RILEY V. CALIFORNIA AND THE BEGINNING OF THE END FOR THE THIRD-PARTY SEARCH DOCTRINE

David A. Harris[*]

TABLE OF CONTENTS

---

* Distinguished Faculty Scholar and Professor of Law, University of Pittsburgh School of Law. The author wishes to thank the student editors of the *University Of Pennsylvania Journal of Constitutional Law* for the opportunity to present this paper at their Symposium on January 23, 2015. The Symposium was well conceived and carefully organized. It was a great pleasure to attend and participate.

INTRODUCTION

The U.S. Supreme Court's decision in *Riley v. California*[1] made national headlines[2] when it was announced in late June of 2014. Chief Justice John Roberts' opinion, for an all-but-unanimous[3] Court, declared that a search of the data available on a smart phone[4] required a warrant issued by a judge.[5] According to the opinion, these devices functioned as far more than phones. While capable of a making a traditional telephone call, they also operated as cameras, electronic calendars, video recorders, GPS devices, rolodexes, audio recorders, and diaries; in every way, they performed as extremely capable pocket-sized computers, storing millions of pages of text, thousands of photographs and video recordings, and thousands of web searches going back years.[6] In addition, they may contain data such as GPS coordinates, requested directions, appointment calendars, and other information that would allow the state to construct a highly detailed depiction of the activities of the user for a considerable time in the past, as well as a mosaic of the user's personal interests, relationships, medical conditions, and the like.[7] The Court did not view the phone as a mere physical object; rather, it said, the phone performs as a digital tool as multifunctional as a Swiss Army knife, and as a massive storage unit, for all of the user's present and past digital life. Given the deep privacy concerns such technology raised, law enforcement would henceforth need a warrant to burrow into this rich trove of material.[8] Chief Justice Roberts conceded that smart phones had, indeed, "become important tools" for "criminal enterprises," and searching the devices would no doubt provide incriminating evidence. The Court's decision would therefore have a negative impact "on the ability of law enforcement to combat crime."[9] But this did not, and should not, change the outcome. "Privacy," the Chief Justice said, "comes at a cost"[10]—a sentiment that no doubt surprised many observers of the Supreme Court's cases involving police power over the last several decades.

---

1 Riley v. California, 134 S. Ct. 2473 (2014) (decided with United States v. Wurie, No. 13-212 (decided June 25, 2014)).

2 Jess Bravin, *Supreme Court: Police Need Warrants to Search Cellphone Data*, WALL ST. J. (June 25, 2014), http://www.wsj.com/articles/high-court-police-usually-need-warrants-for-cellphone-data-1403706571; Adam Liptak, *Major Ruling Shields Privacy of Cellphones*, N.Y.

Deep in the opinion, exploring the considerable privacy interests at stake in a police search of a smart phone, the Court admitted that these concerns went further than just the data stored on the device.

> [T]he data a user views on many modern cell phones may not in fact be stored on the device itself . . . . [The device may be] used to access data located elsewhere, at the tap of a screen. That is what cell phones, with increasing frequency, are designed to do by taking advantage of "cloud computing."[11]

Cloud computing, the Court explained, allows any device connected to the Internet to "display data stored on remote servers rather than on the device itself[,]" without knowing the difference.[12] The scale of the privacy interests in such a massive amount of data available remotely makes it inconceivable, the Court said, that any standard exception to the warrant requirement (such as the search incident to arrest doctrine) could justify a search of all of the data accessible through the device.

The Court's discussion of how cloud computing makes the unlimited capacity of the digital world accessible from any smart phone surely makes sense. But this exploration of cloud computing does something more than just illustrate the vast scope of private data searchable in the digital realm: it brings the Court face to face with the shortcomings of the third-party search doctrine.

The third-party search doctrine arose in two cases from the 1970s: *United States v. Miller*[13] and *Smith v. Maryland*.[14] In both cases, the government sought access to the private information of a defendant: in *Miller*, it took banking records by using a subpoena;[15] in *Smith*, it obtained the numbers dialed from defendant's telephone by using a de-

---

TIMES, June 25, 2014, http://www.nytimes.com/2014/06/26/us/supreme-court-cellphones-search-privacy.html?_r=0.

3 *Riley*, 134 S. Ct. at 2495 (Alito, J., concurring in part and in the judgment).

4 Chief Justice Roberts defined a smart phone as "a cell phone with a broad range of other functions based on advanced computing capability, large storage capacity, and Internet connectivity." *Id.* at 2480.

5 *Id.* at 2495.

6 *Id.* at 2479, 2487–92.

7 *Id.* at 2487–92.

8 *Id.* at 2495.

9 *Id.* at 2493.

10 *Id.*

11 *Id.* at 2491.

12 *Id.*

13 425 U.S. 435 (1976).

14 442 U.S. 735 (1979).

15 *Miller*, 425 U.S. at 438.

vice called a pen register.[16] In neither case did the government obtain a search warrant before getting the information. The Court used *Miller* and *Smith* to say that no one could have a reasonable expectation of privacy in information willingly conveyed to a third party. When a person conveyed information to a third party—a bank's customer to a bank, in order to use a checking account, or a telephone user to the telephone company, in the form of numbers dialed for the purpose of making a connection to another phone—the person "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[17] This remains true "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."[18]

This line of reasoning made little sense when it appeared in the 1970s. To participate in the basics of modern life, like banking and using a telephone, a person essentially forfeited any Fourth Amendment expectation of privacy in any information that the receiving institution might obtain as part of any transaction. One could not maintain privacy rights in relation to the government except by giving up any interaction with any entity, public or private, that used or processed one's data. But in today's world, the very idea of the third-party doctrine seems downright absurd. All aspects of participation in the digital worlds of commerce, entertainment, and everything else require—indeed, they depend upon—conveying data to an intermediary third-party organization. Yet the third-party doctrine still stands and its implications become breathtaking in scope. Digital privacy simply disappears.

But with *Riley*, perhaps a crack has appeared in this façade—one that will inevitably widen, and at last get rid of the outdated and pernicious third-party doctrine. This is because the whole idea behind the doctrine—that giving any information to anyone else means that law enforcement can search or seize it—must yield to the Court's (correct) understanding of the use of data from the cloud, as articulated in *Riley*. If the use and availability of cloud-based data makes for a vastly expanded privacy interest, and therefore adds to the justification of the need for a search warrant before searching the data exposed by a user's smart phone, the third-party doctrine has outlived whatever usefulness it once might have had. Cloud-based data is, by

16 *Smith*, 442 U.S. at 737.

17 *Id.* at 744 (quoting *Miller*, 425 U.S. at 443).

18 *Miller*, 425 U.S. at 443.

its very nature, conveyed to and possessed by third parties. That is both its function and its *rasion d'être*. If we now live in the world of the cloud, and that world enjoys Fourth Amendment protection, as *Riley* says, the Court must now recognize the third-party doctrine for the relic it has become and cast it aside.

This is not to say that the Supreme Court seems ready to dump the third-party doctrine. It has said nothing of the sort, and it actually cited *Smith v. Maryland* in the *Riley* opinion.[19] But the seeds of the argument appear in *Riley*, and they seem likely to sprout and grow.

I. *RILEY V. CALIFORNIA*: WHETHER TO RECOGNIZE AN EXCEPTION TO THE WARRANT REQUIREMENT FOR SMART PHONE SEARCHES, AND THE IMPORTANCE OF THE CLOUD

A. A Search Incident to a Valid Arrest: Balancing Government Need Against the Intrusion on Individual Privacy

In *Riley*, the United States Supreme Court confronted a situation that police encounter more and more often. In both cases, police made arrests, and performed standard searches of the suspects incident to that arrest. Officers seized smart phones during these searches, and then searched the data on the phones.[20] These searches produced incriminating evidence, which both defendants moved to suppress; courts denied these motions, and both defendants suffered convictions.[21]

The government attempted to justify the searches of the data in the smart phones under the "well accepted" exception to the warrant requirement for searches incident to a lawful arrest.[22] In *Riley*, the Court explained that this exception rests on three related precedents.[23] In *Chimel v. California*,[24] involving an arrest inside a home, the Supreme Court decided that police may search the area of the home that is within the arrestee's immediate control, but no other areas.[25] In *United States v. Robinson*,[26] the Court said that the risks of any arrestee obtaining a weapon and the destruction of evidence inhere in all arrests, justifying searches incident to arrest that allow po-

19 Riley v. California, 134 S. Ct. 2473, 2492 (2014) (citing *Smith*, 442 U.S. 735).
20 *Id.* at 2477–79.
21 *Id.* at 2481.
22 *Id.* at 2482.
23 *Id.* at 2483.
24 395 U.S. 752 (1969).
25 *Id.* at 763, 768.
26 414 U.S. 218 (1973).

lice to check the arrestee's pockets and items within them even when there is no specific threat to officers or concern about the loss of evidence.[27] And in *Arizona v. Gant*,[28] the Court filled out the picture in the context of vehicles: it permitted the search of a car when the arrestee remains unsecured and within reaching distance of the passenger compartment, or whenever an officer might reasonably believe that the vehicle might contain evidence of a crime.[29]

The Court's opinion in *Riley* rejected the idea that the police could search the contents of a smart phone found in the pocket of an arrestee, just as police who had searched a cigarette packet found in a pocket could in *Robinson*. The Court balanced the extent to which the police need to search in order to promote legitimate government interests against "the degree to which [the search] intrudes upon an individual's privacy."[30] The Court found that neither of the risks articulated in *Chimel*—the risk of access to a weapon or the risk of the destruction of evidence—could justify the search of the data in the phone without a warrant.[31] The opinion found little reason to think that either the phone itself, or the data within, could constitute a weapon; the police could address any contingent danger—e.g., that the data might indicate that the suspect's confederates might approach—with case-specific exceptions, such as the exception for exigent circumstances.[32] Similarly, the Court dismissed any danger to the evidence, such as the possibility of "remote wiping" of the data or of data encryption.[33] Law enforcement could meet these dangers, should they exist, with technologies of its own or other measures.[34]

