THE YALE LAW JOURNAL FORUM
September 11, 2014

Riley's Implications for Fourth Amendment Protection in the Cloud

Ryan Watzel

In June 2014, the Supreme Court unanimously held in *Riley v. California*[1] that the digital content of cell phones does not fall within the search-incident-to-arrest exception to the Fourth Amendment's prohibition against unreasonable searches. The Court provided a clear answer "to the question of what police must do before searching a cell phone seized incident to an arrest . . . —get a warrant."[2] The Court held that any data on a cell phone requires a warrant for police to access, regardless of whether that data is saved in the cloud—i.e., in online servers managed by a hosting company—or on the phone's internal hard drive.[3]

Riley's protection of cloud-based data for cell phone searches, however, does not address the broader question of whether information stored in the cloud is entitled to Fourth Amendment protection in other contexts. Indeed, the Court went out of its way to state that *Riley* did "not implicate the question [of] whether the collection or inspection of aggregated digital information amounts to a search under other circumstances."[4] The Court also distinguished the facts of *Riley* from those in *Smith v. Maryland*,[5] one of the principal cases to apply the so-called "third-party doctrine." The third-party doctrine, which provides that information voluntarily revealed to third parties is not protected by the Fourth Amendment, may pose the biggest obstacle to whether cloud-based data receives Fourth Amendment protection, since any data stored in the cloud is necessarily conveyed to third-party servers. Yet by sidestepping the third-party doctrine in *Riley*, the Court never had to address how the doctrine applies to private data stored across remote servers.

Nevertheless, while failing to explicitly afford Fourth Amendment protection to cloud-based data, *Riley* still provides the best evidence yet that the Court may be ready to reconsider the third-party doctrine and to recognize Fourth Amendment protection for personal data stored in the cloud.

1. 134 S. Ct. 2473 (2014). *Riley* was decided together with *United States v. Wurie*, another case

2. *Id.* at 2495.

3. *Id.* at 2491, 2493.

4. *Id.* at 2489 n.1.

5. 442 U.S. 735 (1979).

I. THE THIRD-PARTY DOCTRINE AND DIGITAL DATA

The third-party doctrine generally holds that a person has "no legitimate expectation of privacy in"—and therefore no Fourth Amendment protection of—"information he voluntarily turns over to third parties."[6] Its contours were shaped by the Supreme Court's decisions in *Smith* and *United States v. Miller*.[7] In *Smith*, the Court held that no warrant was required to use a pen register[8] at a telephone company to identify phone numbers dialed by a specific caller. According to the Court, callers do not have an "actual expectation of privacy in the numbers they dial," and even if they did, such an expectation would not be reasonable because telephone users "voluntarily convey[] numerical information to the telephone company" and "assume the risk" that the company will reveal to police the numbers they dial.[9]

Recently, however, some courts have distinguished *Smith* in the context of digital data by finding that such data is not "voluntarily" provided to third parties. For example, in *United States v. Warshak*, the Sixth Circuit found that email users have an expectation of privacy in emails saved by their internet service providers.[10] Earlier this year, the Eleventh Circuit in *United States v. Davis* held that cell phone users have an expectation of privacy in cell site location data.[11] Most significantly, Justice Sotomayor stated in her concurrence in *United States v. Jones* that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[12] *Smith*'s approach, according to Justice Sotomayor, "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."[13] Consequently, Justice Sotomayor advised that she "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."[14] Although the *Jones* majority did not reconsider the third-party doctrine in that case, Justice Sotomayor's concurrence questioning

6. *Id.* at 743-44.

7. 425 U.S. 435 (1976).

8. A pen register records the numbers dialed on a telephone by monitoring electrical impulses caused when the dial on the telephone is released. *Smith*, 442 U.S. at 736 n.1.

9. *Id.* at 744.

10. 631 F.3d 266 (6th Cir. 2010).

