Riley and the Third-party Doctrine

This article was originally published in *Westlaw Journal* on April 9, 2015.

by Marley Degner

Marley Degner
Litigation
415.983.1186
marley.degner@pillsburylaw.com

Marley Degnar is a counsel in Pillsbury's Litigation practice in the San Francisco office.

On June 25, 2014, the U.S. Supreme Court issued one groundbreaking opinion in two cases regarding cellphone searches incident to arrest. In a unanimous opinion, the court held that under the Fourth Amendment, police must obtain a warrant prior to searching the cellphone of an arrestee. The court found that the "immense storage capacity" of cellphones and their aggregation of data differentiated them from other items found on an arrestee's person. Chief Justice John G. Roberts Jr. wrote that cellphones "could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."[1]

This commentary situates the *Riley* decision in the broader context of technology search cases and analyzes its potential implications for companies faced with a government request to turn over customer data. The Supreme Court's acknowledgments of the altered technological landscape and the sensitivity of user data signal a potential shift in its third-party guidance, and its decision is a hopeful sign for companies seeking to protect user privacy in the face of digital data requests from the government.

The Third-party Doctrine: An Overview

The third-party doctrine states that an individual does not have a reasonable expectation of privacy in any communication that is "voluntarily conveyed" to another. Whether this concerns a conversation with an informant, or transmissions to banks and telecommunications companies, the Supreme Court has generally held that if the information is made available to a third party, the government may access it without a warrant.[2]

In 1928 the high court held that warrantless wiretapping of telephone lines did not violate the Fourth Amendment, provided there was no physical trespass on an individual's land. In dissent, Justice Louis D. Brandeis argued that the U.S. Constitution must be adapted to a changing world. He noted that "[s]ubtler and more far-reaching means of invading privacy have become available to the government."[3]

Almost 40 years later, the court overturned that decision, holding that the warrantless wiretapping of a public telephone booth violated a defendant's constitutional rights because the Fourth Amendment "protects people, not places."[4] As

explained in Justice John Marshall Harlan II's concurrence, the standard for Fourth Amendment protection was whether the individual had a reasonable expectation of privacy.

In 1971 the court held that a person does not have a reasonable expectation of privacy under the Fourth Amendment in information voluntarily disclosed to a third party who turns out to be a government informant.[5] The court continued extending the third-party doctrine throughout the 1970s, holding in *United States v. Miller* that documents "voluntarily conveyed" to a bank could be shared with the government, regardless of the defendant's subjective expectation of privacy.[6] By the end of the decade, in *Smith v. Maryland*, the court found that an automated machine or system qualified as a third party; it ruled that law enforcement did not need a warrant to obtain telephone numbers that a defendant voluntarily revealed to the switching equipment at the telephone company.[7] The case involved a mechanical device called a pen-register that the telephone company installed at its central offices, at police request, to record the numbers dialed from the defendant's home for four days.

The court found the defendant did not have a reasonable expectation of privacy in the telephone numbers he dialed because it was generally understood that the telephone company can and does record these numbers. The court concluded that regardless of its automated nature, the telephone company's switching equipment was no different from an "operator who, in an earlier day, personally completed calls for the subscriber."

In 2012 the Supreme Court's holding in *United States v. Jones*, and Justice Sonia Sotomayor's concurrence in that case, signaled that it was starting to shift away from its third-party analysis.[8] In *Jones* the Supreme Court unanimously held that placing a GPS tracker underneath a vehicle to trace the owner's movements constituted a search and required a warrant. While the majority opinion was based on a theory of property and trespass, Justice Sotomayor focused on privacy in her concurrence, arguing that the movements of the car revealed far more about the driver than his location. She argued that the third-party doctrine is "ill-suited to the digital age."[9]

The Third-party Doctrine, Internet Communications and Bulk Data

Companies such as Google and Amazon store their customers' personal data on their servers. Under a strict application of the third-party doctrine, an Internet user would lose a reasonable expectation of privacy in such data, as it has been voluntarily conveyed to external servers. The Supreme Court has not directly ruled on this issue, and lower courts have disagreed on how to apply the third-party doctrine to the Internet.[10]

The court found that the "immense storage capacity" of cellphones and their aggregation of data differentiated them from other items found on an arrestee's person.

Federal courts remain at odds as to how to apply the doctrine to National Security Agency requests for bulk customer metadata information.[11] Three NSA cases are pending before appellate courts, and all three turn on those courts' interpretation of *Smith*.[12] The government frequently cites *Smith* in cases involving Internet surveillance and data requests.