On the other side of the balance, the capabilities of smart phones made searches of the data on these devices uniquely intrusive, because searchers would have access to an unprecedented amount of information. The government's argument had ignored this technological reality, saying that the search of the data on a cell phone did not differ materially from searches of physical items such as wallets or purses, but the Court would have none of it. "That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. . . . Modern cell phones, as a category, implicate privacy con-

27 *Id.* at 235, 236.
28 556 U.S. 332 (2009).
29 *Id.* at 353.
30 *Riley*, 134 S. Ct. at 2484 (internal quotation marks omitted).
31 *Id.* at 2485.
32 *Id.* at 2485–86.
33 *Id.* at 2486.
34 *Id.* at 2486–88.

cerns far beyond" the search of any objects found in an arrestee's pockets or on his or her person.[35]

First, the word "phone" does not accurately describe these devices. Rather, the Court said, think of them as "minicomputers" capable of making telephone calls, but equally capable as "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers," making them qualitatively different than other objects a person might carry.[36] Second, this wide-ranging capability comes with "immense storage capacity," enabling the typical smart phone to store and carry an amount of information that people simply could not, were the data in physical form.[37] Third, as a consequence of the portable storage of such an immense amount of data in so many forms (pictures, messages, photos, and videos, etc.), the data "reveal much more in combination than any isolated record," enabling the reconstruction of "[t]he sum of an individual's private life," both present and past (back to the dates on which the first data was stored).[38] Fourth, the use of smart phones has become so pervasive that few Americans do not have these devices on their persons at any given time.[39] Fifth, smart phones collect and store qualitatively different data than any file cabinet could: Internet browsing histories, GPS location data timed to the minute, personal messages to intimates, and the user's substantive interests (the Court mentions political affiliation, addictions, pregnancy or other health issues, religion, and personal finance).[40] In sum, a search of cell phone data would expose virtually every aspect of a user's life; indeed, it would "expose to the government far *more* than the most exhaustive search of a house."[41]

Comparing the government's minimal-to-nonexistent interest in searching for weapons or protecting evidence with the enormous intrusion on the arrestee's privacy involved in a warrantless search of the data on a cell phone, the Court declared that a search of a cell phone's data required a warrant.[42] But the Court added one other

35 *Id.* at 2488.
36 *Id.* at 2489.
37 *Id.*
38 *Id.*; *see also* United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) (arguing that such massive data collection about one's location "may 'alter the relationship between citizen and government in a way that is inimical to a democratic society'").
39 *Riley*, 134 S. Ct. at 2490.
40 *Id.* at 2490.
41 *Id.* at 2491 (emphasis in original).
42 *Id.* at 2493.

factor into the mix: remote data storage and use, also called cloud computing.

B. Cloud Computing

Without the user knowing it, smartphones use "data located elsewhere."[43] This occurs not as an anomaly, but as standard operating procedure; manufacturers equip smartphones to engage in cloud computing. According to the Court, "[c]loud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself. Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference."[44]

The Court noted that the government had conceded that the search incident to a lawful arrest exception to the warrant requirement would not cover data stored in the cloud.[45] Indeed, the government could not have said anything else without looking foolish; to argue otherwise would be "like finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house."[46] In fact, said the Justices, police officers searching the data on the phone would not usually know whether or not what they found came from inside the phone itself, or from the cloud.[47]

The Court's definition of cloud computing, along with its explanation of cloud computing's importance in deciding whether to require a warrant, makes eminent sense. First, we can tell that the Court correctly understands how accessing data remotely actually works. This allows future courts to make correct decisions with as-yet-unknown technology, because understanding what the Court in *Riley* values requires an accurate factual picture. If the Court misses the mark in its understanding of technological facts or chooses to ignore what actually makes a new technology important, its rationale will necessarily be unclear to judges looking back on the opinion. The Court has not always succeeded in this respect in other recent opinions. For example, in *United States v. Jones*,[48] decided just two years earlier, the Court had before it the question of whether placing a GPS tracking device on the undercarriage of a vehicle for twenty-

43 *Id.* at 2491.
44 *Id.*
45 *Id.*
46 *Id.*
47 *Id.*
48 132 S. Ct. 945, 948 (2012).

eight days, generating a complete locational record for a full month, constituted a search for Fourth Amendment purposes. Justice Antonin Scalia's opinion for the Court did not center on the fact that tracking the vehicle's location around the clock for twenty-eight days intruded on individual privacy, enabling the police to build a detailed picture of the driver's movements. (This would have paralleled the Court's statement in *Riley* that using a large amount of data allows the authorities to reconstruct "the sum of an individual's private life."[49]) Rather, Justice Scalia decided that the key element of the Fourth Amendment intrusion was the placing of an object—the GPS device—on the vehicle, because this constituted a trespass on the defendant's property (the vehicle).[50] And in *Maryland v. King*,[51] in which the Court upheld a state law that allowed police to take DNA samples from arrested people[52] without waiting for a conviction, Justice Samuel Alito's majority opinion rested, in part, on the fact that police needed DNA testing at the point of arrest in order to determine the arrestee's identity.[53] The majority came to this conclusion despite the fact that determining identity from a DNA sample takes weeks or months using current technology, and would therefore not help police in trying to identify a suspect for the purposes of arrest.[54]

Second, and more important for present purposes, the Court's opinion in *Riley* described cloud computing or remote data storage accurately enough that we can understand how it works and therefore how it fits into our lives, and therefore how it fits into our expectations of privacy. The data, the Court said, does not reside in the phone itself; it sits on another, much larger computer, somewhere else, which does not belong to the user. And it is this quality that emerges as a direct challenge to the third-party doctrine.

---

49 *Riley*, 134 S. Ct. at 2489.

50 *Jones*, 132 S. Ct. at 952. While the decision looks like a failure to understand what GPS tracking does and how it works, it may be that Justice Scalia simply preferred to ignore this in favor of a rationale which he felt had greater appeal as a matter of doctrine.

51 133 S. Ct. 1958, 1965–71 (2013).

52 *Id.* at 1965–66.

53 *Id.* at 1971.

54 *See, e.g.*, New York City Office of the Chief Medical Examiner, *How to Submit a Case*, NYC.GOV (Jan. 16, 2016), www.nycgov.html/ocme/html/hss/how_to_submit_acase_shtml ("A report describing the result of testing will be issued with 120 days of evidence receipt . . . .").

II. THE THIRD PARTY DOCTRINE: AN IDEA WHOSE TIME NEVER CAME, AND WHOSE TIME IS CERTAINLY OVER

The third-party doctrine emerged in the 1970s in two cases that created greater power for police investigators. These decisions seemed to take everyday interactions and turn them into excuses for government overreaching. But if that was true when the Court handed down these opinions, it is much more true now.

A. The Cases: Miller *and* Smith

The third-party issue first arose in *United States v. Miller*,[55] in which the government sought banking records belonging to the defendant: checks, deposit slips, and the like. The government went after the records, not through a search or seizure with a warrant, as in the normal course of an investigation, but instead by issuing subpoenas to two banks that the defendant used.[56] The banks maintained these records under the Bank Secrecy Act of 1970,[57] but they turned the records over to the government anyway, and prosecutors then used those records to convict the defendant.[58] The defendant objected to the use of the records against him, arguing that the government had violated his reasonable expectations of privacy in those records by seizing them without a warrant.[59]

The Supreme Court sided with the government, saying that the defendant had no privacy rights in his own banking records.[60] Most people might regard their own personal financial records as private, especially with the Bank Secrecy Act in play. But that did not matter to the Justices. Rather, the Court based its decision on the fact that the defendant had conveyed his private information to his banks.[61] Any exposure of private information to a third party, the Court said, defeated any possible claim that the defendant could claim any privacy right in the information shared.[62] "[W]e perceive no legitimate 'expectation of privacy'" in the records or their contents, the Court said.[63]

---

55 425 U.S. 435, 436 (1976).
56 *Id.* at 437–38.
57 *Id.* at 440–41.
58 *Id.* at 437–38.
59 *Id.* at 442.
60 *Id.* at 444–45.
61 *Id.* at 442.
62 *Id.* at 442–43.
63 *Id.* at 442.

> The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. . . . [T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[64]

In short, said the Court, "no Fourth Amendment interests of the [defendant] are implicated here,"[65] notwithstanding that the information came to the bank with the understanding that it would remain confidential. Such an understanding might seem like the very essence of an "expectation of privacy," yet the Court says, in effect, that such an expectation could not be reasonable. By conveying his information to a third party—his bank—the defendant "takes the risk" that the bank will betray him to the government, simply because the bank *could* betray him.

This notion seems curious indeed. Information in the hands of one's bank differs greatly from information one might tell a friend or acquaintance, which the friend might repeat to others. Rather, it constitutes private information about one's finances—income earned, debts paid, amounts owed, the far-too-small nest egg because of poor savings habits. Most people would not share this kind of information widely, if at all. If one had told a very close friend about these matters, one would likely feel deeply uncomfortable if this friend had conversations with others—gossiping, if you will—about such private matters. To call personal finances "private matters" may seem to simply assume the correctness of the answer with which the Court disagrees. Nevertheless, the reaction of most people to finding out that a bank had shared personal financial information would be simple: get a new bank. In this situation, expecting privacy could *only* be reasonable.

