones*, 132 S. Ct. at 955.

88. *Id.* at 954 ("and answering it leads us into additional thorny problems.").

89. *Id.* at 956.

90. *Id.* at 957 ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.").

91. *Id.* at 961.

ment vehicles and aerial surveillance would be constitutional.[92] Justice Alito's opinion echoes the lower court's mosaic theory-based decision in *Maynard*[93] that warrantless, extended law enforcement surveillance violates the Fourth Amendment when the length of the surveillance goes beyond what people would reasonably expect.[94]

IV. Criticisms of the Third-Party Doctrine

Unlike when ECPA was passed in 1986, now almost 90 percent of Americans own some sort of computerized technology[95] and many of them share personal information through cell phones, e-mail, social media and web-based applications. The ubiquity of technologies that permit information sharing is one of the major arguments against the third-party doctrine.[96] Critics say the traditional third-party doctrine, which looks at a combination of reasonable expectations and physical trespass, is ill-suited for a society where information can be easily obtained without any physical trespass, and where new technology and current events are constantly reshaping expectations of privacy.[97] Because the traditional doctrine clashes with modern society, some critics propose doing away with the third-party doctrine entirely, forcing law enforcement officers to always seek a warrant to get this information. These critics fail to take into account the public safety interest in giving law enforcement the necessary tools, and support their criticisms with misguided notions about privacy or the role of federal law enforcement.

When criminals avail themselves of the benefits of third-party assistance, they should not receive the same amount of privacy that criminals acting alone receive.[98] Most law enforcement investigations are based on the two-step investigatory scheme that has been established and developed through Fourth Amendment jurisprudence. This scheme starts with less invasive, open surveillance techniques, followed by more invasive steps that require law enforcement to make certain showings (such as the probable

92. *Id.*

93. *See* United States v. Maynard, 615 F.3d 544, 560 (D.C. Cir. 2010).

94. *See Jones*, 132 S. Ct. at 964. It is also worth mentioning that one criticism of using the *Katz* test is that society's reasonable expectation of privacy can be manipulated by government policies that elevate national paranoia; *see* Ghoshray, *supra* note 10, at 62–63 (mentioning specifically the Patriot Act legislation passed after 9/11 that used the heightened sense of fear to pass laws infringing more on citizens' privacy).

95. *See* Peters, *supra* note 64, at 118–20; *see also*, Dennis, *supra* note 3, at n.20.

96. *See*, Thompson II, *supra* note 6, at 2 ("[T]he third-party doctrine has been criticized by Members of Congress, various commentators and others as overly constrictive of Americans' privacy rights . . . .").

97. *See* Ghoshray, *supra* note 10, at 63; *see also infra* note 112 (regarding current events that have shaped expectations of privacy).

98. Kerr, *supra* note 2, at 573–75 (explaining the substitution effects that criminals experience when using third parties, by replacing the criminal's public actions with a third party's actions).

cause required for a search warrant).[99] If the third-party doctrine is eradicated and criminals are able to use third parties to conduct entire criminal acts, law enforcement agencies will lose some of their most basic investigative abilities.[100] Third parties that would have previously met in public, or could be observed leaving a subject's house, can now be e-mailed from a basement, entirely out of sight of law enforcement officers.[101] The traditional open surveillance techniques are no longer effective. Even if officers have reasons to investigate a subject further, they are hamstrung by a technologically-advanced world that puts physical surveillance out of reach and, for example, allows child pornography to be shared across the world without a subject ever leaving home.

Some critics of the third-party doctrine argue that privacy is an all-or-nothing concept.[102] This concept posits that once a person (or government entity) has access to the information, the information is essentially public knowledge—phone numbers and call times identified by police could be discovered by the subject's employer or spouse. This argument fails to consider the secrecy involved in most investigations at this stage, and fails to consider that the third parties receiving the information (such as phone companies and ISPs) have a commercial interest in protecting customer information.[103] While a limited business purpose does not shield a bank from disclosing information to the government, banks have a very high commercial interest in protecting client information. In fact, companies who have suffered recent breaches of privacy have responded to declining stock prices by spending additional money on public relations to assure customers of their security, and guaranteeing credit monitoring for customers.[104] Compa-

---

99. *Id.* at 574.