11. 754 F.3d 1205 (11th Cir. 2014). Cell site location data includes a record of calls made by a cell phone user and the cell towers that carried the call. This information allows police to extrapolate the location of the cell phone user at the time in the call record. *Id.* at 1210-11.

12. 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

13. *Id.*

14. *Id.*

the doctrine's applicability to digital data has become influential among judges,[15] scholars,[16] and even the Court itself.[17]

II. *RILEY*'S IMPLICATIONS FOR CLOUD-BASED DATA

Instead of directly addressing how the third-party doctrine applies to digital data, the Court in *Riley* distinguished the case's facts from those of *Smith*. In *Riley*, the government conceded that cell phones were different than pen registers, stating that "unlike a pen register, the search of a cell phone is a Fourth Amendment 'search,' because the owner has a property right in the phone entirely apart from any reasonable expectation of privacy in its contents."[18] Nevertheless, the government argued that "to the extent that the Court creates a novel exception to officers' otherwise-plenary authority to search items found on an arrestee because of special privacy concerns raised by cell phones, it would be incongruous to apply that holding to information on the phone in which an individual lacks any reasonable expectation of privacy"—in other words, information that had been voluntarily disclosed to a third party, such as call logs.[19] But the Court didn't bite. Because there was "no dispute here that the officers engaged in a search of Wurie's cell phone," all data stored on that phone was protected, at least inasmuch as police accessed the data from the phone itself.[20] The Court did not have to address *Smith*'s application to data stored in the cloud because the government conceded that "retriev[ing] files beyond those stored on the phone could not be justified as a search incident to arrest," which is "limited to the area within the arrestee's immediate control."[21]

Riley thus does little to clarify how the third-party doctrine applies to information stored in the cloud in other contexts, leaving open the question of whether police can acquire cloud-based information from third parties who host the cloud servers. For example, if an iPhone owner backs up her personal data such as email, contacts, calendars, internet history, notes, photos, and

---

15. *See, e.g.*, *In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 623-24 (5th Cir. 2013) (Dennis, J., dissenting).

16. *See, e.g.*, Miriam H. Baer, *Secrecy, Intimacy, and Workable Rules: Justice Sotomayor Stakes Out the Middle Ground in* United States v. Jones, 123 YALE L.J. F. 393 (2014), http://www.yalelawjournal.org/forum/secrecy-intimacy-and-workable-rules [http://perma.cc/VN3Q-B4RG].

17. *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2490 (2014) (citing *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring)).

18. Brief for the United States at 54, Riley v. California, 134 S. Ct. 2473 (2014) (No. 13-212).

19. *Id.* at 55.

20. *Riley*, 134 S. Ct. at 2492-93.

21. Brief for the United States, *supra* note 18, at 43-44.

documents on Apple's iCloud,[22] police would be unable to access that data in a search of the iPhone incident to arrest under *Riley*. But could police acquire the cloud-based data from Apple without a warrant by arguing that the owner, after disclosing the data to Apple via the cloud, no longer had a reasonable expectation of privacy to it under the third-party doctrine?

On its face, *Smith* suggests that this argument would probably succeed. Users of iCloud "know that they must convey" the information that they intend to back up on iCloud to Apple and that such information is in fact recorded on Apple's servers.[23] Furthermore, iCloud users "voluntarily convey" this information to Apple by initially setting up their iCloud accounts, even if they do not keep track of which specific documents are being saved to the cloud.[24] Thus, users may "assume[] the risk that the company would reveal to police" information saved on its servers.[25] As a result, it is unlikely that iCloud users have a strong claim to a reasonable expectation of privacy under *Smith*'s rationale alone.[26]

Yet *Riley*, despite distinguishing *Smith*, suggested that cloud-based data nevertheless may enjoy some Fourth Amendment protection. First, the Court emphasized the intrusiveness of police access to cloud-based data. It analogized allowing police to search cloud-based data on a cell phone during an arrest to "finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house."[27] If the key is the cell phone in this analogy, then cloud-based storage is presumably the house. The Court recognized that accessing data in the cloud can often be more intrusive than accessing data on a phone's internal storage because of the cloud's ability to hold virtually unlimited amounts of data.