Consider a brief thought experiment. Imagine two customers in the marketplace seeking banking services. One bank advertises in the traditional ways, calling itself friendly, oriented toward customer service, and dedicated to paying the best rates possible and charging the lowest fees. The second bank advertises the same features, in slightly different words. But it also adds that customers should not expect their financial information to remain confidential, especially vis-á-vis a government request, because everyone knows that, in any relationship, one party may betray the confidence of the other. It seems in-

64 *Id.* at 443 (citations omitted).

65 *Id.* at 444.

conceivable that anyone would choose the second bank over the first. While it is understandable that individuals might disclose the secrets of those who have confided in them, knowing that a bank would do so seems like a deal-breaker.

We have seen this very phenomenon recently in a different industry. Major information and telecommunications companies in the United States, such as Google, Verizon, Apple, and Facebook, faced major questions from non-U.S. customers in 2013 and 2014 when disclosures by former National Security Agency ("NSA") contractor Edward Snowden revealed that these firms had regularly cooperated with NSA requests for data on their customers' telecommunications activity.[66] If Americans did not mind that the NSA vacuumed up their private information, and this activity broke no laws or social norms in the United States, fine. But customers outside the United States did not want this happening to their information,[67] and these American companies correctly saw this as a threat to their overseas business.[68] Apple was among the first to react, announcing that henceforth, using a password on its newest iPhones would automatically encrypt the contents of the phone; the company would not have the key to the code, and therefore could not decrypt anything for the government.[69] The Director of the FBI publicly attacked Apple for this move,[70] and others in law enforcement told the media that the iPhone would now serve as the phone of choice for pedophiles and other criminals.[71] But the market had spoken, and Apple and other companies listened to their customer and held their ground.

The Supreme Court revisited the third-party doctrine again just three years later, in *Smith v. Maryland*.[72] After a female victim was robbed, she began to get distressing telephone calls from a man identifying himself as the robber.[73] When police obtained information

66 Charlie Savage et al., *U.S. Confirms That It Gathers Online Data Overseas*, N.Y. TIMES (June 6, 2013), http://www.nytimes.com/2013/06/07/us/nsa-verizon-calls.html.

67 Anton Troianovski & Danny Yadron, *German Government Ends Verizon Contract*, WALL ST. J. (June 26, 2014), http://www.wsj.com/articles/german-government-ends-verizon- contract-1403802226.

68 Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, N.Y. TIMES (Mar. 21, 2014), http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html.

69 Craig Timberg & Greg Miller, *FBI blasts Apple, Google For Locking Police Out of Phones*, WASH. POST (Sept. 25, 2014), http://www.washingtonpost.com/business/technology/2014 /09/ 25/68c 4e08e-4344-11e4-9a15-137aa0153527_story.html.

70 *Id.*

71 *Id.*

72 442 U.S. 735, 743–44 (1979).

73 *Id.* at 737.

that connected the defendant with the robbery and the calls, they had the telephone company install a device called a "pen register" at its central offices. The device would record the numbers dialed from the defendant's home phone number.[74] The police did not obtain a warrant or any other court order before installing the pen register.[75] The device revealed a call from the defendant's number to the home of the victim on one of the dates that the victim had received such a call, and based on that fact and other evidence, the police obtained a search warrant for the defendant's home.[76] The defendant moved to suppress all of the evidence recovered in this search, because the police obtained it by using the pen register without a warrant.[77] The trial court denied the motion to suppress, and all of the evidence from the search helped to convict the defendant.[78]

The Supreme Court began with the basics: whether or not the Fourth Amendment applies in any given situation, the Court said, "depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action."[79] The defendant's argument, the Court said, that he had a legitimate expectation of privacy in the numbers dialed from his home telephone was not correct. Citing *United States v. Miller*, the Court said that even if the defendant himself did expect the numbers he dialed would remain secret, such an expectation was not reasonable because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[80] Like the bank depositor in *Miller* who chose to give his private financial information to his bank, the defendant "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to [the telephone company's] equipment."[81] By doing this, the Court concluded that the defendant "assumed the risk that the company would reveal to police the numbers he dialed," equating the entirely electronic and mechanical switching equipment the telephone company was using to the human operators who used to connect phone calls for people in the past.[82] And humans, of course, could spill secrets.

---

74 *Id.*
75 *Id.*
76 *Id.*
77 *Id.*
78 *Id.* at 737–38.
79 *Id.* at 740.
80 *Id.* at 743–44.
81 *Id.* at 744.
82 *Id.*

B. The Origin of the Idea that a Bank Customer or Telephone Dialer "Assumes the Risk"

Reading the opinions in both *Miller* and *Smith*, one striking feature stands out: their reliance on the idea that a person who conveys information to a third party "assumes the risk" that the third party may disclose that information to another. The genesis of that idea illuminates how poorly the third-party doctrine itself fits within our constitutional framework.

The idea that one "assumes the risk" of a given activity or action comes from torts: the part of Anglo-American law that governs civil liability for noncriminal injuries incurred when one individual or organization harms another. Accurately used, the phrase "assumes the risk"—usually, assumption of the risk—referred to a defense to a tort claim.[83] A defendant in a tort case could argue, under proper facts, that a plaintiff's claim should not succeed, because the plaintiff knew of the dangerous condition at the heart of the case, and chose to expose himself to it anyway. [84] By doing so, the plaintiff assumed the risk inherent in the activity, and cannot now complain that he or she experienced injury because of the defendant.[85] For example, imagine *A* asks *B* if *A* can bring his square dancing club to the hayloft in *B*'s barn for a hoe-down on Saturday night. *B* says: "Sure, but you better think about it first—the floor is rotted through in a bunch of places." *A* goes up to the loft to have a look, sees the weak floorboards, and while striding across the loft anyway, falls through the wood in the floor, injuring his spine. *A* sues *B* for damages, but *B* will have a defense: *A* knew of the risk (he saw the loft floor had been weakened by rot), but went ahead with his inspection of the loft anyway, thereby knowingly and voluntarily assuming the risk of walking across the floor and suffering an injury.

The assumption of the risk doctrine makes sense in torts; one should not have to compensate another for damages when the other person knowingly exposed himself to danger. But the doctrine does not seem an intuitively obvious fit in the realm of constitutional criminal procedure. And its first appearance in modern criminal procedure law illustrates this. In *Lopez v. United States*,[86] a case decided by the U.S. Supreme Court in 1963, the defendant made incriminating

---

83 *See* WILLIAM L. PROSSER ET AL., TORT: CASES AND MATERIALS 590 (8th ed. 1988) ("In most states the defense of assumption of risk [applies] to all negligence cases.").

84 *Id.* at 590–91.

85 *Id.*

86 373 U.S. 427, 427 (1963).

statements while attempting to bribe an Internal Revenue Service ("IRS") agent who was carrying a hidden recording device.[87] The agent had not obtained a warrant before recording the conversation.[88] The Supreme Court's majority opinion refused to recognize any infringement of the Fourth Amendment rights of the defendant by the government, saying the defendant simply took an unwise risk.[89] In dissent, Justice William Brennan argued that the Court had made a mistake: the majority assumed that the Fourth Amendment only protected information held in secrecy, and therefore the only way to have Fourth Amendment protection for one's private thoughts would be to keep them private—from everyone, all the time.[90] In the course of that argument, Justice Brennan imported the assumption of the risk doctrine into Fourth Amendment jurisprudence.

> [The defendant] assumed the risk that his acquaintance would divulge their conversation . . . . The risk inheres in all communications which are not in the sight of the law privileged. It is not an undue risk to ask persons to assume, for it does no more than compel them to use discretion in choosing their auditors, to make damaging disclosures only to persons whose character and motives may be trusted.[91]

Justice Brennan went on to say that the risk in cases like *Lopez* was not a risk of casual gossip that one might expect in the course of human relations. Rather, it was the risk that a third party, like a government agent listening in on a private conversation, would later testify in court about the private conversation.[92] This, Justice Brennan said, could not be justified under the idea that our acquaintances sometimes betray us to others. It is, he said, a risk "of a different order."[93]

In two subsequent cases, a majority of the Court took Justice Brennan's "assumption of the risk" language from his dissent in *Lopez*, and applied it to justify decisions that solidified the rule that conversations with government informants enjoyed no Fourth Amendment protection, even when the informant was a trusted friend of the defendant.[94] But the portion of the Brennan dissent that filled out the full context—that while people must live with the

87 *Id.* at 430–31.
88 *Id.* at 430.
89 *Id.* at 439–40.
90 *Id.* at 449–50 (Brennan, J., dissenting).
91 *Id.* at 450. While assumption of risk comes from torts, it is not clear that Justice Brennan meant to impart a tort concept. Rather, he seems to be reacting to the majority's use of the concept of risk. *See id.* at 439.
92 *Id.* at 450.
93 *Id.*
94 United States v. White, 401 U.S. 745 (1971); Hoffa v. United States, 385 U.S. 293 (1966).

possibility of a confidant spilling their secrets, there should still be Fourth Amendment protection against government intrusions—does not appear. In the first of these two cases, *Hoffa v. United States*,[95] the federal government charged Teamsters Union leader Jimmy Hoffa and three associates in 1964 with jury tampering.[96] An earlier case against Hoffa that took place in 1962, known as the Test Fleet trial, ended in a hung jury; the 1964 case alleged that Hoffa and his associates bribed Test Fleet jurors. In the 1964 case, the government used evidence obtained by one Edward Partin, who was a government informant, to obtain convictions of Hoffa and the others. Partin, a friend and associate of Hoffa's with his own substantial criminal history as well as pending state and federal criminal charges,[97] gained admittance to Hoffa's hotel suite during the Test Fleet trial; he posed as the same ally of Hoffa he had always been, when in fact he had become an informant.[98] After the government obtained convictions for jury tampering, Hoffa argued that placing a government informant within Hoffa's private quarters and among his confidants, without a warrant, violated Hoffa's Fourth Amendment protection against unreasonable searches and seizures.[99] The U.S. Supreme Court did not agree, ruling that Hoffa had no Fourth Amendment protections against the government's use of informant Partin to gather information about him, even though Hoffa's hotel room would have been presumptively private. Hoffa "was not relying on the security of the hotel room; he was relying upon his misplaced confidence that Partin would not reveal his wrongdoing."[100] In making this argument, the Court majority turned to the dissenting opinion in *Lopez* by Justice Brennan. "In the words of the dissenting opinion in *Lopez*," said the majority in *Hoffa*, "'the risk of being overheard by an eavesdropper or betrayed by an informer or deceived as to the identity of one with whom one deals is probably inherent in the conditions of human society. It is the kind of risk we necessarily assume whenever we speak.'"[101] But the *Hoffa* majority omits Justice Brennan's next sentence, emphasizing that intrusion by the government constituted a

95 385 U.S. 293.