100. *Id.* at 576 ("He [a criminal] could use third parties to create a bubble of Fourth Amendment protection around the entirety of his criminal activity.").

101. *See* Stephen Henderson, *The Timely Demise of the Fourth Amendment*, 96 IOWA L. REV. BULL. 39, 44–45 (2011) ("[I]t is true than any protective doctrine permits 'savvy wrongdoers' to hide portions of their crime from public observation.") Henderson goes on to analogize shopping at a bookstore as opposed to buying a book online with committing a crime, but fails to note the interest that people have in keeping that information private. While customers may find the convenience of online book shopping worth the disclosure of payment and purchase information, criminals are likely to be far more cautious about what information they are disclosing to anyone.

102. *See* Kerr, *supra* note 2, at 571; *but cf.* THOMPSON II, *supra* note 6, at 17 (asserting that people also criticize the third-party doctrine for seeing privacy as an all-or-nothing idea).

103. *See* Kerr, *supra* note 2, at 598–99; *see also* Joseph Pomianowski and Jane Chong, *In Order to Protect Users From Intrusive Governments, Apple has Prevented Itself from Unlocking iOs 8 Devices*, FORBES OPINION BLOG (Oct. 16, 2014) http://www.forbes.com/sites/realspin/2014/10/16/in-order-to-protect-users-from-repressive-governments-apple-has-prevented-itself-from-unlocking-ios-8-devices. *But cf.* Kerr, *supra* note 2, at 600 (noting that some companies (especially telecommunications companies) have come under fire for voluntarily assisting the government (the NSA) in actions that likely violated privacy statutes).

104. Robin Sidel, *Home Depot's 56 Million Card Breach Bigger than Target's*, WALL ST. J., Sept. 9, 2014, http://www.wsj.com/articles/home-depot-breach-bigger-than-targets-

nies, then, are likely to understand the value of maintaining customer privacy.

Though companies can, and do, sell subscriber information to third parties for advertising purposes,[105] consumers can generally find out if a particular company does that before giving the company their business.[106]

While some critics rely on a misguided concept of complete privacy loss, other critics pushing for repeal of the third-party doctrine look to state law for support. Stephen Henderson, who wrote in support of completely doing away with the third-party doctrine, substantiated his argument by citing a survey of state laws, showing that the doctrine is not popular at the state level.[107] This fails to take into account the legitimate needs of federal law enforcement, which investigates and pursues larger and more serious crimes and more sophisticated criminals and, for that reason, needs a larger toolbox. While some criticism of the third-party doctrine has merit, critics calling for its total repeal fail to consider the benefits to law enforcement and, subsequently public safety, that result from the doctrine.

V. Modifying Third-Party Doctrine to Reach New Technologies

Keeping the third-party doctrine as it currently stands without modification presents concerns about privacy in a modern world where personal information is frequently released to third parties.[108] While doing away with the doctrine completely has the appeal of easy administration, it poses a very real threat to law enforcement investigations, as previously discussed. Instead, courts should maintain certain aspects of third-party jurisprudence, while incorporating greater protection for information that is not turned over willingly. There is a strong reliance argument in support of law enforcement techniques that have developed around the third party, like allowing bank records[109] and pen registers[110] to be released without a warrant, and these established precedents should continue. The doctrine also fits in relatively

---

1411073571 (quoting a Home Depot estimate that the breach would cost the company $62 million).

105. *See* Ferguson, *supra* note 3, at 376 ("In fact, many businesses, including big-name companies like Google, Microsoft, Yahoo!, and Facebook, are financially successful, in part, because of their ability to sell targeted advertising using user data.").