In 2010 the 6th U.S. Circuit Court of Appeals held in *United States v. Warshak* that a reasonable expectation of privacy applies to the content of emails stored with commercial Internet service providers.[13] The *Warshak* court held that "the mere *ability* of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy." The appeals court analogized emails to letters and phone calls, and noted that the police cannot intercept a letter's contents without a warrant even after the letter has been handed over to mail carriers for delivery. The court distinguished *Miller* by explaining that email communications were more confidential than "simple business records," and by noting that the ISP was only an intermediary and not the intended recipient of the communications.

Congress has also legislated to protect electronic communications. The Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2701, attempts to provide a comprehensive scheme to restrict unauthorized government surveillance of electronic communications. However, the law fails to provide adequate protection; courts have interpreted parts of it to permit the government to acquire electronic communications without a warrant.[14]

In both *Miller* and *Smith*, the Supreme Court held that one who voluntarily reveals information to a

business, like one who voluntarily reveals information to a government informant, takes the risk that that business will betray that confidence and divulge that information to the police. But many Americans expect that all sorts of things exposed to third parties will remain private, and they would argue that their decision to entrust private information to companies is not truly voluntary if they wish to participate fully in society.

Companies, which routinely collect and store customer information for a variety of reasons, including for marketing purposes, thus find themselves trapped between customers who are concerned about privacy and the government. Some companies have resisted the government's attempts to obtain customer data without a warrant—even in the face of statutes that appear to require them to do so.[15]

However, in the aftermath of Edward Snowden's disclosures of classified information from the National Security Agency, some telecommunications and Internet companies were perceived as having a troublingly close relationship with the government. Since the Snowden revelations, more companies are publishing transparency reports and law enforcement guides, as well as publicly opposing mass surveillance.

Some companies, such as Amazon, AT&T, Apple, Verizon, Yahoo, Credo Mobile and Google, have expressed a commitment to requiring warrants from law enforcement before they will turn over the contents of user communications (as opposed to metadata), even though the law is currently unsettled.[16]

Google recently filed a friend-of-the-court brief in a case before the Supreme Court urging the court to reconsider the third-party doctrine.[17] AT&T also filed a friend-of-the-court brief in a case currently in the 11th Circuit where, citing to *Riley* and *Jones*, it argued that *Smith* and *Miller* are ill-suited to the digital age.[18] The *Riley* decision signals that the Supreme Court may be willing to revisit the third-party doctrine so that companies can more effectively shield customer data, including customer metadata.

Riley is Act I

If *Jones* set the stage, *Riley* represents the first act of Supreme Court, as it engages fully with the digital age.

[The Riley] decision is a hopeful sign for companies seeking to protect user privacy in the face of digital data requests from the government.

In *Riley* the court held that police generally may not conduct cellphone searches incident to arrest without a warrant. With this ruling, the court deviated from 1970s precedents permitting the search of items immediately associated with an arrestee's person, such as a wallet. The court recognized that the search of a cellphone implicates substantially greater individual privacy interests than the search of other physical items typically found on an arrestee's person.

The court also justified its ruling with the observation that cellphone searches do not implicate the two rationales underlying the search-incident-to-arrest exception to the warrant requirement: officer safety and evidence preservation or destruction. The court wrote that these concerns, including potential evidence destruction through remote wiping or data encryption, are better dealt with on a case-by-case basis.

The language of the opinion will likely apply to other types of technological searches. For example, the court's observation that cellphones are "minicomputers" suggests that police should also be required to get a warrant to search laptops and tablets incident to arrest.

Like the majority in *Jones*, the court makes no explicit mention of the third-party doctrine in its analysis. Moreover, in a footnote, the court said the two cases did not implicate the question of whether the collection or inspection of aggregated digital information amounted to a search under other circumstances.

However, the court recognized that the volume and type of personal information potentially available to the government at the time of arrest has changed so dramatically since the 1970s that precedents from that era do not control the analysis. This reasoning could apply with equal force to the third-party doctrine, which is similarly grounded in cases decided in the 1970s before the advent of email, smartphones and cloud computing.

