THE LIFE OF RILEY (*V. CALIFORNIA*)

Paul Ohm[*]

I. INTRODUCTION

In *Riley v. California*, the landmark ruling from 2014, the U.S. Supreme Court held that the search incident to valid arrest exception to the Fourth Amendment's warrant requirement did not extend to a police search of the contents of information stored on cell phones found in the pockets of arrestees.[1] This case has been rightly hailed as a significant milestone in constitutional criminal procedure.[2] Prior to *Riley*, several lower courts had allowed the warrantless search of electronic devices at the scene of an arrest, drawing analogies between cell phones and pre-digital artifacts such as diaries, little black books, and the crumpled up cigarette pack the police were allowed to search in *United States v. Robinson*.[3] After *Riley*, analogies like these can no longer stand up to constitutional scrutiny.[4]

---

* Professor, Georgetown University Law Center, and Faculty Director, Center on Privacy and Technology. Thanks to the organizers and participants of the Texas Tech School of Law Criminal Law Symposium and, in particular, to the inimitable and unstoppable Arnold Loewy. Thanks also to Princeton University's Center on Information Technology Policy and Program in Law and Public Affairs and, in particular, to Jonathan Hafetz, Ed Felten, Kim Lane Scheppele, and Andrea Matwyshyn. Thanks also to Fred Bloom and Pierre Schlag.

1. Riley v. California, 134 S. Ct. 2473, 2493–94 (2014).

2. *E.g.*, Richard M. Re, *Symposium*, *Inaugurating the Digital Fourth Amendment*, SCOTUSBLOG (June 26, 2014, 12:37 PM), http://www.scotusblog.com/2014/06/symposium-inaugurating-the-digital-fourth-amendment/ ("[P]rivacy specialists will be celebrating [*Riley*] for a long time."); *see also Riley v. California*, SCOTUSBLOG, http://www.scotusblog.com/case-files/cases/riley-v-california/ (last visited Nov. 1, 2015) (providing similar commentary and additional inks to symposium posts).

3. United States v. Robinson, 414 U.S. 218, 223 (1973); United States v. Finley, 477 F.3d 250, 260 (5th Cir. 2007) (cell phone); United States v. Hill, No. CR 10-00261JSW, 2011 WL 90130, at *2 (N.D. Cal. Jan. 10, 2011) (iPhone photos); People v. Diaz, 244 P.3d 501, 502–03 (Cal. 2011) (cell phone).

4. *Riley*, 134 S. Ct. at 2493 ("[A] warrant is generally required before such a search, even when a cell phone is seized incident to arrest.").

Riley does much more than establish this relatively narrow holding. The Court could have focused only on the failure of the analogies, recited some facts and figures about the amount of information stored on smartphones, and reiterated the observation that Fourth Amendment cases tend to be fact-intensive ones. Instead, Chief Justice Roberts, writing for at least eight members of the Court, wrote a paean to privacy in the modern, technological era.[5]

The Chief Justice wrote a privacy opinion for the ages. He laced his opinion with small gems of privacy wisdom, many not strictly necessary for the decision. These gems are sure to be cited by advocates immediately, and some lower courts will use them to encourage and justify privacy-enhancing holdings. These quotes will have, in other words, a life of their own.

In this Article, I collect and explore some of these passages. My goal is not to divine why the Chief Justice chose to write the opinion this way, much less why his seven colleagues chose to join him. Instead, my goal is to point out the perhaps surprising contexts in which these quotes will have a life of their own. This Article is an exercise in prediction and description, not prescription.

To investigate this narrowly focused question, I am using a decidedly unorthodox mode of presentation.[6] What follows are a series of hypothetical judicial (and some administrative) opinions from the future, presented *seriatim*, without complete context and with virtually no commentary.[7] Think of this as a chapter from a casebook to be published in 2025, one tracing the expansive and diverse "life of *Riley*."[8]

The Article organizes these hypothetical opinion snippets by topic. Some of these topics are legal questions courts have had to answer in recent years. Other topics center on specific quotes from *Riley* that I predict will have a life of their own.