106. For instance, the Gramm-Leach-Bliley Act requires financial institutions to disclose their information sharing policies to potential customers. *See* Gramm-Leach-Bliley Financial Modernization Act, Pub. L. No. 106–102, 113 Stat. 1338 § 204 (1999).

107. Stephen Henderson, *Learning from All Fifty States: How To Apply the Fourth Amendment and its State Analogs to Protect Third-Party Information from Unreasonable Search*, 55 Cath. U. L. Rev. 373, 376 (2006) ("This study reveals eleven states [in their state constitutions] reject the third-party doctrine and ten others have given some reason to believe that they might reject it.").

108. *See* Peters, *supra* note 64, at 118–19; *see* Thompson II, *supra* note 6; *see also* Dennis, *supra* note 3, at n.20.

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

110. *See* Smith v. Maryland, 422 U.S. 735 (1979).

neatly with general Fourth Amendment case law, supporting its continued existence.

Society would also benefit from allowing law enforcement warrantless access to information that is voluntarily and knowingly disclosed to a third party. Voluntary disclosures to third parties using new technology should be afforded no protection. On the other hand, information that is not affirmatively and voluntarily shared, yet is accessible by third parties as a result of new technology, should be protected by the strongest form of Fourth Amendment protection—a warrant requirement.

A. *Proposed Standard of Voluntary Disclosure*

Courts should consider the following factors to determine whether information was voluntarily released: the reasonable expectation element that was present in *Katz*; the purpose of the disclosure; the frequency of transmissions; and the public access to the information.[111]

The standard of "voluntary disclosure" coheres with the *Katz* reasonable expectation of privacy test, but also allows courts to consider factors other than society's reasonable expectation of privacy—something the average judge may find difficult to ascertain and is likely to shift based on current events.[112] In addition to the reasonable expectation factor, courts can look at the number of data transmissions to determine the intrusiveness of the scope of the warrantless investigation. This factor brings the mosaic theory of *Maynard*[113] squarely into the court's consideration. Whether some other members of the public can access that data should also be taken into account—since that third-party presence forms the initial basis of the doctrine. Instead of doing away with the third-party doctrine and requiring a search warrant to look at a subject's Facebook page that 800 of his closest "friends" can already see, this test allows law enforcement agencies to access his status updates through an evidentiary standard that is slightly easier to meet.[114]

A court should also consider the purpose of sharing the information. While the Court in *Miller*[115] rejected the idea of a limited purpose exclusion

111. *See* Matthew D. Lawless, *The Third-Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth Amendment Protection*, 2007 UCLA J.L. & TECH. 1, 21–23 (2007) (regarding his "Operational Realities" test which focuses on who has the right to view the information).

112. For example, cloud security came into the public sphere after hundreds of photos of celebrities were released online after their iCloud accounts were hacked. *See* Justin Worland, *How That Massive Celebrity Hack Might Have Happened*, TIME (Sept. 1, 2014) http://time.com/3247717/jennifer-lawrence-hacked-icloud-leaked; *see also*, *supra* note 94 (regarding the national climate after the 9/11 attacks).

113. United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010).

114. This factor is similar to the test proposed by Matthew D. Lawless, which would focus on who had a right to view the information and whether the parties agreed to and were aware of the disclosure. *See* Lawless, *supra* note 111, at 1, 21–23.

115. United States v. Miller, 425 U.S. 435 (1976).

to the doctrine, in a world where metadata runs rampant, the purpose of sharing the information contributes to determining what data was voluntarily and knowingly revealed. For example, a person uses FitBit to voluntarily share the number of steps taken in a day, but any location information that helped determine that number would remain shielded. So while bank customers may expect that the bank will disclose information related to banking, they would not expect the bank to reveal their height or eye color—if a bank for some reason chose to identify customers by those factors. In order for the voluntary disclosure standard to be met, the disclosing parties need to know what type of information they are releasing and take the chance that the voluntarily released information could be shared.