96 *Id.* at 294–95.

97 *Id.* at 296–98.

98 *Id.* at 296, 302.

99 *Id.* at 300. Hoffa also argued that his Fifth and Sixth Amendment rights had been violated. *Id.* at 303–04.

100 *Id.* at 302.

101 *Id.* at 303 (citing Lopez v. United States, 373 U.S. 427, 465 (1963) (Brennan, J., dissenting)).

risk "of a different order" and does, in fact, create a constitutional violation.

The Supreme Court misused Justice Brennan's dissent in *Lopez* again the following year, when the Court decided *Katz v. United States*,[102] from which emerged the rule that searches or seizures violate the Fourth Amendment if they intrude upon reasonable expectations of privacy.[103] The question then became whether the *Lopez/Hoffa* "assumes the risk" idea survived the *Katz* decision. In *United States v. White*,[104] in 1971, the Supreme Court said that it did. *White*, another case involving a government informant, gave the Court the opportunity to restate the "assumes the risk" rule. "Inescapably," the majority said,

> [O]ne contemplating illegal activities must realize and risk that his companions may be reporting to the police. If he sufficiently doubts their trustworthiness, the association will very probably end or never materialize. But if he has no doubts, or allays them, or risks what doubt he has, *the risk is his.*[105]

From this brief survey of *Lopez*, *Hoffa*, and *White*, we learn something important about the purpose of this doctrinal transplantation from torts to criminal procedure. The Court used the idea of assumed risk to protect the ability of police to use informants. The Fourth Amendment had taken on new life in the context of every day search and seizure cases. Since *Mapp v. Ohio,*[106] in 1961, the Court had applied the exclusionary rule to the states. Henceforth, no court would countenance purposefully ignoring the Fourth Amendment.[107] After *Katz* and its reasonable expectation of privacy rules, one could not help but ask whether placing an informant into a suspect's home or business to masquerade as a trusted friend violated those reasonable expectations. The continued use of informants, a tool used by police and state authorities since time immemorial, seemed about to collide head on with the Warren Court's new criminal procedure. In

---

102 389 U.S. 347 (1967).

103 The "reasonable expectation of privacy" principle actually comes from Justice Harlan's concurring opinion. *Id.* at 361 (explaining "a twofold requirement" as "[f]irst that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable'").

104 401 U.S. 745.

105 *Id.* at 752 (emphasis added).

106 367 U.S. 643 (1961).

107 For an apt description of what this change meant to a rank and file police office, see Remo Franceschini, A MATTER OF HONOR: ONE COP'S LIFELONG PURSUIT OF JOHN GOTTI AND THE MOB 36–37 (1993) ("All of a sudden . . . [y]ou had to have probable cause . . . . The exclusionary rule essentially shut down police procedure that had been going on for a hundred years.").

order to legally allow continued use of informants, the Court's majority took Justice Brennan's idea of assumed risk (which he did not intend to apply to government action) and turned it on its head (to take away Fourth Amendment protection against government action). And it was the assumed risk idea that became part of the foundation for the third-party doctrine, just a few short years after *White*.

C. The Third-Party Doctrine: An Overreach the Day It Was Decided

When we see that the third-party doctrine rests on a tort idea clumsily grafted into the law of criminal procedure, it becomes clear that this constitutes a shaky rationale for deciding questions of privacy. But the way the third-party doctrine fit into the world at the time of its creation in *Miller* and *Smith* made it something worse than a weak rationale. Even in the 1970s, the third-party doctrine exposed people to government searches that, by any measure, intruded deeply into personal privacy.

The 1970s long pre-dated our era of Internet communications; personal computers did not appear as a mass-produced, fully assembled consumer items until the late 1970s and early 1980s.[108] But even in the 1970s, anyone who wanted to engage in commerce or in the basic connections of social existence needed, at times, to pass information to trusted persons or institutions. *Miller* and *Smith* both make excellent examples. *Miller* involved the use of checks: written orders to an account holder's own bank to pay to the order of a named person a specified amount of money.[109] The account holder uses the check—printed with the crucial information identifying the account holder's bank (the routing number, as well as the name of the bank), the number of the (payor's) account, from which funds will come, and also—filled in by the account holder—the name of the person to receive the money, and the amount of money. All of this information, contained on the check, serves as the set of instructions to a trusted third party (the account holder's bank) to enable a transaction to take place. With modern banks and the banking system, an account holder could transfer large amounts of money and could do so far more safely and faster than if account holder had to use cash. This system enables the parties to more easily engage in greater numbers of commercial exchanges, big and small. This, of course, increases commerce and stimulates activity of all kinds, creating both

108 *See* Dan Knight, *Personal Computer History: The First 25 Years*, LOW END MAC (Apr. 26, 2014), http://lowendmac.com/2014/personal-computer-history-the-first-25-years/.

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

societal and personal benefits. Imagine, then, trying to exist in modern America without the advantages of banks taking and safeguarding our deposits, paying them out as we command, whenever and to whomever we demand. We can, of course, exist in a cash economy, but its disadvantages are many: the exposure to loss and crime alone, some of this crime potentially violent, makes a banking system worthwhile. Yet under *Miller*, the price of modern banking includes the loss of any Fourth Amendment-based protection for the privacy of all information that one must disclose in order to engage in the most basic transactions.[110] Most people would probably find this surprising: they would expect that the relationship with one's bank, and information about personal finances in particular, would be held in confidence. But *Miller* makes this information available to the government without the protection of a warrant issued by a judge.[111]

Smith may be even more startling. The pen register—a device that "records or decodes dialing, routing, addressing, or signaling information,"[112] i.e., the numbers dialed by a caller—collected only this limited information; it did not record the *content* of calls. Still, a complete list of all of the numbers one has dialed could give someone with that information considerable insight into daily activities, beliefs, and relationships. With particular numbers, one could make reasonable guesses about a person's health status (dialing one's cardiologist or oncologist, for example), religious affiliation (calls to one's mosque or temple), romantic life (calling a paramour), sexual orientation (calling a same sex partner), whether or not one gambles (calls to a known bookmaker), or preference for intoxicating substances (calls to a known narcotics dealer). Thus the numbers dialed can be invaluable in any effort to paint a picture of the dialer's life, and could even create leverage—i.e., blackmail material—over the dialer.

Certainly, one could live in the world without using a telephone in the 1970s; some people did (but usually because they could not afford one). But few would do this by choice if they could choose otherwise. By the 1970s, the telephone had become such a ubiquitous feature of life in the United States, 103 years after the invention of

110 *Id.* at 442–43.

111 *Id.* at 443.

112 This definition comes from the federal law governing use of pen registers, particularly 18 U.S.C. § 3127(3). *See also* Smith v. Maryland, 442 U.S. 735, 736 n.1 (1979) (defining the term "pen register").

the device,[113] that no business could exist without one. Yet the price of using a telephone was that the government was absolutely unrestrained in its ability to obtain information about whom a dialer had called. As with banking, the use of something as basic as telephone communication required the surrender of a certain amount of Fourth Amendment rights, even forty years ago.

Thinking back to the 1970s, the price of the third-party doctrine did not stop with Americans' ability to keep private their bank records or phone numbers dialed. A quick thought back to that era easily produces a short list of disclosures that would also not be private under the third-party doctrine:

- Transactions with utility companies to buy electric power, heating fuel, water, and the like, since information on the quantity of each used by the household must be conveyed to the utility;
- Health information, when conveyed to an insurance company, a billing department in a medical services company, or the like;
- Library books and other materials checked out under one's card;
- Information on education, such as which courses one has taken, grades received, or even school disciplinary records; or
- Credit information.

Of course, any of these types of information could receive protection under federal or state legislation. For example, educational information now enjoys protection from disclosure under the Family Educational Rights and Privacy Act ("FERPA").[114] Information given to a health care professional (doctor or pharmacist, for example) is protected from disclosure under the Health Insurance Portability and Accountability Act ("HIPAA").[115] But statutory protections do not give anyone the type of protection afforded by the Constitution. The Fourth Amendment's guarantee of protection against unreasonable searches and seizures remains beyond reach under the third-party doctrine.

III. A DOCTRINE TOO BROAD IN THE 1970S HAS BECOME TODAY'S PRIVACY NIGHTMARE

Let us leave the 1970s, and think about the place of the third-party doctrine in today's world. If sharing important information with

113 Ben Zigterman, *How We Stopped Communicating Like Animals: 15 Ways Phones Have Evolved*, BGR (Dec. 13, 2013, 12:35 PM), http://bgr.com/2013/12/13/telephone-timeline-a-brief-history-of-the-phone/.

114 20 U.S.C. § 1232g.

