What Would a Martian Think of Cell Phones? The Third-Party Doctrine and Technological Extensions of the Human Self

*Joshua Vittor**

When former National Security Agency (NSA) analyst Edward Snowden publicized the fact that the U.S. government had been systematically spying on the cell phone usage of millions of Americans for many years, the news was naturally met with its fair share of attention and outrage.[1] The right to privacy, particularly with respect to government intervention, is by no means a new concern.[2] The Snowden revelations struck a particularly sensitive nerve by highlighting the inextricable tension between the increasing capacity of information technology and the correspondingly increased capacity to surveil that information. One might assume that as technology evolved, the legal principles that safeguard individuals from the increasing pervasiveness of that technology would have evolved as well. Such an evolution never occurred. The resultant gap between technology and outdated legal privacy protections is the problem this paper seeks to address. The paper focuses on cell phones—as did the surveillance programs that Snowden unearthed—for good reason. Cell phones have become digital simulacrums of our day-to-day lives, and the legal safeguards that protect our *physical* privacy have not yet been updated to encompass the increasingly large digital space in which we all live.

After the Snowden leaks, per the natural course of the universe, lawsuits ensued. These cases contested the legality of the telephony metadata surveillance program, attacking it on both statutory and constitutional grounds.[3] In one such case, *Klayman v. Obama*, Judge Richard Leon de-

* Harvard Law School, J.D. expected 2016. There are many people whose efforts contributed immensely to this piece, and to whom I am greatly appreciative. Professor Susan Crawford and the students of the Fall 2014 Law of Surveillance seminar deserve an initial acknowledgement because without them I would have never been driven to interrogate the conflict between privacy and technology. Professor Crawford was particularly vital during the paper's infancy, urging me to explore further the connection to personhood. Thanks as well to former *Harvard Law & Policy Review* colleague Rebecca Lipman, whose scholarly insights also helped shape my own. I am particularly grateful to the *Harvard Law & Policy Review* for this opportunity, and to the journal's tireless editors who improved the paper by orders of magnitude. Any errors that do remain are entirely my own.

[1] *See, e.g.*, Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [http://perma.cc/2QY7-ZN2N].

[2] *See, e.g.*, Bruce Schneier, *The Eternal Value of Privacy*, WIRED (May 18, 2006), http://archive.wired.com/politics/security/commentary/securitymatters/2006/05/70886 [http://perma.cc/6KLV-MMS7].

[3] This program, secret prior to the Snowden leak, authorized the NSA to collect, in bulk, the metadata (dates, times, and phone numbers) of phone calls on U.S. soil. *See* Greenwald, *supra* note 1. Section 215 of the USA PATRIOT Act ("Section 215"), which allows for the

clared, for the first time, that the program was likely unconstitutional.[4] Those concerned with the privacy implications of technology and surveillance viewed *Klayman I* as a major triumph.[5] But it was a short-lived victory. Less than two years later, the D.C. Circuit vacated the *Klayman I* decision on procedural grounds, without reaching the ultimate constitutional question.[6]

Klayman I is indicative of a growing crisis in the United States surrounding the tension between technology and personal privacy. As technology advances, the ability to protect personal privacy naturally shrinks. This is a tradeoff that society is often quite comfortable with—we gladly sacrifice, for example, the data that companies like Google mine about our search histories in exchange for the ability to obtain information quickly on the Internet.[7] But sometimes technology intrudes too far, threatening our sense of privacy and freedom, core aspects of our individuality.[8] As cases like *Klayman I* make plain, technology has the simultaneous power to conveniently provide and freely disseminate information, without much regard for whether that information is private. The Snowden news highlighted one particularly alarming example of this dichotomy: cell phones and law enforcement's ability to monitor their use against individual citizens.

---

collection of "tangible things" in support of an investigation into international terrorism, provided the statutory authorization for the program (or so the government has argued). USA PATRIOT Act, Pub. L. No. 107–56, § 215, 115 Stat. 272 (2001).

[4] Klayman v. Obama (*Klayman I*), 957 F. Supp. 2d 1, 41 (D.D.C. 2013). In May 2015 the Second Circuit also struck down the metadata program, but it did so on statutory rather than constitutional grounds. *See* Am. Civil Liberties Union v. Clapper, 785 F.3d 787, 810 (2d Cir. 2015) (holding that Section 215 did not authorize the NSA telephony metadata program on statutory interpretation grounds). *Klayman I* is still the only ruling on the Fourth Amendment issue, though the question was rendered somewhat academic when the Section 215 sunset clause was triggered in June 2015. *See, e.g.*, Orin Kerr, *Second Circuit Rules, Mostly Symbolically, That Current Text of Section 215 Doesn't Authorize Bulk Surveillance*, VOLOKH CONSPIRACY (May 7, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/05/07/second-circuit-rules-mostly-symbolically-that-current-text-of-section-215-doesnt-authorize-bulk-surveillance/ [http://perma.cc/KTA6-CW95].