This idea ties into the "assumption of risk" arguments used in earlier cases[116] and incorporates the more recent mosaic theory into a standard that is easily administrable by courts and easily understood by citizens.[117] Texts, phone calls, and e-mails are released to ISPs, phone companies, and (in the case of e-mails), the servers of the e-mail host. Like the pen register cases, allowing law enforcement access to the non-content "envelope information" at the lower statutory standard required for a court order should be continued.[118]

Similar to the *Katz* test, a knowing, voluntarily release standard would be based on peoples' understanding (a reasonable expectation) of the disclosure of information. Facebook statuses,[119] online shopping orders, and interaction with a smartphone application, such as Google Maps or Spotify, would be disclosures that are understood to be reviewed by a third party (either automated or human review). However, cell site tracking location that is periodically sent to the cellular company would not fall into this category.[120] Similarly, websites visited would not be considered voluntary disclosures to the ISP, under the reasonable expectation of privacy that most

116. *See* Smith v. Maryland, 442 U.S. 735, 744 (1979).

117. For more on the assumption of risk idea, *see* Kerr, *supra* note 2 at 588 (asserting that viewing the third-party doctrine as a consent doctrine helps clarify and reconcile the cases).

118. This line of logic has been upheld by the 6th and 9th Circuits. *See* United States v. Warshak, 631 F.3d 266 (6th Cir. 2010); United States v. Forrester, 512 F.3d 500 (9th Cir. 2007).

119. For more on the third-party doctrine implications of Facebook, *see* Monu Bedi, *Facebook and Interpersonal Privacy: Why the Third-Party Doctrine Should not Apply*, 54 B.C. L. Rev. 1, 27 (2013).

120. Even if most cell customers are aware their smartphones track location data, they generally have no control over the release of that information; *see* Orin Kerr, *Eleventh Circuit, disagreeing with the Fifth, holds Fourth Amendment protects cell-site records*, Washington Post: Volokh Conspiracy Blog (June 11, 2014) http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/06/11/eleventh-circuit-disagreeing-with-the-fifth-holds-fourth-amendment-protects-cell-site-records.

people have in their Internet browsing habits,[121] as well as the mosaic theory proposed in *Maynard* and discussed in *Jones.*

In addition to the reasonable expectation element, courts should consider the frequency of transmissions and the public access to the information (e.g., whether the average person could access this information or whether this information would only be available through a subpoena).[122] The addition of these more concrete factors assuages some of Justice Alito's concerns about subjectivity and circularity that he expressed in the *Jones* concurrence.[123]

B. *Application of Proposed Standard to Modern Technology*

Facebook and social media fall on the disclosure end of the third-party spectrum. Participants knowingly and willingly share information with others. The transmission is directed entirely by the person sharing the information; that person dictates the frequency of transmissions.[124] Orin Kerr, who has written at length about the third-party doctrine, highlighted this idea of knowingly transmitting data, stating that "courts should assume that users of a technology understand the technology. . . [t]he Constitution shouldn't safeguard ignorance."[125] This bar for technological "ignorance" is likely getting higher every year, as more people use new technologies and see how these tools can be misused.[126]

---

121. One aspect of this expectation of privacy comes from the fact that much Internet usage happens in one's home. As seen in the development of Fourth Amendment cases, and the fact that the Third Amendment explicitly protects the home, there is both Constitutional and case law support for shielding the activities taking place in one's home; *but cf.* Kerr, *supra* note 2 (about a criminal who conducts all crime from home—however that level of interaction would require more than passively browsing websites—it would require the type of voluntary information disclosure that this paper asserts should be fair game for law enforcement officers under the third-party doctrine.).

122. *See* Lawless, *supra* note 114 (regarding his "Operational Realities" test which focuses on who has the right to view the information).