One criticism of the doctrine is that entrusting information to third parties is not truly voluntary in the modern age. We could theoretically store our money in shoe boxes under our beds and communicate with others exclusively via letter, but that does not make our decision to open a

bank account or use email "voluntary." The Supreme Court hints it might be receptive to the argument that something is not voluntarily conveyed to a third party if it is commonly or ubiquitously conveyed when it writes that modern cellphones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[19]

A passage in the majority opinion also has potential implications for cases involving cloud computing, as well as for cases where the government argues that it can adequately protect constitutional rights with self-imposed safeguards.[20] Chief Justice Roberts notes that modern storage technologies allow a person to store data beyond a physical device, adding that this presents practical problems for law enforcement officers, who typically do not know where data is stored.[21]

The government proposed, among other solutions, that law enforcement agencies could develop protocols to address the concerns raised by cloud computing. Chief Justice Roberts' retort was that this was "[p]robably a good idea, but the Founders did not fight a revolution to gain the right to government agency protocols."[22]

Chief Justice Roberts analogizes the ability of law enforcement to access the cloud through a cellphone search to "finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house."[23] This language suggests that the court would view government access to data stored on the cloud, in situations beyond a search incident to arrest, as comparable to access to a person's home, because of the volume of private information that can be stored on the cloud.

The government suggested, among other limiting principles, a holding that officers could search cellphone data if they could have obtained the same information from a pre-digital counterpart such as an address book found in a person's pocket. The court rejected this analogue proposal on the grounds that such a test would result in a significant diminution in privacy and would force the government to determine which digital files were comparable to which physical records (the court asked, "Is an e-mail equivalent to a letter?").[24] This language demonstrates that the court may hold that email cannot be reduced to the electronic version of postal letters and, as such, suggests that the court will not adopt a content/non-content approach like the one adopted by many courts, including the *Warshak* court.

The third-party doctrine states that an individual does not have a reasonable expectation of privacy in any communication that is "voluntarily conveyed" to another.

The opinion also quotes Justice Sotomayor's concurrence in *Jones* to show that even noncontent records such as call logs and location data (as generated by a GPS) can reveal sensitive information about an individual. This reasoning could, among other things, undermine the government's third-party argument in NSA data collection cases.[25]

Riley is also noteworthy because it is the Supreme Court's second unanimous opinion in two years regarding technology and searches. At their core, cases such as *Jones* and *Riley* recognize that today's technology was not contemplated in the 1970s (when the third-party doctrine arose), or even 10 years ago. The court's willingness to adapt the Fourth Amendment to the modern era and create a new bright-line rule for cellphone searches suggests that it may continue moving in this direction and close the third-party loophole for digital data.

Endnotes

1 *Riley v. California*, 134 S. Ct. 2473, 2489 (2014).

2 Note that various state courts have interpreted their state constitutions to provide stronger privacy protections than the Fourth Amendment. Congress has also legislated to provide some protection to banking records and telephone dialing records. *See* Hanni Fakhoury, *Smith v. Maryland Turns 35, But Its Health Is Declining*, Electronic Frontier Foundation Deeplinks Blog (June 24, 2014), https://www.eff.org/deeplinks/2014/06/smith-v-maryland-turns-35-its-healths-declining; *see also* Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-22 (2006); 18 U.S.C. §§ 3121-27 (2006) (telephone dialing records).

3 *Olmstead v. United States*, 277 U.S. 438, 473-74 (1928) ("Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.").

4 *Katz v. United States*, 389 U.S. 347, 351 (1967).

5 *United States v. White*, 401 U.S. 745, 752 (1971).

6 425 U.S. 435, 442 (1976).

7 442 U.S. 735 (1979).

8 132 S. Ct. 945 (2012).

9 *Id.* at 955, 957 (According to Justice Sotomayor, the third-party doctrine "is ill-suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. …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.").

10 *See, e.g., Smith*, 442 U.S. 735; *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010); *United States v. Hambrick*, No. 99-4793, 2000 WL 1062039, at *3 (4th Cir. Aug. 3, 2000); Monu Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply*, 54 B.C. L. Rev. 1, 3 (2013).

11 Compare *ACLU v. Clapper*, 959 F. Supp. 2d 724 (S.D.N.Y. 2013), with *Klayman v. Obama*, 957 F. Supp. 2d 1, 31-32 (D.D.C. 2013). The New York federal court ruled that the NSA's collection of phone metadata was constitutional based on *Smith*, while the Washington federal court enjoined the government from collecting plaintiffs' call records under the mass surveillance program on the grounds that plaintiffs had demonstrated a substantial likelihood of success on the merits of their Fourth Amendment claim, and held that the limited pen-register records in *Smith* could not be analogized to the bulk metadata collection of the NSA.