[5] *See, e.g.*, Joe Mullin, *Updated: Federal Judge Finds NSA Phone Spying Likely Unconstitutional*, ARS TECHNICA (Dec. 16, 2013), http://arstechnica.com/tech-policy/2013/12/federal-judge-finds-nsa-spying-unconstitutional [http://perma.cc/RZN5-Z3FW].

[6] Obama v. Klayman (*Klayman II*), 800 F.3d 559, 561 (D.C. Cir. 2015) (per curiam); *see also* Benjamin Wittes, *Standing Confusion in* Obama v. Klayman, LAWFARE (Aug. 31, 2015), https://www.lawfareblog.com/standing-confusion-obama-v-klayman [http://perma.cc/7F7Q-BATJ] ("The D.C. Circuit has spoken in *Obama v. Klayman* . . . and has announced its refusal to speak on the subject."). The D.C. Circuit held that plaintiffs had failed to sufficiently prove that *their* phones had been targets of the government's surveillance program and therefore didn't have standing to obtain a preliminary injunction. *See Klayman II*, 800 F.3d at 562 (Brown, J.). The Court offered no opinion on the constitutional question: whether such warrantless surveillance would be constitutional *had* the plaintiffs proven that their phones were included.

[7] *See* Joel Stein, *Data Mining: How Companies Now Know Everything About You*, TIME (Mar. 10, 2011), http://content.time.com/time/magazine/article/0,9171,2058205,00.html [http://perma.cc/9KT8-NFPA].

[8] Continuing on the theme of data mining, Google was sued over its (now discontinued) practice of scanning student emails for advertising purposes. *See* Doug Miller, *Google Data Mining Changes: Privacy Reform Needed*, INFORMATION WEEK (May 8, 2014), http://www.informationweek.com/strategic-cio/executive-insights-and-innovation/google-data-mining-changes-privacy-reform-needed/d/d-id/1251116 [http://perma.cc/JTF9-2TUC].

As Judge Leon's opinion in *Klayman I* makes clear, the law simply has not caught up to technology. The antiquated (yet still surviving) legal framework for categorizing information as private, for the purposes of exempting it from legal surveillance, focused on the relationship between information and its dissemination to third parties. This is an outdated and dangerous approach in the face of advancing technology, and *Klayman I* set a worthy example by refusing to apply it.[9] This paper presents an alternative approach, using cell phones as a proxy for technology more broadly: it is the closeness of our relationships with the devices that contain and convey information about us that should matter from a legal perspective, as opposed to the mere fact that those devices act as conveyors.

Some doctrinal background is necessary here. The government's primary constitutional defense of its surveillance program in *Klayman I* is indicative of the massive implications of cases like it for the intersection between advancing technology and shrinking personal privacy. One might expect the high-tech, Brave New World-esque surveillance program under review to warrant a similarly groundbreaking, modern legal defense. Instead, the government's justification for the surveillance program hinges upon a Supreme Court decision from 1979. That case, *Smith v. Maryland*,[10] and the so-called third-party doctrine it created, serve as the primary (and, prior to *Klayman I*, impenetrable) constitutional defense for the telephony metadata surveillance program.

In *Smith*, the Court declared that individuals who voluntarily provide information to a third party cease to have a "legitimate expectation of privacy" and are therefore unprotected by the Fourth Amendment from warrantless search and seizure.[11] The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[12] Simply put, the Fourth Amendment demands that the government obtain a warrant, issued upon probable cause, prior to conducting a search of an individual.[13] But what qualifies as a *search*, let alone a *reasonable* one, has been fodder for legal and academic debate for centuries. Since the seminal 1967 decision in *Katz v. United States*, the touchstone for Fourth Amendment protection has been personal privacy—or the "reasonable expectation" thereof.[14] After *Smith*, searches pursuant to information voluntarily divulged to third parties are considered per se reasonable under the Fourth Amendment.

Defenders of government surveillance have successfully ported the *Smith* ruling to the modern world of widespread, pervasive (and invasive)

