Washington University Journal of Law & Policy

Volume 44 *Conceptualizing a New Institutional Framework for International Taxation*

2014

The Technology We Exalt Today Is Everyman's Master

Evan Peters
Washington University School of Law

Follow this and additional works at: https://openscholarship.wustl.edu/law_journal_law_policy

Recommended Citation

Evan Peters, *The Technology We Exalt Today Is Everyman's Master*, 44 WASH. U. J. L. & POL'Y 103 (2014), https://openscholarship.wustl.edu/law_journal_law_policy/vol44/iss1/11

This Note is brought to you for free and open access by the Law School at Washington University Open Scholarship. It has been accepted for inclusion in Washington University Journal of Law & Policy by an authorized administrator of Washington University Open Scholarship. For more information, please contact digital@wumail.wustl.edu.

The Technology We Exalt Today Is Everyman's Master[1]

Evan Peters*

I. INTRODUCTION

In *United States v. Jones*,[2] Justice Sotomayor rightly articulated the need to reformulate privacy law. In *Jones*, the Supreme Court unanimously held that the government's GPS placement on Antoine Jones's vehicle constituted a search warranting Fourth Amendment protection.[3] On the surface, the result appears to be a win for pro-privacy interests.[4] However, some scholars are cautious about what *Jones* portends for privacy law.[5] Even the Justices, while unanimous in judgment, differed in rationale. The Court split into three opinions, authored by Justices Scalia, Alito, and Sotomayor, respectively.[6]

Justice Scalia's opinion, joined by Justices Roberts, Thomas, and Kennedy, departed from the then-accepted formulation of what constituted a Fourth Amendment search,[7] finding the GPS placement

* J.D. (2014), Washington University School of Law; B.A. (2009), University of Michigan, Ann Arbor. I would like to thank Professor Mae Quinn for introducing me to the topic, to everyone on the *Journal* editing staff, and, most of all, to my family and friends for their patience and support.

1. United States v. White, 401 U.S. 745, 757 (1971) (Douglas, J., dissenting).
2. United States v. Jones, 132 S. Ct. 945 (2012).
3. The police acquired a warrant but did not fashion the GPS until after the warrant expired. All nine members of the Court found the warrantless placement of the GPS to be worrisome. *Jones*, 132 S. Ct. at 954, 964.
4. Jim Harper quoted the decision as a "big win for privacy." Jim Harper, *U.S. v. Jones: A Big Privacy Win*, CATO INST. (Jan. 23, 2012), http://www.cato-at-liberty.org/u-s-v-jones-a-big-privacy-win/.
5. Tom Goldstein called the decision "less of a pro-privacy ruling than many people" think. Tom Goldstein, *Why Jones is still less of a pro-privacy decision than most thought*, SCOTUSBLOG (Jan. 30, 2012, 10:53 AM), http://www.scotusblog.com/?p=138066.
6. *See Jones*, 132 S. Ct. at 945.
7. *See id.* at 947.

Washington University Open Scholarship

to be a search of Jones's physical effect.[8] While Scalia's formulation can be easily applied, it might open doors in privacy law that were slammed shut in the 1960s, when the Court declined to find a search in the mere presence of physical contact or trespass on a person's effects.[9]

Justice Alito, joined by Justices Breyer, Kagan, and Ginsburg, authored a scathing dismissal of Justice Scalia's decision.[10] Justice Alito applied the *Katz* expectation-of-privacy test to the facts, finding the long-term monitoring of Jones to be a search.[11] In finding such a search, Justice Alito embraced a mosaic theory of Fourth Amendment search protection, which aggregates all surveillance activity as related to an event in question in order to find a search.[12]

Justice Sotomayor issued a separate concurrence, though she agreed with parts of both Justice Scalia's and Justice Alito's opinions.[13] Justice Sotomayor wrote separately to indicate her

8. Justice Scalia cited the word "effects" in the Constitution to apply to property. U.S. CONST. amend. IV. In this case, the "effect" referred to Antoine Jones's car, despite the fact that it was not actually Antoine Jones's car but his wife's car. By focusing on the "effects" portion of the Fourth Amendment, Justice Scalia declined to apply the *Katz* test. *Jones*, 132 S. Ct. at 949.

9. In the landmark case of *Katz v. United States*, the Court reasoned that physical intrusion was not an accurate determination for Fourth Amendment cases. *See* 389 U.S. 347, 352–53 (1967) (holding the trespass doctrine enunciated in *Olmstead* and *Goldman* is no longer a controlling test).

10. In particular, Justice Alito called the majority's decision an attempt to solve twenty-first century privacy concerns using eighteenth century tort law. *See Jones*, 132 S. Ct. at 957.

11. *See id.* at 964. Justice Alito does not directly address short-term GPS monitoring, but the language in his opinion suggests Justice Alito would uphold short-term GPS monitoring. *See id.* at 958 (stating that there was no meaningful interference when the GPS device did not interfere with the operation of the vehicle). Further, Justice Alito stated that "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable." *Id.* at 964 (finding that society is comfortable with minor surveillance such as video cameras at stoplights). This, perhaps rightly, scares pro-privacy enthusiasts.

12. The mosaic theory asks for judges to aggregate all sequences of government activity to see whether, together, they could be seen as a search. Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012), *available at* http://www.volokh.com/category/mosaic-theory-of-the-fourth-amendment/. The mosaic theory is new; the original *Katz* analysis asked judges to evaluate each step of an investigation individually. *Id.*

13. *Jones*, 132 S. Ct. at 954. Specifically, Justice Sotomayor agreed with Justice Scalia's assertion that a physical intrusion is the baseline for Fourth Amendment protection. She also agreed with Justice Alito that under the *Katz* test, the actions taken by the government constituted a search. Justice Sotomayor also argued that short-term GPS monitoring would constitute a search. *See id.* at 956.

concern that technological advances are outpacing Fourth Amendment privacy concerns.[14] In her concurrence, Justice Sotomayor articulated this concern by stating, "[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[15]

While each of the three opinions communicates a new way to comprehend Fourth Amendment search protection, it is Justice Sotomayor's concurrence that will likely have the same historical impact that Justice Harlan's concurrence in *Katz* has had.[16] This Note will evaluate Justice Sotomayor's desire to modify the third party doctrine, an aspiration brought on by emerging technology. Part II will trace the Court's historical development of Fourth Amendment search protection law in the context of emerging technology, and will consider the role the third party doctrine has played in this development. Part III will examine current technology, the government's attempts to rectify gaps in the law resulting from the third party doctrine, and Justice Sotomayor's conclusion that it is up to the Court to fix the third party doctrine. Part IV will consider responses from the academic community to the third party doctrine. Finally, Part V will analyze how recent courts have grappled with the third party doctrine in the midst of emerging technology, and will conclude that the Supreme Court must reformulate its tests for privacy law.

II. HISTORY

The Fourth Amendment states that "the right of the people to be secure in their persons, houses, papers and effects, against

14. *See id.* at 957. Justice Alito is also aware of this concern, noting that cell phones and other wireless devices now permit wireless carriers to track the location of users without having to physically implant a GPS monitor. *See id.* at 963. Justice Scalia, perhaps unsurprisingly, does not address this concern.

15. *Id.* at 957.

16. The *Katz* test is articulated in Justice Harlan's concurrence as opposed to Justice Stewart's majority opinion. *Katz*, 389 U.S. at 360 (Harlan, J., concurring). *See also* John P. Elwood & Eric A. White, *What Were They Thinking?*, 15 GREEN BAG 2d 405, 409 (2012) (proclaiming that Justice Sotomayor's concurrence is the dynamic portion of the decision).

Washington University Open Scholarship

unreasonable searches and seizures shall not be violated."[17] This clause prevents the government from conducting an unreasonable search or an unreasonable seizure in an investigation. Of particular interest to this Note is what constitutes an unreasonable search and how technological developments over time have affected search and seizure jurisprudence.

*A. Search Pre-*Katz

Prior to *Katz*, decided in 1967, Fourth Amendment search protection relied on the presence of a physical trespass. In *Olmstead v. United States*,[18] a wiretap[19] was found to not be a protectable search because there was no physical trespass.[20] Chief Justice Taft declared, "The language of the [Fourth] [A]mendment cannot be extended and expanded to include telephone wires, reaching to the whole world from the defendant's house or office. The intervening wires are not part of his house or office."[21] Likewise, in *Goldman v. United States*,[22] the use of a detectaphone was found to not be a search.[23]

---

17. U.S. CONST. amend. IV. The second clause of the Fourth Amendment states, "[A]nd no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." *Id.*

18. 277 U.S. 438 (1928).