123. United States v. Jones, 132 S. Ct. 945, 962 (2012) ("The Katz expectation-of-privacy test avoids the problems and complications noted above, but it is not without its own difficulties. It involves a degree of circularity. . .and judges are apt to confuse their own expectations of privacy with those of the hypothetical reasonable person to which the Katz test looks.") (internal citations omitted).

124. E.g., the number of Facebook statuses created, or the average number of tweets per day.

125. Orin Kerr, *Cell Phones, Magic Boxes and the Fourth Amendment*, VOLOKH CONSPIRACY (Nov. 8, 2010), http://volokh.com/2010/11/08/cell-phones-magic-boxes-and-the-fourth-amendment/.

126. *E.g.*, Biana Bosker, *The Twitter Type that Exposed Anthony Weiner*, HUFFINGTON POST (June 7, 2011), http://www.huffingtonpost.com/2011/06/07/anthony-weiner-twitter-dm_n_872590.html (explaining Weiner's mistaken direct message that was published as a public tweet); *see* Sidel, *supra* note 104 (regarding credit card breaches); *see also* Worland, *supra* note 112.

On the other end of the voluntary disclosure spectrum, some releases of information would not count as disclosure, e.g., location information transmitted from a FitBit. A FitBit tracks steps, counts calories burned, and monitors sleeping habits. Consumers purchase the device to monitor their health, and indeed, while the device records location data, consumers are not using a FitBit for that purpose and may not even be aware of the location data function. The users, then, have a reasonable expectation that any tertiary location data used to calculate the number of steps they took is safe from government seizure. There is also the concern about the frequency with which FitBit data is transmitted. The device automatically backs up to a computer or mobile device every twenty minutes if it can connect to wireless Internet.[127] However, FitBit does allow users to "friend" other FitBit users and it allows data to be shared with third parties.[128] So information broadcasted to FitBit friends would fall under the third-party doctrine, while the minute-by-minute data and daily totals that are stored on the device would not be accessible without a search warrant.

Of course people share information with technology in ways that are less clear than the previous two examples. Venmo and ApplePay are two different applications that both allow their users to pay other people. However, they operate in very different realms. Venmo is a social payment medium where users can find their friends, make payments public and add cheeky descriptions of payments that other users can "like."[129] ApplePay presents itself as a payment method that is more secure than credit cards because Apple uses a tokenized, random account number for each credit card, so the actual credit card number is not even shared with the retailer.[130] While a traditional credit card transaction involves revealing the credit card number to the cashier, and possibly to anyone within eyeshot of the card, Apple markets its payments as far more private.[131] By contrast, Venmo users understand the social aspect of their payments, appreciating that the information is revealed publically to their friends and other users of the app. A Venmo payment would fall squarely within the kind of disclosures subject to the third-party doctrine, whereas an ApplePay transaction would not.

---

127. *Help Article: How do I get data from my tracker to the website?*, FITBIT HELP, http://help.fitbit.com/articles/en_US/Help_article/How-do-I-get-data-from-my-tracker-to-the-website/?l=en_US&fs=RelatedArticle (last updated Jan. 8, 2015).

128. *Help Article: 3rd Party Integration*, FITBIT HELP, http://help.fitbit.com/?l=en_US&c=Topics%3AX3rd_Party_Integration (last visited March 27, 2015).

129. John Patrick Pullen, *You Asked: What is Venmo?*, TIME (Dec. 15, 2014), http://time.com/3632048/you-asked-what-is-venmo/.

130. H.O. Maycotte, *Sorry Walmart-NFC and Apple Pay have Already Won*, FORBES (Nov. 4, 2014), http://www.forbes.com/sites/homaycotte/2014/11/04/nfc-apple-pay-already-won/.

131. *Id.* ("Because Apple doesn't store the credit card information, it is never shared with the merchant. So if a retailer's system is breached, the hackers won't have access to a user's financial information.").