12 *Klayman v. Obama*, Nos. 14-5004, 14-5005, 14-5016, 14-5017 (D.C. Cir.); *ACLU v. Clapper*, No. 14-42 (2d Cir.); *Smith v. Obama*, No. 14-35555 (9th Cir.).

13 *Warshak*, 631 F.3d at 286.

14 Bedi, *supra* note 10, at 31-35; 18 U.S.C. §§ 2510-22, 2701-11, 3117, 3121-27 (2006); *see, e.g., Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107 (3d Cir. 2003) (ECPA does not protect email communications stored on servers); *United States v. Weaver*, 636 F. Supp. 2d 769, 773 (C.D. Ill. 2009) (no protection for previously read emails).

15 *See, e.g., Doe v. Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y. 2004), *vacated sub. nom. Doe v. Gonzales*, 449 F.3d 415 (2d Cir. 2006) (Internet service provider that received a national security letter from the FBI requiring the production of customer records without a warrant brought an action challenging the Patriot Act provisions authorizing national security letters and imposing a permanent gag order on those who received the letters); *Weaver*, 636 F. Supp. 2d at 770 (in response to a government subpoena, Microsoft forced the government to move to compel to access the content of certain customer emails); *In re Nat'l Sec. Letter*, 930 F. Supp. 2d 1064 (N.D. Cal. 2013) (electronic communication service provider petitioned under national security letter statute to set aside letter and associated gag order); *In re Google Inc.'s Petition to Set Aside Legal Process*, No. 13-80063 (N.D. Cal. 2013).

In 2012 the Supreme Court's holding in United States v. Jones, and Justice Sonia Sotomayor's concurrence in that case, signaled that it was starting to shift away from its third-party analysis.

16 *See, e.g.*, Nate Cardozo, Cindy Cohn, Parker Higgins, Kurt Opsahl & Rainey Reitman, Elec. Frontier Found., *Who Has Your Back? Protecting Your Data from Government Requests* 7, 8, 11 (May 15, 2014), https:// www.eff.org/files/2014/05/19/who-has-your-back-2014-govt-data-requests.pdf; see also *Twitter Inc. v. Holder*, 14-cv-4480, 2014 WL 5012514 (N.D. Cal. Oct. 7, 2014) (Twitter filed complaint seeking declaratory judgment that it can publish a transparency report containing information that has not been preapproved by government officials—including information on the "limited scope of U.S. government surveillance of Twitter user accounts"); AT &T Transparency Report (2014), http://about.att.com/content/dam/csr/PDFs/ATT _Transparency%20Report_July%202014.pdf ("[W]e require a search warrant or probable cause order before providing any stored content.").

17 *City of L.A. v. Patel*, No. 13-1175, 2015 WL 456252 *amicus brief supporting respondents filed* (U.S. Jan. 30, 2015).

18 *United States v. Davis*, No. 12-12928, 2014 WL 7503825 *amicus brief in support of neither party filed* (11th Cir. Nov. 17, 2014) ("[N]othing in [*Smith and Miller*] contemplated, much less required, a legal regime that forces individuals to choose between maintaining their privacy and participating in the emerging social, political, and economic world facilitated by the use of today's mobile devices or other location based services.").

19 *Riley*, 134 S. Ct. at 2484. The court also writes that "[n]ow it is the person who is not carrying a cell phone, with all that it contains, who is the exception." *Id.* at 2490.

20 See Marc Rotenberg & Alan Butler, *Symposium: In* Riley v. California, *a unanimous Supreme Court sets out Fourth Amendment for digital age*, ScotusBlog (June 26, 2014), http://www.scotusblog.com/2014/06/ symposium-in-riley-v-california-a-unanimous-supreme-court-sets-out-fourth-amendment-for-digitalage/.

21 *Riley*, 134 S. Ct. at 2491. Chief Justice Roberts describes cloud computing as "the capacity of Internetconnected 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. …Moreover, the same type of data may be stored locally on the device for one user and in the cloud for another." *Id.* (internal citation omitted).

22 *Id.*

23 *Id.*

24 *Id.* at 2493.

25 *Id.* at 2490, 2493; see, *e.g., Clapper*, 959 F. Supp. 2d at 749-52; *see also* Rotenberg & Butler, *supra* note 20.

Pillsbury Winthrop Shaw Pittman LLP