19. At the time, wiretapping, first used in the 1890s, was a relatively new procedure for U.S. law enforcement. William Lee Adams, *Brief History: Wiretapping*, TIME, Oct. 11, 2010, *available at* http://www.time.com/time/magazine/article/0,9171,2022653,00.html. *Olmstead* was the first case to establish wiretapping's constitutionality. *See id*.

20. In *Olmstead*, suspects were convicted of a conspiracy to violate the National Prohibition Act by unlawfully possessing, transporting, and importing intoxicating liquors. *Olmstead*, 277 U.S. at 456–57. The police obtained the evidence chiefly through the interception of telephone messages by wiretaps. *Id.* The wiretaps were executed in the basement of a large office building where the conspirators worked, and did not physically trespass on any of the conspirators' property. *Id.* The wiretaps were up and running for several months. *Id.*

21. *Id.* at 465. The Court was struggling with assessing the Fourth Amendment's role as applied to new technology. "[O]ur contemplation cannot be only of what has been, but of what may be. The progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping." *Id.* at 474 (Brandeis, J., dissenting) (internal quotation omitted).

22. 316 U.S. 129 (1942).

23. A detectaphone is a device that allows one to eavesdrop on a nearby conversation. Here, federal agents placed the detectaphone on the wall adjoining the defendants' office and listened to their conversations. Agents used this evidence to prosecute the defendants. *See id.* at 131–32.

While *Olmstead* and *Goldman* represent the Court's then-belief that an investigative act had to physically break through the constitutionally protected area to qualify as a search, this apparently bright line rule was subject to subtle distinction. This fine line was best exhibited in *Silverman v. United States*.[24] The facts in *Silverman* resembled the facts of *Goldman*,[25] except that the electronic listening device used in *Silverman* did penetrate the wall, whereas in *Goldman*, the detectaphone rested behind the wall.[26] The Court in *Silverman* found this penetration to be "an actual intrusion into a constitutionally protected area."[27]

B. Katz v. United States

Six years after *Silverman*, the Court fundamentally altered Fourth Amendment search protection in *Katz v. United States*.[28] Recognizing the impact technological advances were having on police investigations, the Court downplayed the importance of the constitutionally protected area.[29] The Court stated, "[T]he Fourth Amendment protects people, not places."[30] Thus, the presence of a physical intrusion was no longer a key element in search analysis. The Court instead asked whether the person knowingly exposed the information to the public, holding, "[W]hat he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[31]

---

24. 365 U.S. 505 (1961).

25. In *Silverman*, police officers obtained evidence through use of a spike mike. A spike mike is a microphone with a foot-long spike attached to it. The spike mike, like the detectaphone, is used to listen to conversations. The police officers placed the spike mike into a crevice that reached the suspect's home by way of a heating duct. *See id.* at 506.

26. *See id.* at 512 (Douglas, J., concurring). *See also Goldman*, 316 U.S. at 131.

27. *Silverman*, 365 U.S. at 512.

28. 389 U.S. 347 (1967). In *Katz*, the police suspected Katz of illegal gambling. The police placed an electronic listening device on the outside of a public telephone booth from which Katz placed his calls. The appellate court upheld the monitoring, citing the lack of physical intrusion into the constitutionally protected area. *See id.* at 348–49.

29. *See id.* at 351 (holding that "this effort to decide whether or not a given 'area,' viewed in the abstract, is constitutionally protected deflects attention").

30. *Id.*

31. *Id.*

Washington University Open Scholarship

In his concurrence, Justice Harlan established a two-part test to determine whether the Fourth Amendment protects what a person has preserved as private.[32] To find a protected search, Harlan's test requires first that "a person ha[s] exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[33] The *Katz* test reshaped the definition of what constitutes a search from one of physical trespass to an inquiry into both the subjective and objective reasonableness of the privacy expectation, based on one's intent to reveal the information and society's expectation of that intent.[34]

*C. Post-*Katz *Search and Emerging Technology*

Since *Katz*, the Court has grappled with technological advances amidst the reasonable expectation concerns. In *Smith v. Maryland*,[35] the Court found the use of a pen register[36] on a suspect's home phone did not constitute a search. The Court doubted that "people in general entertain any actual expectation of privacy in the numbers they dial."[37] While the defendant likely had the subjective intent to maintain his privacy, the Court found society did not have a reasonable expectation of privacy in information voluntarily given, and held that the use of the phone numbers did not violate the Fourth Amendment.[38]

---

32. *See id.* at 360–61 (Harlan, J., concurring).

33. *Id.* at 361.

34. Scholarship has largely supported this observation. *See, e.g.*, Caren Myers Morrison, *The Drug Dealer, The Narc, and The Very Tiny Constable: Reflections on United States v. Jones*, 3 CALIF. L. REV. CIRCUIT 113 (2012); William J. Stuntz, *The Distribution of Fourth Amendment Privacy*, 67 GEO. WASH. L. REV. 1265 (1999); Carol S. Steiker, *Second Thoughts About First Principles*, 107 HARV. L. REV. 820 (1994). *Contra* Orin Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004) (finding that property norms are still the basis of post-*Katz* search protection).

35. 442 U.S. 735 (1979).

36. A pen register is a mechanical device that records numbers dialed on a telephone. It does not record the contents of phone calls. The pen register in this case was installed at the telephone company to record the defendant's phone calls, believing the defendant to be the one harassing the witness. *See id.* at 736 n.1.

37. *Id.* at 742.

38. For a more in-depth discussion of *Smith*, see *infra* notes 83–101 and accompanying text.

In *Knotts v. United States*,[39] the Court dealt with another new form of police surveillance technology, the installation of a police beeper.[40] The beeper allowed agents to track the defendant's movements on a public road. The Court found that placing the beeper in a tin and selling it to the defendant was not a search.[41] The Court concluded that a person has no reasonable expectation of privacy when traveling on a public throughway.[42]

In 2001, the Court was faced with determining the constitutionality of thermal imaging, in *Kyllo v. United States*.[43] The Court found that a person has a reasonable expectation of privacy within their home as it relates to what can be acquired by powerful new technology.[44] The Court placed an emphasis on the suspect's effort to shield his information from public view.[45] This attempt to keep one's information secret, the Court found, is what makes the intrusion a search.[46]

As each of these Fourth Amendment technology cases indicates, the Court tends to afford protections where it finds a person has an

39. 460 U.S. 276 (1981).

40. A police beeper is a radio transmitter that, when activated, allows the police to track the beeper's movement. *Id.* at 277. In *Knotts*, the police suspected the defendant of manufacturing illicit drugs, and placed a beeper in a chloroform container that was then purchased by defendant. *Id.* at 278. The police tracked the traveling container on public highways to a cabin, where they discovered a drug lab. *Id.* at 279.

41. *Id.* at 285.

42. *Id.* at 281. The Court took particular interest in the fact that the information obtained from the beeper could have been obtained through visual observation of the defendant. *Id.* at 282. In *United States v. Karo*, 468 U.S. 705, 714 (1984), the Court found the obtainment of information by a police beeper used within a private residence to be a search, because a person does have a reasonable expectation of privacy in her home.

43. 533 U.S. 27 (2001). In *Kyllo*, the government suspected the defendant of growing marijuana in his house. *Id*. at 29. To grow marijuana in a house requires high-intensity heat lamps. *Id*. As such, police took a thermal imaging camera and pointed it at defendant's house. *Id*. at 29–30. The pictures revealed a high concentration of heat, which the government used as evidence against the defendant. *Id*. at 30.

44. *See id*. at 34.

45. *Id.*

46. The government cited *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986), as evidence that the use of high-powered technology does not always amount to a search. *Kyllo*, 533 U.S. at 37. The Court disagreed with the government, holding that people have a greater reasonable expectation of privacy in their homes than they do at an industrial area, where the photos in *Dow Chemical* were taken. *Id*.

Washington University Open Scholarship

active intent to keep the searched information secret.[47] Generally, if the Court finds a person is attempting to keep information secret, the Court is more willing to afford that effort Fourth Amendment search protection.[48] However, even when the Court finds that a person has a subjective intent to keep information private, if there is voluntary disclosure by the person, the Court's analysis changes. To assess whether a person has voluntarily disclosed information, the Court applies the third party doctrine.