115 *See generally* 45 C.F.R. § 164.502.

third parties such as banks and telephone companies had already become hard to avoid by the 1970s, in today's world no real options exist. Across multiple dimensions of life, almost anything that does not require physical contact now happens through the Internet. The ubiquity of the online world, in every sector of our activities, means that people can no longer avoid third-party contact involving the exchange of personal data. In short, for the great majority of people in the United States today, much of life takes place online.

Take a brief inventory of the activities of an average American's daily life, and we see that the Internet plays a growing role in most of them. While it is certainly possible not to use online capabilities for some activities, or to use them only sometimes, others have all-but-completely transitioned to the online world, leaving the physical world as a less convenient, seldom used option.

BANKING—Start with banking and telecommunications, the subjects of *Miller* and *Smith*, respectively. In 1973, one could not perform basic personal banking tasks—open an account, write or deposit a check, or withdraw funds, for example—without giving the (third party) bank information about the transaction in a way that, according to the opinion in *Miller*, removed from the transaction any Fourth Amendment protection. This remains true now, only more so. For decades, banks have moved customers toward the use of electronically-connected intermediaries we call automatic teller machines ("ATMs") and away from interaction with bank tellers.[116] ATMs can now do almost anything a human teller can: withdraw cash, check account balances, accept deposits and payments, and the like.[117] For many bank customers, debit cards have supplanted cash and checks as the mode of point-of-sale payment; together, debit and credit card transactions have overtaken total cash and check payments.[118] Bill payment may also run through banks and online services; millions of Americans list their regular payment recipients on the online sites

116 *See* Lauren Abdel-Razzaq, *Banks Redefine Role of Teller in Move Toward Technology*, DETROIT NEWS (Feb. 27, 2015, 11:12 PM), http://www.detroitnews.com/story/ business/ 2015/ 02/27/ technology-changing-bank- teller-role/24156071/ (explaining that moves toward automated technology is "making it much less likely that a customer will interact with a human").

117 Constance Gustke, *Speedy, New ATMs Get High-tech Makeover*, BANKRATE.COM (Feb. 24, 2014), http://www.bankrate.com/finance/banking/new-breed-of-atms-get-high-tech-makeover.aspx.

118 Jeremy M. Simon, *Paper to Plastic: Checks and Cash Losing To Debit and Credit*, CREDITCARDS.COM (Oct. 3, 2007), http://www. creditcards.com/credit -card-news/ debit-credit- card-preferred -payment-1271.php.

and use the sites to make their monthly payments.[119] And of course, all of the information transmitted to third-party banks by individual customers and businesses comes through another third party: Internet service providers ("ISPs").[120] In short, almost any aspect of personal or commercial financial activity will involve giving personal data to a third party—sometimes more than one third party. When dealing with anything except cash, one simply cannot escape the rationale of *Miller*.

TELECOMMUNICATIONS—Like banking, the telecommunications industry—what we would have called the telephone companies in 1979[121]—has become an even more significant recipient of third-party data than it was at the time of *Smith*. In fact, in many practical ways, the telecommunications industry is *the* third party. Telecommunication companies—including not just the descendants of the legacy telephony carriers, but also cable companies (formerly cable television companies) and companies that focus on Internet communications—are the intermediaries for virtually all of the commercial and personal communications of daily life. These companies serve as the third-parties for companies that, by themselves, would not necessarily have third party status. For example, imagine a small business of almost any kind: a specialty cigar store, or a gourmet food business, perhaps. Both of these businesses would likely have brick and mortar locations, at which a customer could come in, browse and locate goods, and pay in cash. But today, many such businesses have online presences as well. The cigar shop or the gourmet outlet can create a website, using online tools and hosted by an Internet service provider. The site will advertise the stores' products, and sell their goods through the third-party web host, and will utilize third-party payment options (debit or credit card companies, non-cash, non-credit payment options like PayPal, or the like). The customer will receive the physical product through shipping by yet another third party: United Parcel Service, Federal Express, or the U.S. Postal Service, just to name a few options, all of whom share connections to the merchant through the Internet. In each phase of these transactions, information is flowing from the consumer to one or more businesses, through third-party telecommunications intermediaries. In turn, the

119 *See* Jane Bryant Quinn, *Should I Pay Bills Online?*, MONEYWATCH (Feb. 5, 2010, 11:38 AM), http://www.cbsnews.com/news/online-bill-pay/ (explaining that millions of users enjoy the efficiency and security benefits of paying bills online).

120 *See supra* note 116 and accompanying text.

121 Smith v. Maryland, 442 U.S. 735, 741 (1979) ("[T]he pen register was installed on telephone company property at the telephone company's central offices . . . .").

sellers of the goods use other businesses, such as shipping companies, to complete the transactions, and this generates yet more data flowing through third-party telecommunications operations.

RETAIL SALES—Amazon started in the 1990s as a company that sold books online, using credit cards or other electronic payment systems. Amazon now sells almost any consumer product imaginable, delivered to the homes of its customers; streaming video entertainment; and even server capacity for businesses.[122] Amazon's Internet-based model has proven so successful that virtually all retail businesses have had to reassess their business models. Even Wal-Mart, the largest American retailer, has had to fight Amazon by enlarging its own Internet presence significantly.[123] More to the point, all of this commerce, and the company's astounding growth, has its basis in third-party transactions: individual customers transmit information to third-party retailers like Amazon, including orders and payment information, and none of this has any Fourth Amendment protection under *Miller* and *Smith*.

MEDICAL INFORMATION—For some years, both the government and large health care companies have moved toward electronic medical records systems.[124] Along with these changes, individual consumers of health care may now manage the day-to-day aspects of healthcare through Internet portals. For example, one typical medical insurance provider encourages all enrollees to use its electronic system for making and changing appointments, obtaining prescription refills, receiving the results of diagnostic tests, and basic communications with their doctors.[125] Patients can access all of their medical records through the system. The system also encourages enrollees to use the system for medical consultation, for 24/7 online

122 *See* BRAD STONER, THE EVERYTHING STORE: JEFF BEZOS AND THE AGE OF AMAZON (Prologue) (2013). This last item does not, strictly speaking, constitute retail sales. At this writing, Amazon makes growing shares of its revenues and operating income. Neil McAllister, *Amazon Lifts Lid on AWS Money Factory, Says It's A $5 BEEEELLION Biz*, THE REGISTER (Apr. 23, 2015), http://www.theregister.co.uk/2015/04/23/amazon_q1_2015_earnings_cloud/.

123 Clare O'Connor, *Wal-Mart vs. Amazon: World's Biggest E-Commerce Battle Could Boil Down to Vegetables*, FORBES (Apr. 23, 2013, 4:53 PM), http://www.forbes.com/sites/clareoconnor/2013/04/23/wal-mart-vs-amazon-worlds-biggest-e-commerce-battle-could-boil-down-to-vegetables/print.

124 *See* Suzanne Allard Levingston, *Electronic Health Records' 'Make-or-Break Year'*, BUSINESSWEEK (Nov. 14, 2013), http://www.bloomberg.com/bw/articles/2013-11-14/2014-outlook-electronic-health-records-make-or-break-year (describing the Obama administration's efforts to introduce a digitally connected health care system).

125 MYUPMC, https://myupmc.upmc.com (last visited July 22, 2015).

medical visits.[126] These systems have many advantages for patients and medical professionals, and they may represent a great improvement in service delivery and cost control. But they also fit perfectly within the *Miller/Smith* paradigm: no Fourth Amendment protection when information goes to a third party, such as the web-based health portal. Of course, Congress has created statutory privacy protections, through HIPAA.[127] But this protection lasts only as long as Congress wants it; Congress can repeal the law tomorrow.

Keep in mind that "medical information" will not only include information about how many appointments a person may have and whether and how the patient pays bills. Information passed through these systems, to physicians, nurses, and other medical service providers—especially through a system that asks patients to submit their symptoms by email and to receive an answer about them same way, and to request prescription medicine refills—will mean that the information about those symptoms and the information about what to do about them will enjoy no Fourth Amendment protection. It is an easy thing to draw inferences from this information: a requested refill for Prozac? The patient probably has some depression or maybe another mental illness. It helps the doctor and the patient when the patient can communicate symptoms and other information to the doctor, quickly and efficiently. But one could imagine a different reaction—a far less positive one—to the idea that this information has no constitutional protection from a government snooping without a warrant.

SOCIAL LIFE AND RELATIONSHIPS—The examples of the ways that social life requires submission of information to and through third parties keeps growing. Facebook comes to mind first; with its 1.49 billion active users,[128] it remains the 800-pound gorilla of social media. A host of others also fill this space: Twitter, LinkedIn, Pinterest, and any number of smaller entities. Aside from these are sites for dating and romance, such as eHarmony.com, Match.com, Chemistry.com, OKCupid.com, Zoosk.com, PlentyofFish.com,[129] and even religiously

126 *Id.*

127 *See supra* note 115 and accompanying text.

128 *Number of Monthly Active Facebook Users Worldwide as of 1st Quarter 2015 (In Millions)*, STATISTA, http://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ (last visited Nov. 2, 2015).

129 *See, e.g.*, Kristen Buck, *Online Dating Review, Reviews and Comparisons*, TOP TEN REVIEWS, http://online-dating-review.toptenreviews.com/ (last visited Apr. 4, 2016) (reviewing the qualities of the best online dating sites such as Match.com).

oriented sites such as ChristianMingle.com and JDate.com.[130] Even those interested in adultery have had a site to visit: AshleyMadison.com.[131] All of these sites oriented to one or another kind of social connection operate with either user-generated content (Facebook), or by using data supplied by the user to the third party to generate a particular result (e.g., the large-database dating sites, such as Match.com, eHarmony.com, and OKCupid.com, use data submitted by users in answers to online surveys to help create matches for patrons). In every way, social media and sites designed to serve a particular social function surely qualify as third parties under *Miller/Smith*.