While looking up directions using MapQuest on a computer is simple web browsing, which would be protected from law enforcement requests, using a mapping application like Google Maps on a smartphone transmits real time location information to Google. Users see the dot corresponding to their location move as they move, and have turned over this location information for the purpose of orienting themselves. Unlike the FitBit information, or regular cell phone data transfers, as seen at issue in *Davis*,[132] the smartphone users' location directly correlates to their purpose in sending this information to a third party. While the volume of transmissions is large, users are clearly aware that their location information is being used by a third party to convenience them.

C. *Alternative Proposals*

Scholars and practitioners have suggested other limits to the third-party doctrine. Many of these suggestions incorporate the same general ideas of the voluntary disclosure standard, but present other issues that make them undesirable options.

One suggestion is based on the automation, as opposed to human observer, distinction, mentioned briefly in the *Smith* opinion.[133] Championed by Matthew Tokson, this theory holds that since the machines processing most electronic information lack the ability to actually understand the content of the information, privacy is not lost when information is voluntarily disclosed to machines.[134] Under this proposal, information released to a third party would maintain its privacy if that third party used an automated process to collect and analyze the information.[135]

From an administrative perspective, this argument fails to address that businesses would have to develop a uniform procedure for receiving and analyzing data. As to the subjective reasonable expectations side of the equation, consumers would have to generally be aware of that procedure and know which companies use automated review as opposed to occasional human review to understand which information could be turned over to the government and which information is protected. However under this justification, the government could theoretically run automated searches of documents and communications without even a court order.[136] The administrative

132. U.S. v. Davis, 754 F.3d 1205 (11th Cir. 2014).

133. *See* Tokson, *supra* note 59.

134. Bedi, *supra* note 119, at 19–20 (citing *Tokson*, *supra* note 59); *see also*, Henderson, *supra* note 101, at 46.

135. *See* Henderson, *supra* note 101, at 47–48 (noting that automation feeds into consumers' opinions of how invasive an act feels.) Like a reasonable expectation of privacy, survey respondents did not mind spam filters looking for certain words in the content of their e-mails, but were more disturbed by targeted advertising based on similar automated e-mail reviews.

136. Henderson, *supra* note 101, at 48.

costs and practical consequences of such a regime would outweigh the benefits of what may or may not be additional privacy.[137]

The voluntary disclosure standard incorporates some of the ideas behind the automation principle, but in a more administrable format—as it relies on reasonable expectations of society, and not on how a particular website was reviewing traffic that week.

One critique of the use of voluntariness as a standard for the third-party doctrine is the idea that citizens "volunteer" this information ignores the realities of a world where it is difficult to function without disclosing information to third parties.[138] Justice Marshall suggested this in his dissent in *Smith*,[139] and some critics have suggested that without voluntarily disclosing information, today's individual "will not be able to live in society."[140] This hyperbolic statement seems to forget that many of the reasons people voluntarily disclose information is for convenience.[141] Online banking doesn't require waiting in line to talk to a teller, e-mail can be sent at any time of the day, and writing a Facebook status may be the fastest way to disseminate life updates to friends. But there are unquestionably people who live in society without all, or any, of these conveniences.[142] Admittedly, functioning in today's society without e-mail would be difficult, but many employers provide e-mail addresses for their employees and, at an individual level, these employees lack an expectation of privacy when using the computers and e-mail servers of their employers.[143]

Some proposed tests require courts to weigh numerous factors, and present the same administrative difficulties seen in the automation standard. One such test is a competing-interests test that considers the human/automation distinction as well as the disclosing individuals' underlying autonomy interest.[144] In addition to administrative concerns, that test presents a concern

137. The amount of additional privacy each person receives would depend on the various third parties they are giving information to, and how intimate they consider that information. A bank may use human review, opening that information up to the government, while a third-party advertiser may use an automated system for cataloging users, shielding a customer's e-mail address from law enforcement.