D. Third Party Doctrine

Formulated prior to *Katz*, the third party doctrine is centrally concerned with disclosure. The doctrine focuses on methods through which the government acquires information about people it suspects of committing a crime. In gathering evidence, the government may employ one or both of two techniques without infringing on the Fourth Amendment: (1) eavesdropping; and (2) directly participating in a conversation, either personally or through a third party (characterized as a "false friend"). This "false friend" may use technology, such as a wiretap, to document the conversation.[49]

In *Hoffa v. United States*,[50] the Court concluded that the voluntary disclosure of information to a third party "false friend" without a wiretap is not a search.[51] The Court stated that the Fourth Amendment does not "protect a wrongdoer's misplaced belief that a

47. *But see* Smith v. Maryland, 442 U.S. 735, 743 (1979) (where the defendant was actively attempting to keep the content of his phone conversations secret from the police). In *Smith*, the Court agreed that the content was afforded protection. *Id*. However, the Court found the defendant had no expectation of privacy in information that he voluntarily turned over to a third party. *Id*. at 743–44. Here, the defendant surely knew he was giving the dialed phone numbers to the phone company. *See id*. at 743. Justice Marshall disputed this assertion in his dissent. *Id*. at 749 (stating he did not assume individuals know that the phone company monitors phone calls). *See infra* notes 83–101 and accompanying text.

48. *Compare* Knotts v. United States, 460 U.S. 276 (1981) (where the defendant was out in the public), *with* Kyllo v. United States, 533 U.S. 27 (2001) (where the defendant was inside his own home, behind his own walls).

49. *See* JOSHUA DRESSLER & GEORGE C. THOMAS III, CRIMINAL PROCEDURE: PRINCIPLES, POLICIES AND PERSPECTIVES 100 (4th ed. 2009).

50. 385 U.S. 293 (1966).

51. *See id.* at 302–03. In *Hoffa*, the defendant was suspected of bribing a jury. *Id*. at 294–95. Hoffa's friend told the government Hoffa had confessed to him that he bribed members of the jury, and the friend later testified to that fact at trial. *Id*. at 295.

person to whom he voluntarily confides his wrongdoing will not reveal it."[52] At the heart of the analysis is the belief that the defendant initiates the conversation and gives up the information voluntarily. Therefore, the defendant is afforded no protection regarding what a third party does with the information voluntarily provided.

In *On Lee v. United States*,[53] a government agent, unbeknownst to the suspect, secretly listened to a conversation as a suspect gave information to a "false friend."[54] The government agent testified about the conversation in court. The Court found that even though the suspect did not voluntarily give his information to the government agent secretly listening, the information given to the informant did not constitute a search because the suspect voluntarily gave his information to a third party.[55] Even the act of an agent impersonating a prospective buyer was not considered a search.[56] The Court reasoned that so long as the information was given voluntarily, use of the information given was not a search.[57]

Lopez v. United States[58] stretched this analysis to cover undercover agents who wear tape-recording equipment.[59] The Court

52. *Id.* at 302.

53. 343 U.S. 747 (1952).

54. *Id.* at 749. In *On Lee*, the government thought the suspect was trafficking narcotics through his store. *Id.* As a result, they equipped Chin Poy, a former employee of the suspect, with a microphone that was wired to pick up sound. *Id*. The government agents stationed themselves directly outside the suspect's store. *Id*.

55. It is notable that *On Lee* was decided before the *Katz* expectation of privacy test. As a result, much of the Court's deliberation focused on whether there was a physical trespass. *Id.* at 752–53. The Court concluded that because On Lee consented to Chin Poy's entrance into the store, it was not a physical trespass. *Id*. at 752–53. This line of reasoning is not followed in future cases. However, the second ground for the Court's decision, that the suspect was talking confidently and indiscreetly, allowed for *On Lee* to survive for future decisions.

56. *See* Lewis v. United States, 385 U.S. 206 (1966).

57. *See id*. at 212. In *Lewis*, the agent, identifying himself as Jim, telephoned the defendant to ask if he could purchase some marijuana, telling the defendant they had mutual friends. The defendant invited the agent to his home, where they discussed prospective future business. They finalized the arrangement and made a second deal two weeks later. *See id.* at 207. The Court reasoned that finding a Fourth Amendment violation would unduly limit a government agent's ability to be deceptive. *Id*. at 210.

58. 373 U.S. 427 (1963).

59. *See id.* In *Lopez*, the government agent approached the defendant twice to ask about the entertainment at the defendant's establishment. *Id*. at 431. The defendant, seeking to avoid paying taxes, talked to the undercover agent about an "arrangement." *Id*. At the last of these meetings, the undercover agent recorded their conversation and presented the recording as evidence. *Id.* at 432. As with *On Lee*, both *Lewis* and *Lopez* were decided before *Katz*.

Washington University Open Scholarship

reasoned that since an undercover agent may testify on the basis of a conversation, it was reasonable to allow the undercover agent to record the conversation. Because the information given to the recorded undercover agent was given voluntary, the Court did not find the government intrusion to be a search.[60]

Underlying each of these cases is the rationale that it is immaterial whether a party knows that his disclosure of information will be used against him. Because each of these cases was decided prior to *Katz*, the Fourth Amendment search protection analysis focused on the trespass of the search as opposed to the reasonableness of the intrusion.

E. Third Party Doctrine, Katz*, and Emerging Technology*

The Court connected the *Katz* two-part test with the third party doctrine in *White v. United States*.[61] In *White*, a third party recorded conversations with a suspect, much like in *Lopez*.[62] The Court afforded no Fourth Amendment protection to the acquisition of electronically obtained evidence, because the privacy interest failed the *Katz* two-part test.[63] The Court concluded that a suspect had no expectation of privacy when he articulated information to a third party.[64] The Court reasoned that this applied to a third party wearing an electronic device: "If the law gives no protection to the wrongdoer whose trusted accomplice is or becomes a police agent, neither should it protect him when that same agent has recorded or transmitted the conversations which are later offered in evidence to prove the State's case."[65] The Court recognized the complications of

60. Because the device in question was not planted by means of an unlawful physical intrusion, the use of an electronic device by the undercover agent was not considered a search. *Id.* at 439.

61. 401 U.S. 745 (1971).

62. *See id.* at 746–47. In *White*, the defendant engaged in four separate conversations with a government informant, who was equipped with an electronic monitoring device. *Id.* Government agents listened-in on these conversations and later testified about what was on the recording. *Id.* It is this testimony that was under dispute, not the actual introduction of the recording device. *Id*. However, the Court still looked at whether the information found on the electronic recording device was a search. *Id.* at 747.

63. *See id.* at 747.

64. *See id.* at 749.

65. *Id.* at 752.

attaching the two-part test to electronically acquired evidence, acknowledging that the Court should "not be too ready to erect constitutional barriers."[66] Still, the Court looked favorably on the use of electronic monitoring, citing the practice as "a more accurate version" of evidence.[67]

In his dissent, Justice Douglas chastised the Court for failing to comprehend the power that electronic monitoring would afford the government, arguing that "electronic surveillance is the greatest leveler of human privacy ever known."[68] Justice Douglas believed electronic surveillance would have a long-range impact that the Founders did not grasp, and that the Court's conception of societal expectations needed to be adjusted to account for new technology.[69] Justice Douglas concluded that the "use of electronic surveillance . . . uncontrolled, promises to lead us into a police state."[70]

Justice Douglas then performed the same *Katz* test the majority had, but came to a different result, due, in part, to the evolution of technology in Fourth Amendment search protection. Justice Douglas focused heavily on society's expectation of privacy and its ability to engage in private conversations.[71] By focusing on these societal considerations, Justice Douglas concluded that the electronic surveillance performed in *White* failed the *Katz* test and was thus a search.[72]

---

66. *Id.* at 753. The Court championed the use of electronic recordings in this instance, finding an electronic recording "more reliable" than "the unaided memory of a police agent." *Id.* The Court focused heavily on the accuracy of the electronic recording, and did not give any insight into whether the electronic recording itself was a violation, a consideration brought up by both Justice Douglas and Justice Harlan in their dissents. *See id.* at 762 (Douglas, J., dissenting) (believing that electronic surveillance must be subject on its own to Fourth Amendment search protection); *see also id.* at 786 (Harlan, J., dissenting) (arguing that electronic monitoring has no place in our society if it is restricted only by the self-restraint of enforcement officials).

67. *See id.* at 753.

68. *Id.* at 756 (Douglas, J., dissenting).

69. *See id.*

70. *Id.* at 760 (Brennan, J., dissenting).

71. *See id.* at 763. Chiefly, Justice Douglas focused on how a conversation would be undertaken if speakers knew the conversation was not private. *Id*.