ENTERTAINMENT—Many entertainment experiences do not require the transmission of personal data and information to third parties. One can still pay cash at the box office for a ticket for a movie or play or concert, an art exhibit or a sporting event, and enjoy the performance or game (assuming, that is, no need for advance purchases or reservations, which could require submission of information, probably including credit card numbers, perhaps via the Internet). But the largest and fastest growing type of entertainment is often quite different. The video gaming industry is now larger than the movie business, with $70.4 billion in worldwide revenue in 2013, compared to $35.9 billion in worldwide box office revenue for movies.[132] And while much of that gaming activity may take place in one's home on one's own equipment, a fast-growing portion of the business consists of multiplayer games: games in which one joins other players online, to play against others or in groups.[133] For these online activities, one needs not only a connection to the Internet (the ISP is, itself, a third party), but also a set of transactions—registration, payment, etc.—with the provider of the game. For this, one must—of course—submit information to the game provider.

---

130 *See Christian Reviews*, RELIGIOUS DATING, http://www.datingsitesreviews.com/staticpages/index.php?page=12 (last visited Nov. 12, 2015) (providing user reviews on religiously oriented dating websites).

131 *See* Charles Riley, *Hackers Threaten to Release Names from Adultery Website*, CNN MONEY (July 20, 2015, 6:16 PM), http://money.cnn.com/2015/07/20/technology/Ashley-madison-hack/ (explaining that the popular online dating website for individuals seeking extramarital relationships was hacked).

132 David Mullich, *Who Makes More Money: Hollywood or the Video Game Industry?*, QUORA (Dec. 14, 2014), http://www.quora.com/Who-makes-more-money-Hollywood-or-the-video-game- industry.

133 *See* Anya Kamenetz, *Why Video Games Succeed Where the Movie and Music Industries Fail*, FAST COMPANY (Nov. 7, 2013, 2:36 PM), http://www.fastcompany.com/3021008/why-video-games-succeed-where-the-movie-and-music-industries-fail (arguing that video games operate as services rather than products).

LEARNING—Parents have always had to give schools some information in order to enroll their children and to keep them eligible to attend. Typically, parents submit information concerning the student's resident status in the district, the student's vaccination and other medical records, who to call in case of an emergency, and even information on medical issues that could arise on any given day, such as allergies, the need for an inhaler, or the like. But today, at every level of the educational process, data on students in the hands of schools abounds. When using software-based learning products, students may be recording their competencies, or evidence of learning disabilities.[134] They may use school computers (e.g., iPads or laptops) that take in all manner of personal information. In higher education, the growing presence of online learning—whether in the form of courses for students at one particular university, or in the form of Massive Open Online Courses ("MOOCs"),[135] which can include thousands of students all over the world—means that students will, as a matter of course, transmit their data to third-parties regularly. These data may identify students, such as information for purposes of registration or payment, or may be the coursework or questions in the course. Whatever it is, the third-party doctrine leaves these data without constitutional protection against government intrusion.

Nevertheless, the third-party doctrine has defenders. Notably, Professor Orin Kerr has defended the doctrine in two articles,[136] because it does no more than ensure a kind of technological neutrality, giving the government the same power under the Fourth Amendment vis-à-vis communications networks as it has in the physical world.[137] Under his analysis, the *Smith* decision is a way to allow the police the same power over a communications network that the police could wield in the physical world.[138] He points out that what happens in the home has Fourth Amendment protection, but that protection does not cover what happens in public. He analogizes the

134 Natasha Singer, *Uncovering Security Flaws in Digital Education Products for Schoolchildren*, N.Y. TIMES (Feb. 8, 2015), http://www.nytimes.com/2015/02/09/technology/uncovering-security-flaws-in-digital-education-products-for-schoolchildren.html?_r=0.

135 Rachel Fishman, *Arizona State to Offer MOOCs for Credit. What Will It Mean for Students?*, NEW AMERICA ED CENTRAL (Apr. 22, 2015), http://www.edcentral.org/global-freshman.

136 *See generally* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005 (2010); Orin S. Kerr, *The Case for the Third Party Doctrine*, 107 MICH. L. REV. 561 (2009).

137 *See* YALE KAMISAR ET AL., BASIC CRIMINAL PROCEDURE: CASES, COMMENTS, AND QUESTIONS 517 (13th ed. 2012) (considering the role of the third-party doctrine in monitoring communications over networks in comparison to communications within physical space).

138 Kerr, *The Case for the Third Party Doctrine*, *supra* note 136, at 578.

contents of communications—in *Smith*, what people say during a phone conversation—to things happening inside a home; metadata—in *Smith*, the numbers dialed—is like what happens in public. Under the Fourth Amendment, the police could surveil actions in public without raising any Fourth Amendment concerns, but they would need a warrant to gather data in any way about what happens inside a home. The same should be true in a communications network: contents (the conversation itself, on the phone; the message itself, in an email message) enjoy Fourth Amendment protection, but the metadata—equivalent to physical information about who the caller interacts with publically—does not. When the defendant in *Smith* harassed his victim using the telephone system, he could hide himself in a way that he could not if the harassment took place in public, where police could observe it.[139] Using a technological device (the pen register) to see who the defendant had called from his phone number does no more than a police officer could do by observing the defendant walking to his victim's house to harass her in the physical world.[140]

Professor Kerr's argument is certainly logical. But it fails to deal with at least two important things. First, *Smith* may be the Supreme Court case most people think of today when they discuss the third-party doctrine, but it was not the only, or even the first, case from the Court to set down the doctrine's parameters. *United States. v. Miller*[141] preceded *Smith* by three years, and the material in that case that received no Fourth Amendment protection went beyond so-called metadata (which phone numbers called what others). Recall that *Miller* created the third-party doctrine in the context of banking, with the government seizing the records themselves, including their contents—not just who had these records or who received them. The government captured the defendant's bank records: "all records of accounts, i.e., savings, checking, loan or otherwise, in the name of Mitch Miller."[142] These items included checks, deposit slips, financial statements, and monthly statements.[143] In the ruling in *Miller* that laid the groundwork for *Smith*, the Supreme Court said that "we perceive no legitimate 'expectation of privacy' in their *contents* . . . . All of the documents obtained . . . contain only information *voluntarily conveyed* to the banks and exposed to their employees in the ordinary course

139 *Id.* at 578.
140 *Id.* at 577–78.
141 *See generally* United States v. Miller, 425 U.S. 435 (1976).
142 *Id.* at 437.
143 *Id.* at 438 (internal quotation marks omitted).

of business."[144] In other words, the Court did not differentiate between message content and message metadata in *Miller*; rather, content had no more Fourth Amendment protection than any "to" or "from" information on the documents because the defendant had given that content to others, voluntarily. Thus assuming Professor Kerr's analogy explains *Smith*, it cannot explain *Miller*.

But there is a larger, more important point that tells us that, even if we accept Professor Kerr's justification of *Smith*, the doctrine remains outdated. There is, quite simply, an immense difference between collecting the numbers called by one person from his or her telephone, and collecting all of the numbers he or she has called for the past year or five years, along with identifying information on all of the web sites the person has visited, every physical location visited, and all of the photographs and videos the person has taken. To quote Chief Justice Roberts' in *Riley*, it is "like saying a ride on horseback is materially indistinguishable from a flight to the moon."[145] The digital world, and the ways in which we can collect, store, analyze, and map the ever-growing pile of data produced on each of us every day is qualitatively different from what we can observe in the physical world. As Justice Sonia Sotomayor said in her concurrence in *United States v. Jones*, the GPS case, the doctrine simply does not fit the digital age.[146] The assembled digital mosaic of our individual lives, contained in any smart phone, must receive Fourth Amendment protection, unless we would grant our government unlimited access to a detailed record of virtually everything we do in our lives, just for the asking. As Justice Sotomayor implies, this just cannot be right, and it is ludicrous to think that Americans would simply accept it without question.[147]

IV. THE SUPREME COURT'S DISCUSSION OF THE THIRD-PARTY DOCTRINE IN *RILEY*

In the *Riley* opinion, the Court discussed the third-party doctrine once, and only briefly.[148] The Justices spent far more time discussing issues that spring from the concerns above: so much of the information we depend upon today finds its way onto the phones that an incredibly high percentage of Americans carry with them almost all

144 *Id.* at 442 (emphasis added).
145 Riley v. California, 134 S. Ct. 2473, 2488 (2014).
146 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).
147 *Id.* (Sotomayor, J., concurring).
148 *Riley*, 134 S. Ct. at 2486.

the time.[149] These two parts of the discussion might look unrelated, but in the end they have much to do with each other.

The Court's direct discussion of the third-party doctrine came toward the end of the opinion, in the context of an argument by the government that officers seizing a phone should always have the authority to search the phone's call log without having to obtain a warrant. The authority cited by the government for this proposition was *Smith v. Maryland*, of course, which allowed police to use a pen register to obtain the numbers dialed from a particular phone without first getting a warrant.[150] The Court dismissed the government's argument out of hand, because in *Smith* the Court had "concluded that the use of a pen register was not a 'search' at all under the Fourth Amendment."[151] By contrast, there was no question that in *Riley* that "the officers engaged in a search of [Defendant's] cell phone."[152] This statement seems curious indeed. If *Smith* is still good law (and the Court does not repudiate *Smith* in *Riley*), then a search of a phone's data that revealed only the numbers dialed on the phone's call log[153] cannot amount to a search for Fourth Amendment purposes, either. The Court seems to want to have things both ways: searching data on a smart phone, even just the numbers dialed as listed in the call log, is a Fourth Amendment search according to *Riley*; but under *Smith*, the third-party doctrine says that obtaining the numbers dialed using another technology is not a Fourth Amendment search. This reveals a conflicted rationale: on the one hand, wanting the data on smart phones protected, because of the massive intrusion on privacy that warrantless searches of smart phone searches would constitute, and on the other hand not wanting to overrule *Smith* and the third-party doctrine, which has always favored and served law enforcement.