---

5. Justice Alito, the lone member of the Court who did not join the Chief Justice's opinion and instead wrote a concurring opinion, did not disagree with any of the fundamental points made by the other eight. *Id.* at 2495 (Alito, J., concurring). Justice Alito also demonstrated in his concurrence in *United States v. Jones* that he was willing to embrace broad and aggressively pro-privacy arguments in a very similar context. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Alito, J., concurring). Indeed, it is the silent concurrences of Justices Scalia, Thomas, and Kennedy, as well as the authorship by the Chief Justice that I find most surprising after *Jones*.

6. This mode of presentation pays homage to the classic law review article by Lon L. Fuller, *The Case of the Speluncean Explorers*, 62 HARV. L. REV. 616 (1949).

7. This Article uses an unorthodox mode of citation, too. In the "judicial opinions" that follow, I will follow the citation conventions used by judges in their opinions, most importantly by utilizing in-text citations. *See generally* THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION (Columbia Law Review Ass'n et al. eds. 20th ed., 2015) (providing conventions for citations in court documents).

8. With apologies to the creators and fans of the radio and television shows that inspired the title. *The Life of Riley* (NBC television broadcast 1953–1958); *The Life of Riley* (NBC television broadcast 1949–1950).

II. LOCATION INFORMATION

Targaryen v. United States
(U.S. Supreme Court 2018)

We hold that the police must obtain a warrant, signed by a judge and backed by probable cause, when they use any technology that tracks the precise location of a person, regardless of the technology used; the role of a third party in the collection, storage, or processing of the information; and the amount of location information tracked.

We thus reverse lower court opinions that have upheld the warrantless use of cell phone tracking. *United States v. Skinner*, 690 F.3d 772, 778 (6th Cir. 2012) ("While the cell site information aided the police in determining Skinner's location, that same information could have been obtained through visual surveillance."); *In re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600, 615 (5th Cir. 2013) ("We understand that cell phone users may reasonably want their location information to remain private, just as they may want their trash, placed curbside in opaque bags, or the view of their property from 400 feet above the ground to remain so." (citations omitted)).

As we said recently in *Riley v. California*, "Historic location information is a standard feature on many smartphones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building." 134 S. Ct. 2473, 2490 (2014). In that opinion, we also quoted the concurring opinion of Justice Sotomayor in *United States v. Jones* that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Id.* (quoting *United States v. Jones*, 132 S. Ct. 945, 955 (2012) (Sotomayor, J, concurring)). It is because of this impact on privacy that we hold that the targets of police tracking enjoy a reasonable expectation of privacy in their location and movement.

III. THE MOSAIC THEORY

United States v. Baratheon
(4th Cir. 2021)

We decline suggestions to draw a line of privacy based on the quantity of location information obtained, what some have called the "Mosaic Theory" of the Fourth Amendment. *United States v. Maynard*, 615 F.3d 544, 562 (D.C. Cir. 2010), *aff'd sub nom. United States v. Jones*, 132 S. Ct. 945 (2012); Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 311 (2012). There are multiple problems with the Mosaic

Theory. As with any line-drawing exercise, there may be easy cases at the extremes, but in the zone where the line is drawn, it is hard to justify why one quantity of surveillance requires a warrant but a little less surveillance does not. Kerr, *supra* at 333. This inherent fuzziness defeats the goal of giving police clear guidance. Consider Justice Alito's suggestion, joined by three other Justices, that even though he could not at that time identify "the point at which the tracking of [a] vehicle became a search," it was clear to him that "the line was surely crossed before the 4-week mark." *Jones*, 132 S. Ct. at 964 (Alito, J., concurring).

But much more importantly than these pragmatic, operational concerns, the recent opinion in *Riley v. California* suggests that when it comes to the privacy of sensitive digital information, the Supreme Court seems inclined to find significant privacy interests in minimal amounts of information. 134 S. Ct. 2473, 2477 (2014). Although the Court focused on the quantity of private information throughout the opinion, the Court refused to draw lines based on quantity. The companion case to *Riley*, *United States v. Wurie*, involved a simple "flip phone," one in which the police pressed two buttons and did no more. *Id.* at 2481.