72. Interestingly, Justice Douglas wrote a concurring opinion, joined by Justice Brennan, in *Katz*. 389 U.S. 347, 359 (1967) (Douglas, J., concurring). In his concurrence, Justice Douglas took particular issue with any attempt by the Court to articulate a clear line of acceptable

Washington University Open Scholarship

Justice Harlan shared Justice Douglas's concern about the evolution of electronic surveillance, focusing on "the constitutional validity of instantaneous third-party electronic eavesdropping."[73] Yet, Justice Harlan applied the *Katz* test in a different manner than Justice Douglas, arguing society's expectations of privacy were shaped by prior Court decisions on what is an appropriate expectation of privacy.[74] Accordingly, Justice Harlan focused on the extent of the intrusion.[75] In this case, Justice Harlan concluded that the practice of electronic monitoring, here through a third party, would undermine society's expectation of privacy and "sense of security in dealing with one another that is characteristic of individual relationships between citizens in a free society."[76] Justice Harlan did, however, "leave room for the employment of modern technology in criminal law enforcement."[77]

According to Justice Douglas and Justice Harlan, the primary third party doctrine inquiry, whether information is voluntarily disclosed, should no longer be the pertinent question. Instead, the question should be whether both the individual and society have a reasonable expectation of privacy in the information disclosed, even

---

electronic eavesdropping without a warrant. *Id.* Here, again, Justice Douglas worried about unfettered electronic surveillance without Fourth Amendment search protection. *Id*. at 360.

73. White v. United States, 401 U.S. 745, 769 (1971) (Harlan, J., dissenting). Justice Harlan noted that the prevalence of electronic surveillance was making feasible the Orwellian Big Brother. *Id.* at 770. Harlan cites Alan Westin's book *Privacy and Freedom* to show that police officers are cooperating parties that "'wear[] . . . concealed device[s] that record[] . . . conversation[s] or broadcast[] [them] to other[] [police officers] nearby . . . tens of thousands of times each year.'" *Id.* (citing ALAN WESTIN, PRIVACY AND FREEDOM 131 (1967)). Justice Harlan also wrote a separate dissent to discuss his dissatisfaction with the majority's decision to not overrule *On Lee*. *See id.* at 780. In particular, he argued the "validity of the trespass rationale was questionable" at best and no longer relevant, given the ruling in *Katz*. *Id.* at 774. Further, Justice Harlan found the prior trespass rationale, central to Fourth Amendment search protection, to "have been destroyed." *See id.* at 784.

74. *See id.* at 786.

75. *See id.* Another landmark Fourth Amendment case, *Terry v. Ohio*, had recently been decided. 392 U.S. 1 (1968). While *Terry* focused on the necessity of a warrant for a police stop, Justice Harlan found the policy concern in *Terry*, namely the self-restraint required by law enforcement officials, to be particularly relevant to the search protection discussion in *White*. *See id.* It is unclear whether a minor intrusion would be acceptable for Harlan under *White*.

76. *Id.* at 787.

77. *Id.* at 790. Again, Justice Harlan did not explain just what room should be given to technology. However, he did suggest that the issue should be decided "in the stream" of Fourth Amendment search protection. *Id.*

if it is voluntarily disclosed. Thus, the technology involved with the disclosure becomes a critical component in the third party doctrine.

A few years later, in *United States v. Miller*,[78] the Supreme Court applied the third party doctrine to bank records.[79] The Court reasoned that society did not have a sufficiently reasonable expectation of privacy in bank records where the defendant voluntarily gave his information to the bank. The Court explained:

> This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[80]

In his dissent, Justice Brennan pushed back on the third party doctrine, arguing that the defendant did not forsake all of his Fourth Amendment rights when he willfully gave his information to the bank. Justice Brennan rationalized that, since everyone essentially needs a bank account, it does not follow that society then expects a bank might give a person's bank information to the police. If such were the case, then all bank information would be public.[81] To allow a policeman to access bank records upon request "opens the door to a vast and unlimited range of very real abuses of police power," Justice Brennan argued.[82]

Smith v. Maryland[83] addressed the application of technology to the third party doctrine.[84] In *Smith*, the Court limited its Fourth

78. 425 U.S. 435 (1976).

79. *See id.* In *Miller*, the government suspected the defendant of operating an illegal distillery. *Id*. at 436. As a result, the government requested copies of checks and other bank records from the defendant's bank. *Id.* The defendant moved to suppress this evidence, arguing he had a reasonable expectation of privacy that the documents would be kept in secret, pursuant to the Bank Secrecy Act of 1970. *Id*. Ironically, while the bank kept the records at the behest of the government to keep them secret, it was only because the bank complied that the documents could be shared with the government. *See id.* at 443.

80. *Id.*

81. *See id.* at 451 (Brennan, J., dissenting).

82. *Id.*

83. 442 U.S. 735 (1979).

84. *See id.* In *Smith*, a robbery victim gave a description of her assailant to the police. *Id.* at 737. After giving the description, the victim began seeing a car that matched the assailant's

Washington University Open Scholarship

Amendment review to the question of whether the police committed a violation when they gathered information on the defendant through the phone company, a third party. The Court avoided the question of whether it was an electronic intrusion[85] and instead focused on whether the defendant had an expectation of privacy regarding the phone numbers he dialed.[86] The Court concluded that a person does not have an expectation of privacy in such a context.

As to the first prong of the *Katz* test, whether the defendant himself harbored any expectation of privacy, the Court reasoned that since subscribers see their bills, they must realize that the phone company has the means of cataloging the numbers dialed.[87] The Court explained, "[I]t is too much to believe that telephone subscribers . . . harbor any general expectation that the numbers they dial will remain secret."[88] The Court rationalized that a person, by voluntarily dialing the numbers, has consented to the phone company's release of that information.[89]

As to the second prong, whether society has an expectation of privacy regarding the phone numbers they dial, the Court, invoking the third party doctrine, found that this expectation would be unreasonable. The Court said, "This Court consistently has held that a person has no legitimate expectation of privacy in information he

---

vehicle around her house. *Id*. Then, the victim began receiving threatening phone calls from a man identifying himself as the robber. *Id*. The victim went back to the police, who found the defendant by running a trace on the vehicle. *Id.* Then, the police wiretapped the defendant's phone through the phone company without a warrant. *Id*. The device used to wiretap the phone company was a pen register. *Id.* A pen register is a device that traces outgoing signals from a specific phone or computer to their destination, producing either a list of phone numbers or Internet addresses. *Id*. at 736. A pen register does not provide any substantive information, such as the content of the phone conversations or websites. *See Pen Register*, LEGAL INFO. INST. (Aug. 19, 2010), http://www.law.cornell.edu/wex/pen_register.

85. The Court noted that because the pen register did not acquire the content of messaging, the pen register did not require heightened scrutiny like a listening device. *Smith*, 442 U.S. at 741.

86. *See id.* at 742. This information is called envelope information, because it is information that can be found on the outside of a mailed letter, as opposed to content information, which is information that can be found inside the mailed letter. *See* Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2112 (2009).

87. *Smith*, 442 U.S. at 743.

88. *Id.*

89. *Id.*

voluntarily turns over to third parties."[90] Similar to the first prong, because people voluntarily use their phones, they voluntarily turn over the numbers dialed to the phone company, assuming the risk that the phone company will turn over those numbers to the police.[91] As a result, the wiretap was not held a search.[92]

Justice Stewart, along with Justice Brennan, disagreed with this final point. Justice Stewart reasoned that "numbers dialed from a private telephone . . . are not without content."[93] Because phone numbers by themselves can reveal persons and places dialed, it did not follow that society has no expectation of privacy in the disclosure of phone numbers to a third party.[94] Because society does not expect this disclosure, Justice Stewart would have held the electronic wiretap a search.[95]

Justice Marshall, along with Justice Brennan, leveled a critique of the first prong of the Court's analysis, arguing that "it does not follow that [a person] expect[s] this information to be made available to the public in general or the government in particular."[96] Further, "[t]hose 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."[97] Justice Marshall understood that the notion that "the defendant presumably had exercised some discretion in deciding who should enjoy his confidential communications" is an incorrect presumption.[98] The pen register, by automatically recording the information, prevented the defendant from exhibiting any choice in the matter. As such, according to Justice Marshall, the *Katz* analysis "depends not on the

90. *Id.* at 743–44 (citing *Miller*, 425 U.S. at 442–44).

91. *See id.* at 744. The Court did not address whether it was reasonable but only whether people do it on a day-to-day basis.

92. *Id.* at 746.

93. *Id.* at 748 (Stewart, J., dissenting).

94. *See id.* Justice Stewart also took issue with the fact that the phone numbers were dialed from inside the defendant's home, noting that under the first prong, a person has a reasonable expectation of privacy in numbers dialed from within her own home. *See id.* at 747.

95. Justice Stewart also disregarded the technological advancement of the wiretap and merely assessed whether the phone numbers fell under *Katz*, concluding that they did. *See id*. at 747–48 (Stewart, J., dissenting).

96. *Id.* at 749. (Marshall, J., dissenting).

97. *Id.*

98. *Id.*

Washington University Open Scholarship

risks an individual can be presumed to accept when imparting information to third parties, but on the risks he should be forced to assume in a free and open society."[99]

This strict reading of the third party doctrine was based on Justice Marshall's fear of "unregulated government monitoring" through the use of new technology, such as pen registers.[100] To restrict the government's use of this new technology, Justice Marshall sought to narrow the third party doctrine to the purposes for which the acquiring party obtains the information. In this instance, the defendant volunteered his information "solely for the phone company's business purposes."[101] Therefore, the defendant retained a privacy interest in the phone numbers when used for something else, such as a government investigation.