Second, the Court suggested that privacy is compatible with certain data stored online. When describing how cell phone data is qualitatively different

---

22. iCloud, like other cloud storage and computing, has continued to grow. More than 250 million people worldwide now use the service. *See* Mikey Campbell, *Apple Sees 2 Billion iMessages Sent Daily from Half a Billion iOS Devices*, APPLEINSIDER (Jan. 23, 2013), http://appleinsider.com/articles/13/01/23/apple-sees-2b-imessages-sent-every-day-from-half-a-billion-ios-devices [http://perma.cc/C6LZ-F5PD].

23. Smith v. Maryland, 442 U.S. 735, 743 (1979).

24. *Id.* at 744.

25. *Id.*

26. User agreements may also extinguish reasonable expectations of privacy, *see* United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010), but that would likely not apply to iCloud. According to Apple's Privacy Policy, the company can collect users' names, addresses, phone numbers, and email addresses, but the policy does not give Apple permission to collect other stored information like email contents or photos. *Privacy Policy*, APPLE, http://www.apple.com/legal/privacy/en-ww [http://perma.cc/NFM2-YAG9] (last visited Aug. 30, 2014).

27. Riley v. California, 134 S. Ct. 2473, 2491 (2014).

from physical records, the Court explained that "[a]n Internet search and browsing history . . . can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD."[28] An individual's "private interests or concerns" may therefore remain private despite being accessible by a third-party internet provider. It seems unlikely that the Court would conclude that online data containing an individual's "private interests or concerns" is nevertheless entitled to no "legitimate expectation of privacy."[29]

Third, the Court suggested that the precise medium in which digital data is stored is irrelevant to whether that data receives Fourth Amendment protection. The Court observed that "the same type of data may be stored locally on the device for one user and in the cloud for another."[30] And in perhaps *Riley*'s most significant moment for cloud-based data, the Court explained that "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*."[31] Whether it makes little difference because personal data stored on the cloud categorically enjoys the same protection as locally-saved data, or because the act of searching a cell phone without a warrant violates the Fourth Amendment regardless of where its content is located, the Court did not say. But the Court's apprehension about police access to the wide array of private information found on cell phones without a warrant, and its contention that it "makes little difference" whether such data is stored in the cloud, seem to be irreconcilable with a conclusion that cloud-based data receives no Fourth Amendment protection.

III. BEYOND *RILEY*: THE CONSEQUENCES OF PROTECTING CLOUD-BASED DATA

The Court in *Riley* had good reasons to defer the issue of Fourth Amendment protection for cloud-based data to another day. Cloud computing presents an array of additional questions outside the scope of *Riley*. For instance, what type of user agreements would waive an expectation of privacy? What type of third-party use would eliminate an expectation of privacy

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

29. *Smith*, 442 U.S. at 744.

30. *Riley*, 134 S. Ct. at 2491.

31. *Id.* (emphasis added).

notwithstanding a user agreement? Does it matter whether a cloud service acts as a recipient of information rather than simply a conduit for it?[32]

Holding that cloud-based data receives Fourth Amendment protection would also cast serious doubt on the constitutionality of the Stored Communications Act ("SCA"), which allows the government to obtain via subpoena, as opposed to warrant, "stored wire and electronic communications and transactional records" that have been in storage for more than 180 days.[33] In fact, the Sixth Circuit recently declared part of the SCA unconstitutional on precisely such Fourth Amendment grounds.[34] Since there are currently bills in Congress that propose amending the SCA,[35] the Court may be reluctant to address the issue and invalidate parts of the statute until Congress amends it.