Wurie's flip phone was not capable of many, and maybe not even most, of the types of sensitive information handling that the Court focused on in explaining the privacy of a smartphone. Yet the Court refused to draw a line based on this type of quantity. *Id.* at 2492–93. The police in *Wurie* took almost the minimum number of steps one could imagine the police taking in the investigation of a digital device. Yet the Court refused to draw a line based on this type of quantity too. *Id.* (rejecting the "suggestion that officers should always be able to search a phone's call log, as they did in Wurie's case"). The Supreme Court's message is clear. The Mosaic Theory is dead. If information crosses a threshold of sensitivity, then any intrusion into it, even a minimal one, triggers constitutional privacy protections. In *Riley*, the Court embraced this approach in the search incident to valid arrest context, but because it was premised on the privacy we deserve in the kind of information of smartphones, we apply the same reasoning to whether Defendant had an expectation of privacy in location information. Even a single "ping" on a cell tower is enough to trigger the warrant requirement. Because the police in this case obtained more than a dozen pings without a warrant, the location information will not be admissible in evidence.

IV. EXTENDING THE HOME

United States v. Clegane
(3d Cir. 2019)

In *Riley v. California*, the Supreme Court noted a shift in the balance of privacy, which has placed some of our most intimate secrets no longer in our

bedrooms but instead in our pockets. 134 S. Ct. 2473, 2477 (2014). "[A] cell phone search would typically expose to the government far *more* than the most exhaustive search of a house." *Id.* at 2491. The myriad technological revolutions that brought the world to that conclusion by the time the Court wrote these words have only accelerated, and a mere five years later few reasonable people today would doubt them. A new touchstone of the Fourth Amendment is that a police search of an individual's digital information requires at least as much constitutional protection as the search of the individual's bedroom. Because the police in this case searched through Defendant's hard drive without a warrant, we suppress the information obtained, just as we would the information obtained from a warrantless search of a bedroom closet or dresser drawer.

United States v. Greyjoy
(C.D. Cal. 2018)

Riley v. California recognized that "a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house." 134 S. Ct. 2473, 2491 (2014). Today, we extend that analogy, recognizing other ways in which the data stored in the cloud and on our devices is like the most protected sphere of privacy within the Fourth Amendment. For one thing, the home enjoys protection not only within its four walls but also in a space just beyond—the idea of a constitutionally protected "curtilage." *Oliver v. United States*, 466 U.S. 170, 182 n.12 (1984). Reasoning by analogy, we hold today that smartphones and other connected devices (sometimes called part of the "Internet of Things") so too have a "virtual curtilage," which protects them beyond the closed container of the device's on-board memory. Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CAL. L. REV. (forthcoming 2016), http://papers.ssrn.com/sol3/papers.cfm?abstract_id= 2577944. In this case, the police erred by using a wireless sniffer to track the information emanating from Defendant's automobile's diagnostic system, thereby intruding into that virtual curtilage.

V. THE THIRD-PARTY DOCTRINE

United States v. Lannister
(7th Cir. 2018)

We believe the Supreme Court will some day reverse *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Miller*, 425 U.S. 435 (1976), and remove from the Fourth Amendment the concept of a third-party doctrine. Justice Sotomayor came close to calling for this change in *United States v. Jones*, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring), in an

opinion cited favorably by seven of her colleagues in *Riley v. California*, 134 S. Ct. 2473, 2491 (2014). It is not our place, of course, to call the death of this patient before the surgeons in the high court have had their say. We are more than comfortable, however, trying to anticipate this result by recognizing the narrow and necessary preconditions of *Smith* and *Miller*, which simply do not apply in this case. The sensitive health data obtained from Defendant's fitness tracker are different in both degree and kind from the numbers dialed in *Smith* and the bank transactions in *Miller*, so the police violated the Fourth Amendment rights of the accused by obtaining it without probable cause and without notice to the owner of that information. Telephone companies use telephone numbers to route phone calls and banks use transaction information to direct the transfer of money. Fitness tracker companies simply do not sit in relation to the health data of its customers in the same way, notwithstanding the Government's attempts to highlight the many ways in which the fitness tracker company may hypothetically try to monetize this information. The information shall be suppressed along with all information obtained as "fruit of the poisonous tree."