Following the aforementioned cases, the third party doctrine has become a zero-sum game for citizens. Citizens have a choice: they can either keep their information strictly private or give up all Fourth Amendment rights to the information, regardless of whether they give up that right knowingly or unknowingly, willingly or unwillingly.[102] In other words, "as technology becomes more embedded in society, consumers will be increasingly forced to waive their Fourth Amendment rights in order to obtain vital goods and services."[103]

III. THE THIRD PARTY DOCTRINE'S STRANGLEHOLD ON TODAY'S PRIVACY LAW

Since *Miller* and *Smith*, consumer technology can now be found in most U.S. households.[104] Products such as the personal computer and

99. *Id.* at 750. Justice Marshall cited Justice Harlan's *White* dissent, finding it important that the "task of the law [is] to form and project, as well as mirror and reflect," and that "we should not . . . merely recite . . . risks without examining the desirability of saddling them upon society." *Id.* (citing *White*, 401 U.S. at 786).

100. *Id.* at 751.

101. *Id.* at 752.

102. *See* Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211, 245 (2006). In their article, Brenner and Clarke push back against the assumption of the risk doctrine imbedded in the third party doctrine. *See id.* at 280.

103. *Id.* at 245–46.

104. For instance, in 2011, thirty-two years after *Smith*, CNN reported that 90 percent of Americans owned some form of consumer technology. Amy Gahran, *Report: 90% of*

the smartphone have allowed the average American to access their personal calendars, notes, e-mails, and bank records at home, and to make purchases on-the-go.[105] As a result, technology concerns under the *Katz* test no longer focus on what technology police possess that the general public does not, but instead focus on what technology the general public has access to that the police can utilize in a search.[106]

New technology presents an obvious flaw in the third party doctrine's ability to protect the American citizen. Take email, for example. Alex sends Bob an e-mail through his Yahoo! e-mail account. While Alex initially has a privacy interest in this e-mail, his disclosure to Bob relinquishes that right through the third party doctrine, and Bob may disclose the e-mail to government authorities. However, Yahoo! the company may disclose the email, as well, because they have also "seen" the e-mail. The government can compel Yahoo! to disclose Alex's e-mail, and Alex cannot object because he has lost his privacy interest.[107] This is troubling, because the same logic extends to someone who uses the internet through an internet service provider (ISP). Under the third party doctrine, that

---

Americans own a computerized gadget, CNN (Feb. 3, 2011), http://www.cnn.com/2011/TECH/mobile/02/03/texting.photos.gahran/. In addition, PC sales had risen from 48,000 in 1977 to 125 million in 2001. Michael Kanellos, *PCs: More than 1 billion served*, CNET (June 30, 2002), http://news.cnet.com/2100-1040-940713.html. Further, in 2009, 47 percent of Americans used online banking. *See* Lance Whitney, *Online Banking is Booming*, CNET (June 16, 2009), http://news.cnet.com/8301-1001_3-10265409-92.html.

105. Average Americans can use wireless broadband access, Wi-Fi (wireless local area network), and wireless ISP (internet service provider) on their smartphones or computers to perform these activities, perhaps soon at no subscription cost to the consumer. *See* Christina Thomas, *Google 2013: Could Wireless Internet Be Free Soon!?*, TECHNORATI (Jan. 24, 2013), http://technorati.com/business/article/google-2013-could-wireless-internet-be/. *See also* MARY J. CRONIN, BANKING AND FINANCE ON THE INTERNET (1997) (explaining the impact financial service institutions can have in the marketplace by embracing the internet).

106. *See* Kyllo v. United States, 533 U.S. 27 (2001). In addition to addressing privacy interests in a home, in *Kyllo*, Justice Scalia expounded upon the fact that the thermal imaging device the police used was "not in general public use." *Id.* at 34. *See also supra* notes 43–46 and accompanying text.

107. One only needs look at the recent controversy surrounding General David Petraeus to see how easy it is for the FBI to look at a consumer's e-mails. The Department of Justice will not release exactly how they obtained the scandalous e-mails, but they purport their tactics were legal. *See* Scott Shane, *Online Privacy Issue is Also in Play in Petraeus Scandal*, N.Y. TIMES, Nov. 13, 2012, *available at* http://www.nytimes.com/2012/11/14/us/david-petraeus-case-raises-concerns-about-americans-privacy.html?_r=0. In essence, when the FBI searched Paula Broadwell's e-mail in relation to a harassment complaint, they were able to look at older, non-protected e-mails in her account, which revealed the affair. *See id.*

Washington University Open Scholarship

person will have relinquished any privacy rights if the ISP chooses to disclose such information.

Utilizing the third party doctrine, courts have increasingly concluded that a person loses her privacy interest when she interacts with technology.[108] Faced with this troubling trend, Congress has attempted to parry back.

A. Congress and the Third Party Doctrine's Technology Conundrum

Recognizing the privacy hole created by new technology under the third party doctrine, Congress acted to fill the gap with the Electronic Communications Privacy Act of 1986 (ECPA)[109] and, sixteen years later, the Stored Communications Act (SCA).[110] Despite these noble attempts, these statutes have proven ineffective.[111] In fact, the U.S. government continues to obtain a great deal of personal information from private citizens. From July 2012 to December 2012,

108. Courts have largely concluded there is no privacy interest in a wide array of information held by third parties. United States v. Suarez-Blanca, No. 07-CR-0023-NHS/AJB, 2008 WL 4200156, at *8 (N.D. Ga. 2008) (finding no privacy interest in historical cell site information). *See also* United States v. Hynson, No. 05-576, 2007 WL 2692327, at *5 (E.D. Pa. 2007) (cell phone records); United States v. Phibbs, 999 F.2d 1053, 1077-78 (6th Cir. 1993) (credit card statements); United States v. Starkweather, No. 91-30354, 1992 WL 204005, at *1-2 (9th Cir. 1992) (kilowatt consumption from electric utility records); United States v. Willis, 759 F.2d 1486, 1489 (11th Cir. 1985) (motel registration records); and United States v. Hamilton, 434 F. Supp. 2d 974, 979 (D. Or. 2006) (employment records).

109. *See* 18 U.S.C. §§ 2510–2522 (1986). The ECPA was designed to protect in-transit communications, such as wire transfers, from being intercepted.

110. *See* 18 U.S.C. §§ 2701–2712 (2002). The SCA is a subset of the ECPA. It specifically protects stored data transmissions, such as e-mails, from being intercepted through an ISP. Other important subsets of the ECPA include the Wiretap Act, codified at Title I of the ECPA, 18 U.S.C. §§ 2510–2522 (2002), which protects voice communications, as well as certain electronic communications. The exclusionary rule applies to voice communications under the Wiretap Act, but it does not apply to electronic communications under either the Wiretap Act or the SCA. *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 316–17 (4th ed. 2012).

111. This is due to substantial loopholes in the statutes. One such loophole is the compelled e-mail disclosure rule. Under this rule, an e-mail that is sitting in an inbox opened for 180 days is considered abandoned and loses Fourth Amendment protection. *See* Orin Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1218 (2004). The U.S. Congress is debating closing the loophole; an amendment to the ECPA that would close the loophole has left committee and gone to the floor. *See* Hanni Fakhoury, *2012 in Review: Steps in the Right Direction for Email Privacy*, ELEC. FRONTIER FOUND. (Dec. 26, 2012), https://www.eff.org/deeplinks/2012/12/2012-review-steps-right-direction-email-privacy.

the U.S. government made 21,389 requests for user data from Google, alone.[112]

Professor Daniel J. Solove has criticized the effectiveness of legislative efforts to keep up with Fourth Amendment search protection.[113] Recognizing that citizens must "plug in"[114] to society, Professor Solove chastised Congress's statutory regime as archaic and pedantic.[115] In particular, he focused on the holes in the regime, "such as information collected by websites."[116] As a result, he concluded that Congress has failed to protect the privacy interests of its citizens, and that it is up to the Court to rid us of this "gap-riddled statutory regime . . . [and] reverse *Smith v. Maryland* and *United States v. Miller*."[117]

Recently, Senator Rand Paul (R-Ky) introduced a bill in the Senate to change the current statutory regime.[118] If passed, Senator

112. *See Transparency Report: What it takes for governments to access personal information*, GOOGLE BLOG (Jan. 23, 2013), http://googleblog.blogspot.com/2013/01/transparency-report-what-it-takes-for.html.

113. *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2002).