When the Court gets to the larger question of the privacy costs of allowing warrantless searches of data on cell phones, however, it takes a very broad view. Smart phones today are "minicomputers" with "immense storage capacity"[154] that might contain "millions of pages of text, thousands of pictures, or hundreds of videos," not to mention

149 *Id.* at 2484.

150 *See id.* at 2492 (citing Smith v. Maryland, 442 U.S. 735, 745–46 (1979), for the proposition that use of a pen register to record dialed phone numbers was permissible).

151 *Id.*

152 *Id.* at 2492–93 (citation omitted).

153 The Court does say that information, in addition to the numbers dialed, is also available on the call logs of most phones. *Id.* at 2493. But this does not answer the question of whether or not the log might be viewed only to reveal the numbers dialed.

154 *Id.* at 2489.

"text messages, Internet browsing history, a calendar," and other treasure troves of personal data.[155] Putting all of this information together gives the government a unique and nuanced picture of an individual's life, because the data "reveal much more in combination than any isolated record."[156] The browsing data, along with location data, the Court said, seem "qualitatively different" in terms of their capacity to reveal "private interests or concerns," such as health, and physical whereabouts reconstructed along a precise timeline can trace out a person's "familial, political, professional, religious, and sexual associations."[157] These phones have become so ubiquitous, the Court said, that three-quarters of Americans report having their devices within five feet of them most of the time, and 90% of these phones contain, "a digital record of nearly every aspect of [their owner's] lives,"[158] even surpassing the quantity of records one would typically find in someone's entire home.[159]

This vast trove of data, much of it highly personal and extremely revealing, simply had to have the protection of the Fourth Amendment against warrantless searches, the Court said. The new technology of the Internet, and the devices available to us, mean that our old assumptions about searching the objects found in the pockets of clothing simply do not hold when the object in question is a smart phone. And this new reality, the Court said, does not depend on whether the data on the cell phone come directly from inside the phone itself, or from a remote storage area —the cloud, in today's common parlance. It is the nature and quantity of the data accessed from the phone that matters, not where the data resides.

At least in the context of smart phones and other digital devices, the application of the Court's privacy discussion to all data accessible from the device amounts to nothing less than an implicit repudiation of the third-party doctrine. Data located in the cloud can *only* be seen as having been conveyed to a third party: the owner of the servers on which the data sits. Thus, without saying so, the Court's opinion in *Riley* crosses a long-standing barrier. Information passed to a third party, and accessed remotely from the computers of that third party, which would clearly fall on the unprotected side of the *Miller/Smith* third-party rule, *does have protection under the Fourth Amend-*

155 *Id.*

156 *Id.* at 2479.

157 *Id.* at 2490 (quoting United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring)).

158 *Id.* at 2479.

159 *Id.* at 2491.

ment. And if that is so, the third-party doctrine has effectively been breached, and this may be the beginning of its end. True, the Court inserts a sentence to prop up the doctrine. But the very mildness of that support—just saying that, under *Smith*, collecting dialed phone numbers did not constitute a search and required no warrant – may constitute the first faint signal that the Court knows it cannot have things both ways. If the third-party doctrine is correct, data contained on remote servers, accessed by the smart phone user, has no expectation of privacy and no Fourth Amendment protection. If the data on remote servers carries an expectation of privacy for Fourth Amendment purposes, the third-party doctrine can no longer stand as it has since the 1970s. And of these two possibilities, the Supreme Court seems to have chosen the latter. This way of thinking has much less in common with the *Miller/Smith* third-party doctrine's view of privacy than with Justice Sotomayor's concurring opinion in *Jones v. United States*., in which she described the third-party doctrine as

> ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[160]

At bottom, this seeming contradiction comes not as a result of a sudden shift of opinion on the Court with regard to privacy. Rather, it comes from a material change in widely available technology. This change is significant enough that it has forced the Court to re-think its assumptions about privacy, and other changes must follow. Fortunately, we have an example to guide us, from the not-too-distant past, that will allow us to see what the way forward might look like.

V. FROM *OLMSTEAD* TO *KATZ*: HOW ADVANCES IN WIRETAPPING FORCED A CHANGE IN THE LAW

A. The History of Another Technological Innovation

To know whether the U.S. Supreme Court might change its view of the third-party doctrine, even abandoning it, despite the fact that the Court did not do so in *Riley*, we can look back to the early twentieth century. By the 1920s, technology available to law enforcement had changed: with the ubiquity of the telephone and telephone service, wiretapping had become part of law enforcement's arsenal. To-

160 132 S. Ct. at 957 (Sotomayor, J., concurring).

wards the end of that decade, the Supreme Court had to face the question whether using wiretaps without prior judicial approval in the form of a warrant violated the Fourth Amendment.

Today, the case of *Olmstead v. United States*[161] is chiefly remembered for the dissent of Justice Louis Brandeis,[162] as he looks ahead to the country's future if the police are allowed to use wiretapping without restriction by courts. Justice Brandeis believed that warrantless wiretapping violated the Fourth Amendment, and that the prosecution's use of any evidence gathered through a warrantless wiretap violated that constitutional provision. In the simplest terms, wiretapping constituted lawbreaking.[163] Almost ninety years later, judges, scholars, and students still quote his dissent.

> Our Government is the potent, the omnipresent teacher. For good or for ill, it teaches the whole people by its example. . . . If the Government becomes a lawbreaker, it breeds contempt for law; it invites every man to become a law unto himself; it invites anarchy. To declare that, in the administration of the criminal law, the end justifies the means—to declare that the Government may commit crimes in order to secure the conviction of a private criminal—would bring terrible retribution.[164]

Much less remembered, however, is that the majority opinion in *Olmstead* declared that use of a wiretap to gather the contents of a telephone conversation, when the wiretap did not take place inside the home, did not constitute a search for Fourth Amendment purposes and required no warrant. According to Chief Justice William Howard Taft, no violation of the Fourth Amendment occurred "unless there has been an official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or *an actual physical invasion* of his house 'or curtilage' for the purpose of making a seizure."[165] The requirement of "an actual physical invasion" made all the difference in the case, because the Fourth Amendment analysis at that time turned on whether the defendant had suffered a trespass by the government in the gathering of the evidence. The invention of the telephone, the majority said, had upended many of our expectations and customs.

> By the invention of the telephone, fifty years ago, and its application for the purpose of extending communications, one can talk with another at a far distant place. The language of the Amendment can not be extended and expanded to include telephone wires reaching to the whole world

161 277 U.S. 438 (1928).
162 *Id.* at 471 (Brandeis, J., dissenting).
163 *Id.* at 479 (Brandeis, J., dissenting).
164 *Id.* at 485 (Brandeis, J., dissenting).
165 *Id.* at 466 (emphasis added).

> from the defendant's house or office. The intervening wires are not part of his house or office any more than are the highways along which they are stretched.[166]

What the Fourth Amendment protected, Chief Justice Taft implied, was not the conversation itself, but the physical aspect of the home. The defendant had a "telephone instrument" installed in the house, and then wires carried conversations beyond the house;[167] the government intercepted the conversations outside the house, never entering the dwelling – and therefore committing no trespass. Therefore, the warrantless wiretap had not violated the Fourth Amendment. Congress, the Chief Justice said, could create legislation that would make it illegal to use wiretaps outside the confines of the home, but the Court could not do this by interpreting the Fourth Amendment more broadly.[168]

Nearly forty years later, the Court changed course, prompted in no small part by new technology. In *Katz v. United States*,[169] the government charged the defendant with federal offense of transmitting "wagering information" over interstate telephone lines. To prove the case, the government introduced not recordings or transcripts of conversations about gambling captured through traditional wiretaps, but something else: "evidence of the [defendant's] end of telephone conversations, overheard by FBI agents who had attached an electronic listening and recording device to the outside of the public telephone booth from which [defendant] had placed his calls."[170] The agents had obtained the defendant's part of the conversations in the telephone booth by using a contact microphone: a microphone capable of successfully picking up a conversation from inside a telephone booth or an adjacent room, when attached to the other side of the wall.[171] One of these contact microphones was attached to the top of the telephone booths defendant Katz used to discuss gambling and bookmaking. According to the Court of Appeals, which heard the case before it went before the Supreme Court, the agents placed the microphones "on the tops of two of the public telephone booths normally used by the [defendant] . . . with tape. There was *no physical*

166 *Id.* at 465.

167 *Olmstead*, 277 U.S. at 466.

168 *Id.* at 465–66.

169 389 U.S. 347 (1967).

170 *Id.* at 348.

171 According to the *Merriam-Webster Dictionary*, a contact microphone is "a microphone designed to be used in contact with the source of sound or with a resonating or conducting surface." MERRIAM-WEBSTER DICTIONARY ONLINE, http://www.merriam-webster.com/dictionary/contact%20microphone.

penetration inside of the booths."[172] Technology, it seemed, had advanced to the point that microphones *outside* a structure could capture the sound of a person speaking *inside* the structure.

It was this last fact upon which the government leaned in its argument to the Supreme Court. Capturing the defendant's side of the conversation in the telephone booth did not violate the Fourth Amendment, the government said.[173] And this approach made perfect sense at the time. In a ruling which had by then stood for almost forty years, the Court in *Olmstead* had said that the crucial point was whether or not a physical trespass had taken place. Since police had installed the wiretap in *Olmstead* outside the home, with no physical invasion, the wiretap without a warrant did not violate the Constitution. Naturally, the government reasoned that if they could capture a conversation—that is, half a conversation—without invading a constitutionally protected area, its actions in *Katz* did not violate the Fourth Amendment, and should therefore stand.