VI. GOVERNMENT AGENCY PROTOCOLS

In re Order to Obtain Information from Certain Telephone Companies
(FISC 2017) (secret until leaked to the public in 2022)

Even though the Government's minimization protocols complied with the bare requirements of the Foreign Intelligence Surveillance Act (FISA), we nonetheless must also measure it under the requirements of the Constitution. We hold that under the Fourth Amendment's prohibition against unreasonable searches and seizures, it is not enough for the government to use filters and search queries to "minimize" the data it has obtained because the underlying data can be re-filtered or re-searched in the future to learn more. In the meantime, this data (to which the Government concedes it is not entitled to search) lies in wait, like a ticking time bomb of rights invasion. It is no matter that the Government presents us hundreds of pages outlining the myriad and complex data security and auditing protocols it promises to follow, because "the Founders did not fight a revolution to gain the right to government agency protocols." *Riley v. California,* 134 S. Ct. 2473, 2491 (2014).

United States v. Stark
(6th Cir. 2018)

In *United States v. Ganias*, 755 F.3d 125, 128 (2d Cir. 2014), the Second Circuit suppressed the Government's use of information stored on a hard drive seized pursuant to a search warrant but outside the scope of the warrant.

In *Ganias*, law enforcement officers searched the hard drive three years after the original seizure in a different (but related) investigation from the one that supported the original warrant. *See also United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1171 (9th Cir. 2010) (en banc) (suggesting that information outside the scope of the warrant seized while intermingled on a hard drive cannot be retained).

We follow these cases and today suppress the evidence found on Defendant's hard drive that exceeded the scope of the original warrant. As the Supreme Court recognized in *Riley v. California*, the information we all store on our digital devices "hold for many Americans 'the privacies of life.'" 134 S. Ct. 2473, 2494–95 (2014) (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)). We do not see any meaningful differences between the cell phones (including mere flip phones) at issue in that case and the laptops seized and searched in this case. In fact, the 16 gigabytes of memory available in the "current top-selling smart phone" is an order of magnitude smaller than the 500-gigabyte hard drives at issue in this case. *Id.* at 2489. And people tend to keep laptops for many years, amassing information on it all the while, unlike the way they seem to replace their phones every year or two.

Finally, even though we are convinced from the expert testimony that the FBI strictly adhered to its own practices and procedures, and even though external experts have validated these practices and procedures as state-of-the-art technology, still the Constitution requires more. "[T]he Founders did not fight a revolution to gain the right to government agency protocols." *Id*. at 2491.

VII. ANALOGIES

In re Order to Obtain Information from Certain Telephone Companies
(FISC 2017) (secret until leaked to the public in 2022)

The Government analogizes the web browsing data it has collected in this case to the records it routinely obtains from libraries and bookstores. "That is like saying a ride on horseback is materially indistinguishable from a flight to the moon." *Riley v. California,* 134 S. Ct. 2473, 2488 (2014).

United States v. Mormont
(5th Cir. 2017)

The Government's attempts to analogize precedents involving the border search of luggage and pockets to the exhaustive border search of Defendant's laptop "is like saying a ride on horseback is materially indistinguishable from a flight to the moon." *Riley v. California,* 134 S. Ct. 2473, 2488 (2014).

United States v. Snow
(E.D. Tenn. 2018)

Arguing that decryption is no different than the translation of a foreign language "is like saying a ride on horseback is materially indistinguishable from a flight to the moon." *Riley v. California,* 134 S. Ct. 2473, 2488 (2014). We hold that the FBI was obligated to obtain a search warrant before it attempted to decrypt the encrypted partition on Defendant's seized laptop.