114. *Id.* at 1089. Professor Solove details the ways in which citizens disclose information to a third party, from connecting to an ISP, to opening an account with a cable company, to the various records citizens maintain with doctors, lawyers, and businesses. *See id.*

115. *See id.* at 1138.

116. *See id.* at 1148. Additionally, records kept by internet retailers and websites are not protected under the ECPA. *See id.*

117. *Id.* at 1151. However, because the Fourth Amendment's primary remedy for violations is the exclusionary rule, Professor Solove recognizes that Fourth Amendment search protection is not enough to adequately protect citizens, and that some form of a statutory regime must exist. *See id.*

118. In May of 2013, NSA programmer Edward Snowden released NSA documents to the *Guardian* and the *Washington Post*, both of which subsequently released the information to the public. Glenn Greenwald & Ewen MacAskill, *NSA Prism program taps into user data of Apple, Google and Others*, GUARDIAN, June 6, 2013, *available at* http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data; Barton Gellman & Laura Poitras, *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*, WASH. POST, June 6, 2013, *available at* http://articles.washingtonpost.com/2013-06-06/news/39784046_1_prism-nsa-u-s-servers. Edward Snowden also sat down for a video interview. *Video Interview by Laura Poitras and Glenn Greenwald with Edward Snowden*, GUARDIAN, June 9, 2013, *available at* http://www.theguardian.com/world/video/2013/jun/09/nsa-whistleblower-edward-snowden-interview-video. President Obama quickly responded, stating, "Nobody is listening to your telephone calls." Lucy Madison, *Obama: "Nobody is listening to your telephone calls,"* CBS NEWS, (June 7, 2013), http://www.cbsnews.com/8301-250_162-57588239/obama-nobody-is-listening-to-your-telephone-calls/. Since the disclosure, more revelations about the NSA's technological reach have come to light. Glenn Greenwald, *XKeyscore: NSA Tool Collects*

Washington University Open Scholarship

Paul's bill, the Fourth Amendment Preservation and Protection Act of 2013, will drastically curb the ability of law enforcement officials to use the third party doctrine.[119] As of November 2013, the bill is currently in committee.[120]

B. The Supreme Court's Task

Congress has thus far failed to keep up with technology in protecting our privacy interests. This is in large part due to Congress's inability to legislate around the rigid third party doctrine. Because of the third party doctrine, society has no reasonable expectation of privacy in information disclosed to a third party.[121] Thus, it is up to the Supreme Court to regulate where the legislature has failed to act.[122]

Nearly Everything a User Does on the Internet, GUARDIAN, July 31, 2013, *available at* http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data. Of particular note is the disclosure that the federal government has not only mass collected Americans' telephone communications data but has kept these collections from Congress. Peter Wallsten, *House Panel Withheld Document on NSA Surveillance Program from Members*, WASH. POST, Aug. 16, 2013, *available at* http://articles.washingtonpost.com/2013-08-16/politics/41417421_1_briefings-congress-surveillance-program. Following the disclosure, President Obama reassured the public that changes will be made to both the NSA mass surveillance program and to the United States Foreign Intelligence Surveillance Court ("FISA Court"), the secret court that oversees the constitutionality of NSA programs. Scott Wilson & Zachary A. Goldfarb, *Obama announces proposals to reform NSA surveillance*, WASH. POST, Aug. 9, 2013, *available at* http://articles.washingtonpost.com/2013-08-09/politics/41225487_1_president-obama-news-conference-edward-snowden. While the discussion surrounding the NSA surveillance program does concern the constitutionality of mass surveillance programs under the Fourth Amendment, this Note is focused on how the third party doctrine impacts technology and individual surveillance.

119. Fourth Amendment Preservation and Protection Act of 2013, S. 1037, 113th Cong. (2013), *available at* http://beta.congress.gov/bill/113th-congress/senate-bill/1037.

120. *Id.*

121. As Justice Harlan noted in his *White* dissent, society's "expectations, and the risks [individuals] assume, are in large part reflections of laws that translate into rules, and the customs and values of the past and present." United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting). In other words, society's expectations are based primarily on what the Court deems them to be. If the Court applied the third party doctrine differently, society's expectations would adjust. *See supra* notes 61–77 and accompanying text.

122. *See* Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1515 (2010) (arguing it is up to courts to craft rules when the legislature has not adopted an all-inclusive regime). *But see* Unites States v. Jones, 132 S. Ct. 945, 963–64 (2012) (Alito, J., concurring) (stating that in the midst of dramatic technological change, this problem seems best left to the legislature).

Justice Sotomayor agrees. As Justice Sotomayor wrote in *United States v. Jones*, it is time "to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[123] Further, the third party doctrine "is ill suited to the digital age, in which people reveal a great deal of information in the course of carrying out mundane tasks."[124]

Applying the *Katz* test to the facts in *Jones*, Justice Sotomayor concluded that neither prong was satisfied. She doubted that people truly recognize they are forsaking privacy rights when they interact with technology on an everyday basis.[125] Further, Justice Sotomayor contended that, even assuming people do know they are forsaking rights, the second prong of the test regarding societal expectations is not satisfied. She doubted "that people would accept without complaint the warrantless disclosure to the Government of a list of every website they had visited in the last week, or month, or year."[126]

Even though she found neither prong of the *Katz* test satisfied, Justice Sotomayor argued that the third party doctrine and its emphasis on secrecy stands in the way of protecting one's privacy.[127] According to Justice Sotomayor, the only way to properly apply the *Katz* Test is "if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy."[128] For this reason alone, Justice Sotomayor explained she "would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is . . . disentitled to Fourth Amendment protection."[129]

---

123. *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

124. *Id.*

125. *See id.* In particular, Justice Sotomayor discussed the ways in which people use technology and inadvertently voluntarily release their privacy rights. *Id.* She noted that people "disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers." *Id.* Justice Alito responded to Justice Sotomayor's critique, commenting that people may actually prefer "increased convenience . . . at the expense of privacy." *Id.* at 962 (Alito, J., concurring).

126. *Id.* at 957 (Sotomayor, J., concurring).

127. *See id.*

128. *Id.*

129. *Id.* (citing Smith v. Maryland, 442 U.S. 735, 749 (1979)). Justice Sotomayor chose not to posit a new test, as she joined the majority's reasoning that the government physically intruded upon the defendant's "effects." *Id.*

Washington University Open Scholarship

IV. RESPONSES TO THE THIRD PARTY DOCTRINE AND TECHNOLOGY[130]

There has been a variety of responses to the third party doctrine, the question of whether it should be reformed, and, if it should be reformed, how and by whom. For example, while Justice Sotomayor is open to a judicial reinterpretation of the third party doctrine, Professor Orin Kerr[131] strongly insists that the Court should not meddle with the third party doctrine.[132] In his article "The Case for the Third-Party Doctrine," Professor Kerr argues that the third party doctrine provides authorities with a clear window to prosecute savvy criminals.[133] More importantly, he argues, the third party doctrine is unambiguous.[134] Without the third party doctrine as it is currently articulated, "courts would face the difficult challenge of creating a clear regime of Fourth Amendment protection for third party information."[135]

Professor Kerr believes the third party doctrine is essential to the government's ability to bring criminals to justice, because it "requires technological neutrality."[136] Using legendary Teamster "Jimmy" Hoffa as an example, Professor Kerr argues that if Hoffa had the option of using a third party to hide his misdeeds, he would have done so.[137] The third party doctrine prevented Hoffa from using that third party; it encapsulated Hoffa's misdeeds to Hoffa alone and prevented him from personally escaping justice.[138]

---

130. As will be discussed *infra*, Professor Kerr and Professor Epstein's solutions to the third party doctrine's technology conundrum are to keep the third party doctrine as it currently stands.

131. Professor Orin Kerr is the Fred C. Stevenson Research Professor of Law at George Washington University Law School.

132. For instance, Professor Kerr finds fault with the move towards a mosaic theory of search protection. *See* Kerr, *The Mosaic Theory of the Fourth Amendment*, *supra* note 12.

133. Orin Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 564 (2009).

134. *See id.* at 565.

135. *Id.*

136. *Id.* at 580.

137. *Id.*

138. *See id* at 588. Indeed, in his article, Professor Kerr argues Fourth Amendment privacy rights are a two-way street when it comes to technology. That is, if we fear that Fourth Amendment search protection can be threatened by technological practices, so too must we fear that they may be expanded. *See id.*

Even more important to Professor Kerr is the clarity provided by the third party doctrine, which he believes is imperative, given the muddiness of Fourth Amendment jurisprudence.[139] Indeed, it is a clear prophylactic rule: if A tells a secret to B, A loses that privacy interest.[140] "[R]ights in information extinguish when the information arrives at its destination."[141] Furthermore, according to Kerr, there is no better alternative.[142]

Despite Professor Kerr's belief that the third party doctrine's neutrality and clarity justify its continued use, neither of these virtues effectively tackles the challenge brought by the reach of ever-developing technology. For instance, while the third party doctrine is perhaps technologically neutral,[143] it is not neutral in application. This is because the third party doctrine focuses on the privacy interests of the guilty,[144] reasoning that the guilty person is aware of the possibility for a third party to disclose information.[145] However, an innocent person simply may not have the same awareness.[146] Thus, the third party doctrine appears to focus on the guilty at the expense of the innocent; and this is hardly neutral.