But in its *Katz* opinion, the Supreme Court decided that *Olmstead* and the whole idea that a violation of the Fourth Amendment should turn on an invasion of property rights had become outmoded. Technology had made the rule dangerously obsolete: constitutional protection against only physical violations of places seemed quaint, when available devices could change the reality that one usually could not hear into a telephone booth without standing close enough to be seen. With new technology, police had no need to stand close, and have the bad guy see them; instead, they could tape a contact microphone to the top of the booth and listen from a distance, gathering valuable evidence undetected. This technological change forced the Court to change course, and to change the Fourth Amendment's focus. Going forward, the Court said, "the correct solution of Fourth Amendment problems is not necessarily promoted by incantation of the phrase 'constitutionally protected area.' . . . or the Fourth Amendment protects people, not places."[174] Instead of looking to the physical setting and whether the government had penetrated it, look instead to what a person knowingly exposes to the public, versus what he seeks to preserve as private.[175] The place in which this happens—a public telephone booth, a home office, or a public park—constitutes a secondary consideration. In the words of Justice Harlan's oft-

172 Katz v. United States, 369 F.2d 130, 131 (9th Cir. 1966) (emphasis added).
173 *Id.* at 352.
174 *Id.* at 350–51.
175 *Id.* at 351.

quoted concurring opinion in *Katz*, "there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[176] Thus the *Katz* case, and its exposure of how new but common technology that made previous ways of thinking obsolete, became the occasion for overruling *Olmstead*. Trespass upon property rights would no longer constitute the measuring stick for whether an intrusion into Fourth Amendment territory had occurred; that way of looking at things was simply no longer tenable.

We sit now at a similar point. The third-party doctrine may once have made sense to the Court,[177] as basing Fourth Amendment rights on trespass law did in 1928. But widely available technology has progressed to the point that the assumptions underlying the third-party doctrine simply do not fit the world. The contact microphone could capture a conversation inside a closed structure, without penetrating it, rendering the requirement for a violation of trespass law unnecessary. The advent of smart phones that can access data remotely, which is the way that most data today is stored and accessed, renders the third-party doctrine wildly out of step with the world. Unless Americans can say without hesitation that all of their data should become available to the government upon a simple request to a third-party service provider, without the benefit of warrant issued by a judge, things must change. Our moment today resembles what the Supreme Court faced in *Katz*; the old regime must fall.

B. The Way Forward

What, then, should happen if *Riley* turns out to be the beginning of the end of the for the third-party doctrine? This is a question any critic of the existing structure must face. After all, law enforcement makes wide use of its powers under the third-party doctrine now. The question of what, if anything, should take its place looms large, when we consider how police must face criminals and conduct investigations.

176 *Id.* at 361.

177 While the third-party doctrine *may* have made sense to the court at the time, as explained above in notes 3–18, *supra*, I believe it was a mistaken approach and far too broad from the very beginning.

Various solutions, all of some complexity, have been proposed; all take a critical view of the doctrine.[178] They all seek an answer to the real question: what protection should our communications with third parties, so essential in today's digital world, enjoy? But with just one exception,[179] they do not explain how our nation could arrive at any new standards.

The history just reviewed above, from *Olmstead* to *Katz*, holds the key. In the *Katz* era, with its technological advances in wiretapping and other listening technologies, an old fashioned response emerged: legislatures, not the Supreme Court, took the lead. In 1968, the U.S. Congress revised its antiquated wiretapping law[180] and passed the Federal Wiretap Act,[181] also known as Title III. The revised law directly addressed two major concerns at the time: "bugging," the use of secret recording technologies in a room or a space to intercept "oral communications," such as the telephone booth in *Katz*, and the interception of private telephone communications ("wire communications"). The new law addressed these activities by both government and private parties, and required the government to obtain court orders for this activity only if federal agents had probable cause and only if they could meet a number of further requirements. If permitted by a court order, agents would still face a number of important regulations on how they could conduct these activities. State legislatures also responded, passing wiretapping laws of their own.[182] Some of

178 *See generally* ABA STANDARDS FOR CRIMINAL JUSTICE: LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS (3d ed. 2013); CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 153– 54; 156–57; 171; 183– 84 (Univ. of Chicago Press, 2008); David Gray, *The ABA Standards for Criminal Justice: Law Enforcement Access to Third Party Records: Critical Perspectives from a Technology-Centered Approach to Quantitative Privacy*, 66 OKLA. L. REV. 919 (2014); 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); Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information form Unreasonable Search*, 55 CATH. U. L. REV. 373 (2006).

179 Henderson, *Learning from All Fifty States*, *supra* note 178, at 373–76.

180 The old law on wiretapping was part of the Communications Act, 47 U.S.C. § 605 (1934).

181 18 U.S.C. § 2510–2522 (1968).

182 Ala. Code § 13A-11-30(1); Alaska Stat. §§ 42.40.300(a) & 42.20.310(a)(1); Ariz. Rev. Stat. Ann. § 13-3005; Ark. Code Ann. § 5-60-120(a); Cal. Penal Code § 632(a); Colo. Rev. Stat. § 18-9-303(1); Conn. Gen. Stat. Ann. § 52-570d(a); Del. Code. Ann. tit. 11, § 1335(a)(4); D.C. Code. Ann. § 23-542(b)(3); Ga. Code Ann. §§ 16-11-62; Haw. Rev. Stat. §§803-42(b)(3) & 711-1111(1)(d); 720 ILS 5/14-2"(a); Ind. Code Ann. § 35-33.5-1-5(2); Iowa Code Ann. §§ 727.8 & 808B.2(2)(c); Kan. Stat. Ann. §§ 21-4001(a)(3) & 21-4002(a)(1); Ky. Rev. Stat. Ann. § 526.010; Md. Code Section 10-402. Courts and Judicial Proceedings Article; Minn. Stat. Ann § 626A.D2 subd. 2(d); Miss. Code Ann. § 41-29-531(e); Mo. Ann. Stat. § 542.402(2)(3)(Supp.); Mont. Code Ann. § 45-8-213; Neb. Rev. Stat. § 86-702(2)(c); Nev. Rev. Stat. §§ 200.620 & 48.077; N.J. Rev. Stat. § 2A:156A-4(d); N.M. Stat. Ann §30-12-

these state laws were more stringent than the federal law, requiring police to jump through additional hoops and limiting police conducting of surreptitious recording in ways that the federal law did not.[183]

The important point is that, with the third-party doctrine not just accommodated to but wiped away, our legislatures would have the opportunity—indeed, they would face the necessity—of having the kind of conversation about privacy we so badly need. What digital records of citizens should enjoy protection from government surveillance, absent probable cause? What kind and degree of such surveillance is appropriate when probable cause is present? Rather than failing to protect our digital details simply because they are not secret from everyone, our representatives would need to ask "when and how should our digital lives be protected, and how should we protect that in legislation?" Whether or not our digital information is secret from all third parties is no longer a viable way to look at the question of government surveillance, if it ever was. Rather, the question should be what protection for our privacy we, as a society, wish to have.

CONCLUSION

The third-party doctrine, which allows the government to obtain any information that a person sends to a third party without a warrant, has become an open door to government snooping. For more than four decades, under this rule the government has been free to get information sent to a third party by a citizen, even if the citizen and the third party agree that the information will stay private and will only be used for very limited purposes. In today's world, with the

---

1(C)&(E); N.Y. Penal Law §250.00(1); N.C. Gen Stat. § 15A-287(a); N.D. Cent. Code §12.1-15-02(3)(c); Ohio Rev. Code Ann. § 2933.52(B)(4); Okla. Stat. Ann. tit. 13, §176.4(5); 18 Pa. Cons. Stat Ann. § 5704(4); R.I. Gen. Laws §11-35-21(c)(3); S.D. Codified Laws Ann. § 23A-35A-20(1); Tenn. Code Ann. § 39-13-601(b)(5); Tex. Penal Code Ann. § 16.02(b); Utah Code Ann. §§ 76-9-401(2), 76-9-403(1)(a), & 77-23a-4(7)(b); Wash. Rev. Code Ann. § 9.73.030(1)(a); W. Va. Code § 62-1D-3; Wis. Stat Ann. §§ 968.31(c) &885.365(1); Wyo. Stat. § 7-3-602(b)(iv).

183 At least twelve states require more than the Federal Government to allow an interception or a recording of a phone call, in terms of the most basic criterion. While the Federal Government (and most states, for that matter) require only the consent of one party to the conversation to allow interception or recording without a warrant, twelve states require that both parties to the conversation consent. Those states include California, Connecticut, Florida, Illinois, Maryland, Massachusetts, Michigan, Montana, Nevada, New Hampshire, Pennsylvania, and Washington. REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS, REPORTER'S RECORDING GUIDE: TAPE-RECORDING LAWS AT A GLANCE (2012), https://www.rcfp.org/reporters-recording-guide/tape-recording-laws-glance.

most personal kinds of information sent to third parties and accessed from third parties untold millions of times every day, the third-party doctrine has become a distinct danger to the privacy of everyone who uses modern communication tools housed in the typical smart phone.

Fortunately, whether intending to or not, the Supreme Court has begun to move the law away from the third-party doctrine. The Court's opinion in *Riley* does not overrule the *Miller* or *Smith* cases, but *Riley* forced the Justices to recognize reality: if the data in a smart phone enjoyed Fourth Amendment protection, so too did data not in the phone but accessed from a third party through the phone. There is no practical difference between the two, and in a subsequent case, the Court will find the pull to uproot the third-party doctrine too much to resist. That day does not lie far in the future.