State v. Baelish
(N.J. 2018)

The State argues that it should be permitted to obtain from Defendant's wireless phone provider the precise location of her phone every six minutes for the past thirty-two days because this is no different than the type of information it could have obtained by assigning 24/7 physical surveillance of her whereabouts. This "is like saying a ride on horseback is materially indistinguishable from a flight to the moon." *Riley v. California*, 134 S. Ct. 2473, 2488 (2014).

VIII. PRIVACY COMES AT A COST

United States v. Martell
(9th Cir. 2016)

In embracing the concurring opinion in *Comprehensive Drug Testing* and holding that search warrants for computers must specify a detailed search protocol restraining the actions of the executing officer, we recognize that this will slow the process with which modern criminal cases are investigated and prosecuted. *See United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1178–83 (2010) (Kozinski, J., concurring). In some instances, we expect that our ruling today will cause cases to be lost. "Privacy," the Supreme Court reminds us, "comes at a cost." *Riley v. California*, 134 S. Ct. 2473, 2493 (2014).

State v. Drogo
(Wash. 2019)

We thus follow the lead of the United States Sixth Circuit Court of Appeals and extend the full protection of the federal and state constitutional protections against unreasonable searches to the contents of email messages stored by an email provider, irrespective of whether those messages are opened or unopened or have retired in due course. We are mindful of the impact this ruling may have on the police and view this as an unavoidable

cost of recognizing the People's fundamental liberties. *Riley v. California,* 134 S. Ct. 2473, 2493 (2014) ("Privacy comes at a cost.").

Statement of the Federal Trade Commission
In re Westeros, Inc.
File No. 200-1337
(July 27, 2022)

We turn next to the question of unfairness. Under our 1980 Policy Statement on Unfairness, "[t]o justify a finding of unfairness the injury must satisfy three tests. It must be substantial; it must not be outweighed by any countervailing benefits to consumers or competition that the practice produces; and it must be an injury that consumers themselves could not reasonably have avoided." FTC Policy Statement on Unfairness, Fed. Trade Commission (Dec. 17, 1980), https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness. At the time we wrote this, the harm most often visited upon consumers tended to involve "monetary harm, as when sellers coerce consumers into purchasing unwanted goods or services." *Id.* Today, changes in society—many brought about by shifts in technology—have shifted considerably the types of harm consumers suffer and concomitantly, the kind of harm we intend to redress through our congressionally authorized powers in § 5. With this case, the Commission announces a clarification of our 1980 policy, recognizing that consumers deserve protection from harm that is concrete and substantial, even if nonmonetary. In particular, we recognize as cognizable within § 5 unfairness the kind of privacy harm inflicted by the company in this case.

. . . .

The accused company complains that any injury its mobile app may have caused was "substantially outweighed" by the "dramatic efficiencies" the app provided. Brief at 14 (cataloging jobs created and investor returns realized). The accused seems to suggest that *any* benefit justifies significant injury, but the statute and our Policy Statement make plain that we are expected to weigh and balance; the accused company recognizes that even the most wondrous innovations of Silicon Valley are illegal if they cause too much injury. And while we are not eager to enjoin from existence a job-creating and returns-generating product, it is important to remember that, as the Supreme Court has recently made clear: "Privacy comes at a cost." *Riley v. California,* 134 S. Ct. 2473, 2493 (2014).

IX. CONCLUSION

Riley v. California is not the only recent pronouncement from the Supreme Court embracing a new vision of the Fourth Amendment in a

technological age, but it is the most important.[9] By issuing an opinion that went far beyond what was needed to be said to support the holding, the Court will influence debates far beyond the usual impact of a Supreme Court opinion. Riley's life will be long and varied. Whether the broad and sweeping privacy pronouncements in *Riley* become prophetic or instead get whittled down and narrowed remains to be seen. But it represents a pivotal moment, one to watch closely.

9. *See* United States v. Jones, 132 S. Ct. 945, 954 (2012) (Sotomayor, J., concurring); *id.* at 957 (Alito J., concurring); Kyllo v. United States, 533 U.S. 27 (2001).