Yet, Professor Kerr holds fast to the third party doctrine, arguing that an ever-evolving search protection that applies to emerging technology would prove impossible to maintain.[147] While Professor Kerr admits the third party doctrine, as it is currently applied, is not

139. *Id.* at 566.
140. *Id.* at 582.
141. *Id.* at 581.
142. *Id.* at 586.
143. *See* Kerr, *The Case for the Third-Party Doctrine*, *supra* note 133, at 580.
144. *See* Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 MICH. L. REV. 1229, 1252 (1983).
145. *See id.* at 1253.
146. *See id.* at 1253–55. Professor Loewy hypothesizes about the gossiping innocent. In his hypothetical, he compares the impact of a statement made to a police officer directly by an individual versus someone who made a statement to a friend about a police officer. Professor Loewy contends that an innocent party still possesses a privacy interest, even if they have nothing to hide. Because of this belief, the third party doctrine is not neutral but rather unduly harms innocents. *See id.*
147. *See* Kerr, *The Case for the Third-Party Doctrine*, *supra* note 133, at 586. Professor Kerr examines a totality of the circumstances-style test, concluding the third party doctrine would provide better clarity for police. *See id. But see* Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975 (2007) (finding that a factors test is a better system).

Washington University Open Scholarship

perfect,[148] he would more readily see the third party doctrine continue than see the Court throw the doctrine in limbo. Instead, he argues, adjustments to privacy law based on technological advances are best suited for legislative repair.[149]

While Professor Kerr provides a powerful argument for upholding the third party doctrine, Professor Epstein[150] has chartered a middle ground approach between critics and supporters of the third party doctrine.[151] Professor Epstein zeroes in on the two tenets of third party doctrine: assumption of the risk and reasonable expectations.[152] He argues that the Court could better protect privacy interests and keep the third party doctrine intact if it focused more on assumption of the risk.[153] According to Epstein, it is important to remember that "assumption of the risk is forced on individuals by positive law. It is not consensually assumed."[154] Thus, simply using a technology does not generate acquiescence of one's societal right; rather, protection may be limited by the actions of the holder.

This squares with Professor Epstein's conception of reasonable expectations under the third party doctrine. Professor Epstein likens the third party doctrine to an experience at a crowded restaurant.[155] Sure, people can hear what is said at other tables, but it is considered impolite to lean over to listen better. Similarly, just because one person talks loudly doesn't make it reasonable to lean in. Simply put, reasonable expectations are not an all or nothing proposition.[156]

148. In a perfect world, Professor Kerr would prefer the third party doctrine to rest fully in the first prong of the *Katz* test, where disclosure of information would turn on whether the party chose to disclose it, as opposed to whether society believes the information to have privacy rights. *See* Kerr, *The Case for the Third-Party Doctrine*, *supra* note 133, at 588–90.

149. *See id.* at 596–97. *But see* Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747 (2005) (arguing Professor Kerr is incorrect in asserting legislatures can solve privacy law issues).

150. Professor Epstein is the James Parker Hall Distinguished Service Professor of Law and Senior Lecturer at the University of Chicago Law School.

151. *See* Richard Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 BERKELEY TECH. L.J. 1199 (2009).

152. *See id.* at 1202.

153. *See id.* at 1204. Professor Epstein uses the example of walking outside. One sees cars every day when walking, and one knows that they are dangerous, but one does not assume the risk of the danger. *See id.*

154. *Id.* at 1206.

155. *See id.* at 1215.

156. *See id.*

Professor Erin Murphy has pushed back on both Kerr's warm embrace and Epstein's muted acceptance of the third party doctrine.[157] Professor Murphy counters Professor Kerr's technology neutrality claim, arguing that most crime doesn't have technological alternatives.[158] As a result, the idea that the third party doctrine is preventing criminals from using third parties to commit crimes is weak at best.[159]

Instead of the all-or-nothing third party doctrine, Professor Murphy would call for a sliding-scale approach that embodies "important communal and constitutional values."[160] Once the sliding scale is established, enforcement would be akin to current enforcement of the third party doctrine. And as technology developed, different values would be slotted into the sliding scale. In contrast to Kerr's assertions, Murphy argues that it doesn't matter if it is unclear for government enforcement, because the government still has the ability to seek a warrant.[161]

But how could the Supreme Court apply a flexible approach such as the one proffered by Professor Murphy? Professor Stephen Henderson suggests that the Supreme Court should look to where the Fourth Amendment is applied on a daily basis—state courts.[162] Professor Henderson focuses on nine factors that states routinely consider when information is disclosed to a third party.[163] The factors

157. *See* Erin Murphy, *The Case against the Case for Third-Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239 (2009).

158. *See id.* at 1243. In fact, according to Professor Murphy, even if the defendant had gone the technological route, he still would not have been protected. However, if he simply mailed the stalking letter, then he could have been safe. *Id.* at 1244–45.

159. *See id.* at 1245.

160. *See id.* at 1252. Factors in her sliding scale include "the role of trust, the notion of agency, the need and desirability of third party confidences, and some idea of autonomy and consent." *Id.* These factors could be used to determine the level of protection. *See id.*

161. *See id.* at 1253. The dichotomy between Professor Kerr and Professor Murphy lies in the relative ease with which an officer may obtain a warrant under the warrant clause.

162. *See* Henderson, *supra* note 147. Professor Henderson explains that state courts have used a factors test for determining what third party information should be protected and what information should not be afforded protection. *See id.* at 977. For instance, eleven states have rejected the third party doctrine, and eleven more are inclined not to follow it. *See id.* at 976.

163. *See id.* at 989. These factors include (1) the purpose of the disclosure, (2) the personal nature of the information, (3) the amount of information, (4) the expectations of the disclosing party, (5) the understanding of the third party, (6) positive law guarantees of confidentiality, (7) government need, (8) personal recollections, and (9) changing social norms and

Washington University Open Scholarship

eviscerate the neat application of the third party doctrine but allow for flexibility based on the situation. The factor-based review leads courts to focus on the rationale behind the *Katz* test, which includes the expectations of society and the person performing the disclosure.[164] Ultimately, because society relies on "transactional information," our society "require[s] reformulating that [third party] doctrine."[165]

Rather than applying a factor-based test, Matthew D. Lawless proposes the third party doctrine need only shift its focus from the capacity of the information disclosed to the right to view the information.[166] Essentially, the Court should "place an increased emphasis on the agreements and relationships between the parties."[167] Thus, the Court would turn its focus from whether the transaction occurred to whether the parties agreed to and were aware of the disclosure. Similarly, Andrew J. DeFilippis posits the Court should apply a threshold test to disclosure.[168] This threshold test would focus again on the consent of the parties in deciding whether to limit disclosure of the information.[169] DeFilippis takes the suggestion

technologies. *See id.* In addition, Professor Henderson discusses what he believes to be irrelevant considerations that state courts sometimes focus on, such as (1) the form of the information, (2) the "good citizens" motivation of a third party, (3) the government's method of acquisition, and (4) expectations created by police conduct. *See id.*

164. *See id.* at 988.

165. Stephen E. Henderson, *Expectations of Privacy in Social Media*, 31 MISS. C. L. REV. 227, 247 (2012). In his article, Professor Henderson holds that the third party doctrine should "apply only to information revealed [to a third party] for that third party's use." Stephen E. Henderson, *Learning from all Fifty States: How to Apply the Fourth Amendment and its States Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373, 378 (2006).

166. *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, 43 (2007).

167. *See id.* Lawless labels his test the "Operational Realities" test. *Id.*

168. *See* Andrew J. DeFilippis, *Securing Informationships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence*, 115 YALE L.J. 1086, 1109–10 (2006). Of note, DeFilippis recognizes that a fundamental flaw in the third party doctrine is that people now share what they consider to be private with others. *See id.* at 1091.