138. Orin Kerr, *Eleventh Circuit, disagreeing with the Fifth, holds Fourth Amendment protects cell-site records*, WASHINGTON POST: VOLOKH CONSPIRACY BLOG (June 11, 2014) http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/06/11/eleventh-circuit-disagreeing-with-the-fifth-holds-fourth-amendment-protects-cell-site-records.

139. Smith v. Maryland, 422 U.S. 735, 751–52 (1979).

140. Ghoshray, *supra* note 10, at 73–74.

141. United States v. Jones, 132 S. Ct. 945, 962 (2012) ("New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile.").

142. *See* Bedi, *supra* note 119, at 1, 27.

143. Employers often have an established preservation system and may search through e-mails for specific terms, or just monitor generally.

144. *See* Elsbeth Brotherton, *Big Brother Gets a Makeover: Behavioral Targeting and the Third-Party Doctrine*, 61 EMORY L.J. 555 (2012).

about horizontal inequity as it requires courts to determine on a case-by-case basis whether the third party's interests prevail over the individuals, while also factoring in the government's interests.[145]

Some courts and theorists have introduced the idea of ISPs as a "mere conduit" of the information, and therefore not considered an actual third party to the content of the e-mail.[146] The voluntary disclosure standard incorporates that idea, without having to deal with the same practical concerns of notice that the automation standard presents.[147] Some supporters of the third-party doctrine argue support for similar ideas by likening modern technology to what "old fashioned" criminals would have done.[148] Instead of sending an e-mail to a friend asking to borrow a shovel, the criminal would have had to leave her house and could have been seen by neighbors, possibly security cameras, and maybe even a police officer. Instead of actively stalking a victim, a criminal may resort to cyber-stalking to identify their victim's location. This analogizing, while creative, is unnecessary. It is difficult to imagine a court easily engaging in such analogizing or defending the chosen analogy against equally valid alternatives, and furthermore, analogizing every possible technological change to actions taken without technology only muddies the assertion that the doctrine needs to adapt to a society where information is regularly shared with third parties.

As shown with ECPA, Congress is capable of passing laws that protect individuals' electronic communications.[149] Ultimately, Congress can speak again if it finds the Court has failed to strike the appropriate balance between individual privacy concerns and law enforcement interests either by amending ECPA to require a warrant or passing a similar law that grants more protection to electronic information disclosed to third parties.

Conclusion

The third-party doctrine should be modified to better align with modern technology and information sharing, and to achieve this, courts should mod-

145. *Id.* at 592–95.

146. Most notably, Stephen Henderson's idea of a "limited third-party doctrine." *See* Henderson, *supra* note 101. However, Henderson only mentions this idea and then proposes to eliminate the doctrine entirely.

147. E.g., concern that citizens would have to know which entities count as third parties, and which count as mere conduits; just as they would have to know the methodology by which an entity processes its data.

148. See Kerr, supra note 2, at 577–79.

149. Congress has also stepped in to protect financial records (post-Miller) with the Right to Financial Privacy Act (RFPA), and acts like HIPAA, which place additional protections on customer information. For more examples of Congressional action taken to narrow the third-party doctrine, see Kerr, supra note 2, at 596–97. This is by no means a novel idea, as Chief Justice Taft wrote in Olmstead v. United States, 277 U.S. 438, 465–66 (1928) ("Congress may, of course, protect the secrecy of telephone messages by making them, when intercepted, inadmissible in evidence in federal criminal trials, by direct legislation, and thus depart from the common law of evidence.").

ify the standard used when determining which information loses Fourth Amendment protection. Limiting the third-party doctrine to information that is voluntarily disclosed maintains the protection of intimate data that citizens may not even realize is being collected, but still allows law enforcement officers to conduct preliminary investigations when they lack the probable cause required for a warrant. This standard fits in with Fourth Amendment jurisprudence, preserves well-established doctrinal concepts, and does not require a complete rebooting of law enforcement training and techniques. Instead, it grants citizens increased privacy and leaves open the option for Congress to take additional action, if needed.