Finally, while the *Riley* Court correctly noted that cell phones are utilizing cloud computing "with increasing frequency,"[36] the entire concept of local data storage may soon become anachronistic. In Apple's most recent operating system, for example, any application that is compatible with iCloud, including Apple's basic text editing program, uses the cloud as its default save location.[37] (One prolific Mac blogger noted that "saving [a] file anywhere else [besides iCloud] has become somewhat of a chore."[38]) Cloud computing more broadly has also begun to replace local computing in various industries through Software-, Platform-, and Infrastructure-as-a-Service, whereby companies subscribe to or create their own applications for exclusive cloud-based use.

The decision of when to address the issue of cloud-based data thus presents a tradeoff. On the one hand, as the cloud becomes more omnipresent and unavoidable, cloud usage may cease to constitute a "voluntary" disclosure within *Smith*'s third-party doctrine framework. If the Court waits to address the issue until cloud computing becomes integrated into everyday use, then it

---

32. For a debate on these third-party issues, see Orin Kerr and Greg Nojeim, *The Data Question: Should the Third-Party Records Doctrine Be Revisited?*, A.B.A. J. (Aug. 1, 2012), http://www.abajournal.com/magazine/article/the_data_question_should_the_third-party_records_doctrine_be_revisited [http://perma.cc/9MHV-HJPR].

33. 18 U.S.C. § 2703 (2012).

34. United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

35. *See, e.g.*, Email Privacy Act, H.R. 1852, 113th Cong. (2013). *See generally* Matthew Sipe, *Storage Wars: Greater Protection for Messages in Memory*, 124 YALE L.J. F. 29 (2014), http://www.yalelawjournal.org/forum/storage-wars-greater-protection-for-messages-in-memory [http://perma.cc/5E8P-ZXXN] (describing proposed amendments to the SCA).

36. *Riley*, 134 S. Ct. at 2491.

37. Rob LeFebvre, *Mastering iCloud on Your Mac: Dump iCloud as Default Save Location*, CULT OF MAC (Mar. 26, 2013, 6:00 AM), http://www.cultofmac.com/220906/mastering-icloud-on-your-mac-dump-icloud-default-save-os-x-tips [http://perma.cc/DGH3-SENP].

38. Michael Steeber, *Change Mountain Lion's Save Default Away from iCloud*, CULT OF MAC (Sept. 5, 2012, 4:08 PM), http://www.cultofmac.com/188717/change-mountain-lions-save-default-away-from-icloud-video-how-to [http://perma.cc/S6X9-NY67].

may be able to find Fourth Amendment protection for cloud-based data without overruling or reinterpreting *Smith*. On the other hand, developing industries and consumers relying on the cloud currently have little guidance about what Fourth Amendment protection they can expect for their data.

Conclusion

Riley suggests that the Court is ready to find that cloud-based data receives Fourth Amendment protection, and that cloud users do not waive a reasonable expectation of privacy in every file they save simply because storage is moving to the cloud. The cloud is, to use the Court's language in *Smith*, "merely the modern counterpart"[39] of internal hard drives and processors that locally store and compute data. Nevertheless, competing concerns—such as the desire to avoid raising the constitutionality of the SCA's 180-day rule and to delay deciding at what point cloud usage has ceased to be voluntary for purposes of the third-party doctrine—may render the Court reluctant, at least for now, to make explicit *Riley*'s implications for data in the cloud.

Ryan Watzel is a law clerk for Hon. Christopher F. Droney on the United States Court of Appeals for the Second Circuit. *He would like to thank Bert Ma and the* Yale Law Journal *for excellent edits and feedback.*

Preferred Citation: Ryan Watzel, Riley*'s Implications for Fourth Amendment Protection in the Cloud*, 124 YALE L.J. F. 73 (2014), http://www.yalelawjournal.org/forum/rileys-implications-in-the-cloud.

39. Smith v. Maryland, 442 U.S. 735, 744 (1979).