169. *See id* at 1109–10. DeFilippis' threshold test is (1) whether the third party would limit disclosure of the information, and (2) that the limited set of recipients would not include the government agent or agency. *Id.*

further and advocates for the inclusion of a second element: the government's investigatory need for the information.[170]

Professor Christopher Slobogin offers a fundamentally different approach to rethinking the third party doctrine.[171] Professor Slobogin recognizes that "privacy may not be measurable in the predominantly normative terms" that courts use to apply Fourth Amendment search protection under *Katz*.[172] Professor Slobogin points to his empirical study, wherein he asks people to note what degree of government intrusion violates their privacy rights.[173] Professor Slobogin demonstrates that "transferring information to third parties or allowing third parties to accumulate it does not, by itself, lessen the intrusiveness of government efforts to obtain it."[174] In particular, the degree to which people feel they have a privacy interest depends on the third party itself.[175]

As a result of his findings, Professor Slobogin argues that privacy and the third party doctrine should apply a tiered approach to third party information.[176] The authority the police need in order to access particular information should depend on which tier the information disclosed to the third party is located.[177] Professor Slobogin believes this approach allows for the Fourth Amendment to protect the

170. *See id.* If the first two questions are answered in the affirmative, then the government would need to get a warrant, unless it could prove that (1) the government agent or agency had a need to know the information; (2) obtaining a warrant would have unreasonably hindered a government function or investigation; and (3) the methods used to obtain the information were reasonable. *See id.*

171. CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT (2007).

172. *Id.* at 182.

173. *See id.* at 184. Unsurprisingly, people find a bedroom search to be the most intrusive and a roadblock the least intrusive. *Id.* Professor Slobogin also discusses the social network perspective to privacy, concluding that information a person believes to remain in their social network should have an assumption that it will remain private. *See id.* at 183 (discussing Lior Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919 (2005)).

174. *Id.* at 183–84.

175. *See id.* For instance, 80.3 percent of people find a privacy interest in bank records, while only 34.1 percent find a privacy interest in store patron lists. *Id.*

176. *See id.* at 185.

177. *See id.* at 186. The four tiers, from least protected to most protected, are: (1) organizational records, (2) public records, (3) quasi-private individual records, and (4) private individual records. *See id.*

Washington University Open Scholarship

"personal nature" of third party information while still allowing the government to effectively monitor.[178]

Each of the proposals, while offering different tests, focuses on the role a third party plays in the gathering of information.[179] Thus, any reimaging of the third party doctrine by the Court must examine how the third party interacts with the individual. The primary question, whether information is secret, is immaterial to whether information is private. Once this conclusion is accepted, privacy rights can adapt to emerging technology. The Court can then fashion a test to adapt to emerging technology, using a third party doctrine that adequately weighs both security and privacy concerns.

V. CONCLUSION

As Professor Katherine J. Strandburg has stated, "the Fourth Amendment's protections must adapt to the broadened context in which citizens live their private lives."[180] Echoing this sentiment, changes in private lives have led public actors to push more and more cases into the lower courts to examine the third party doctrine.[181] Two such cases provide clues about how courts might respond to increasing questions about the application of the third party doctrine to emerging technology.

---

178. *See id.* at 203. Professor Orin Kerr criticizes Professor Slobogin's approach. Orin S. Kerr, *Do We Need a New Fourth Amendment?*, 107 MICH. L. REV. 951 (2009). Professor Kerr's article finds that Professor Slobogin's method does not adequately balance privacy and security interests, and that the tiered approach is too complicated for courts to apply. *See id.* at 952.

179. The aforementioned approaches range from a sliding-scale that emphasizes a party's trust in the third party (Murphy), to a fact-heavy analysis (Henderson), to a focus on the role of consent in the agreements made between the parties (Lawless and DeFilippis), to creating new tiers based on the type of third party information (Slobogin). *See supra* Part IV.

180. *See* Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 680 (2011). With the increase in cloud computing, it is becoming more and more difficult to distinguish at what point a third party server becomes a home server. *Id.* at 657.

181. Courts have even started to waver on cell phone records, which, as discussed *supra* note 108, are not considered to be sufficiently private. *See* In re U.S. ex rel. Order Pursuant to 18 U.S.C. § 2703(d), Nos. C-12-670M, C-12-671M, C-12-672M, C-12-673M, 2012 WL 4717778, at *3 (Sept. 26, 2012). *But see* United States v. Graham, 846 F. Supp. 2d 384 (2012).

In *United States v. Warshak*,[182] the Sixth Circuit held that the defendant enjoyed a reasonable expectation of privacy in e-mails he sent and received, even though they were sent and stored using a commercial ISP.[183] The *Warshak* court reasoned that the ISP was an "intermediary" and not the intended recipient of the e-mail message.[184] Thus, the court held "a subscriber enjoys a reasonable expectation of privacy in the contents of emails that are stored with, or sent or received through, a commercial ISP."[185] The *Warshak* court felt that opening an e-mail was akin to looking at more than the mere numbers dialed, the result of which was a privacy violation.[186]

The reasoning used in *Warshak* exemplifies one way a new third party doctrine analysis can be framed, focusing on A and B, as opposed to who gets the information from A to B. Other courts are now attempting to apply the *Warshak* court's view on emerging technology and the Fourth Amendment.[187]

The Supreme Court also recently reviewed a case directly concerning the third party doctrine and technology.[188] In *City of Ontario v. Quon*, the Court considered whether text messages were afforded Fourth Amendment protection when they were sent and

182. 631 F.3d 266 (6th Cir. 2010). The government suspected the defendants of money laundering, among other crimes. *See id.* at 281. To acquire evidence, the government seized approximately 27,000 private e-mails through the defendants' ISP, without a warrant. *Id.*

183. *See id.* at 288.

184. *Id.* at 287.

185. *Id.* at 288.

186. *See id.* The *Warshak* court went further, stating that if the SCA allows the government to obtain emails warrantlessly, then "the SCA is unconstitutional." *Id.* Ironically, the defendant still lost, because the court found the agents acted in good faith. *Id.* at 292.

187. *See* United States v. Heckenkamp, 482 F.3d 1142, 1146 (9th Cir. 2007) (holding that a person does not automatically lose her expectation of privacy regarding her e-mails when she logs onto a public network); *see also* R.S. v. Minnewaska, No. 12-588, 2012 WL 3870868 (D. Minn. 2012) (holding that a student had a reasonable expectation of privacy with private information on a social network account); In the Matter of Applications for Search Warrants for Information Associated with Target Email Address, No. 12-MJ-8119-DJW, 2012 WL 4383917 (D. Kan. 2012) (upholding an individual's Fourth Amendment right to e-mails stored on an ISP and denying a search warrant that asserted otherwise); State v. Clampitt, 364 S.W. 3d 605 (Mo. Ct. App. 2012) (finding the defendant had an expectation of privacy for sent text messages even though they were confiscated on another phone). *But see* State v. Hinton, 280 P.3d 476 (Wash. Ct. App. 2012) (holding the defendant does not have an expectation of privacy in sent text messages).

188. City of Ontario v. Quon, 130 S. Ct. 2619 (2010).

Washington University Open Scholarship

received on a public employee's pager.[189] In the opinion, every Justice except Justice Scalia joined the discussion on the reasonable expectation of privacy, concluding, "Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior."[190] While the Court did not come to a conclusion on the third party doctrine, it left open the door to rule on the issue at a later time.[191]

Perhaps that time is now. Congress and the lower courts have struggled with developing a clear, concise test to conclude what is a reasonable search that utilizes third party technology. It is up to the Court of last resort to act and apply either the framework adopted by the *Warshak* court,[192] Professor Murphy's sliding scale,[193] Professor Henderson's factors test,[194] Lawless and DeFilippis' threshold inquiries,[195] Slobogin's tiered approach,[196] or another approach yet to be articulated. The Court must fashion a test that eliminates the third party doctrine's all-or-nothing approach and replace it with a standard that focuses on how a third party acquires an individual's information. At the very least, if a third party is a mere carrier of information from A to B, the law should ensure that A has not given up his privacy interest in that information.

While Justice Sotomayor's concurrence in *Jones* is not mandatory authority, the fact that a Supreme Court Justice articulated the need for a reimagining of the third party doctrine is an encouraging step towards positive change. Just as Justice Harlan's concurrence in *Katz* proved influential, eventually becoming law, so too may Justice Sotomayor's concurrence yield ripe fruit for pro-privacy interests.

---

189. The Court ruled the search was reasonable because it was a government pager, completely side-stepping the Fourth Amendment issue. *Id.* at 2631.

190. *Id.* at 2629.

191. The Ninth Circuit determined the defendant did have a reasonable expectation of privacy in the text messages, due to the informal policy of the employer. This part of the Ninth Circuit opinion was not overruled by the Supreme Court's decision, leaving it open for future courts. *See* Quon v. Arch Wireless Operating Co., Inc., 529 F.3d 892, 902 (9th Cir. 2008).

192. *See supra* note 186 and accompanying text.

193. *See supra* notes 157–60 and accompanying text.

194. *See supra* notes 162–63 and accompanying text.

195. *See supra* note 168 and accompanying text.

196. *See supra* notes 171–75 and accompanying text.