---

[9] *See* 957 F. Supp. 2d at 31.
[10] 442 U.S. 735 (1979).
[11] *See id.* at 743–44.
[12] U.S. CONST. amend. IV.
[13] *Id.* To be fair, the Fourth Amendment actually only protects against *unreasonable* searches and seizures without a warrant. Decades of interpreting what qualifies as "unreasonable" have led to a somewhat murky jurisprudence of exceptions to the Fourth Amendment. The "third-party doctrine," as defined by *Smith*, is one such exception.
[14] *See* Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

technology, like cell phones. This so-called "third-party doctrine,"[15] articulated in *Smith* to validate the use of a pen register to monitor phone numbers dialed by a single person suspected of a crime, is today used to defend the widespread, passive collection of many Americans' cell phone and internet activities.[16] The doctrine is an artifact of a different time that desperately requires a technological update. The need for law enforcement to conduct investigations is obvious. But the government and courts have applied the rule too broadly, extending it to modern technologies unforeseen by the *Smith* Court in 1979. It eviscerates the requirement that law enforcement investigations employing such technology be reasonably targeted, temporary, and without undue intrusion into the private lives of ordinary citizens. These criteria—pillars of Fourth Amendment protections dating back to the American Revolution—crumble when third-party doctrine is applied to modern technology. As Judge Leon wrote in *Klayman I*:

> When do present-day circumstances—the evolutions in the Government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies—*become so thoroughly unlike those considered by the Supreme Court thirty-four years ago* that a precedent like *Smith* simply does not apply? The answer, unfortunately for the Government, is now.[17]

A recent Supreme Court case that, at least on its face, had nothing to do with *Smith*, offers a theoretical solution to the need for a revised third-party doctrine. In *Riley v. California*, the Supreme Court unanimously held that the traditional incident-to-arrest exception[18] to the warrant requirement did not apply to warrantless searches of arrestees' cell phones.[19] *Riley* rejected the application of the incident-to-arrest doctrine to cell phones—a decision that has little doctrinal bearing on *Smith* and the third-party doctrine. But underneath this holding, *Riley* expressed deep concerns with the increasing capacity of technology—cell phones in particular—and their ubiquity in modern society.[20] In his opinion for the unanimous Court, Chief Justice Roberts described cell phones as "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of the human anatomy."[21] Cell phones aren't just modern conve-

---

[15] *See, e.g.*, United States v. Davis, 785 F.3d 498, 512 (11th Cir. 2015).

[16] *See, e.g.*, Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 749–52 (S.D.N.Y. 2013).

[17] *Klayman I*, 957 F. Supp. 2d 1, 31 (D.D.C. 2013) (emphasis added).

[18] Like the third-party doctrine, the incident-to-arrest rule is another exception to the general Fourth Amendment requirement that law enforcement obtain warrants prior to searches and seizures. It allows law enforcement officials to search and seize personal effects of people as they are arresting them (and as long as that arrest is lawful). The rule is meant to ensure the safety of officers and the preservation of evidence. *See, e.g.*, Chimel v. California, 395 U.S. 752, 762–65 (1969).

[19] 134 S. Ct. 2473 (2014).

[20] *See generally id.*

[21] *Id.* at 2484.

niences anymore. They have become part of our *selves*.[22] Surely the aspects of life we hold most private, explicitly listed in the Fourth Amendment ("*persons*, homes, papers, and effects"),[23] deserve the most robust attention and protection. Applying *Riley*'s treatment of cell phones as extensions of the human self to third-party doctrine, I argue that the focus in technology cases should not be on the relationship between information and its dissemination to third parties, as the *Smith* regime would have it, but instead on our relationship with the devices that generate and convey that information.

The *Riley* decision makes abundantly clear that the role of technology was critical to the Court's reasoning. After *Riley*, commentators such as Linda Greenhouse poked fun at the Justices for basing their holding in large part on their knowledge of the amount of private information on their own personal cell phones.[24] Whether acting on real-life personal concern or not, the Justices resoundingly rejected the government's argument that "cellphones [sic] do not raise qualitatively different privacy concerns than items that the police have always had the authority to search incident to arrest, such as letters, diaries, briefcases, and purses."[25] *Riley* makes one thing clear: cell phones *are* different. Letters and briefcases are accessories, offshoots that contain information *about* our lives. Cell phones on the other hand, suggests the *Riley* opinion, are quasi-anatomical outgrowths of our *selves*.

As this paper argues below, the concern about the pervasiveness of modern technology is directly applicable to the third-party doctrine. In fact, the *Riley* opinion is in many ways reminiscent of Justice Marshall's powerful dissent in *Smith*, in which he decried the Court's decision as forcing individuals to "accept the risk of surveillance" unless they forgo "what for many has become a personal or professional necessity . . . ."[26] The cell phone is one of many examples of modern technology that have become necessary to contemporary life. By virtue of technological architecture, they also necessarily communicate a broad swath of personal information to third parties. *Riley* provides a tool for updating the outdated third-party doctrine so as to preserve its survival in its still-necessary form,[27] without allowing it to continue to apply to massive data collections such as those at issue in *Clapper*

---

[22] *Cf.* City of Ontario v. Quon, 560 U.S. 746, 760 (2010) ("Cell phone and text message communication are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification.").

[23] U.S. CONST. amend. IV (emphasis added).

[24] *See* Linda Greenhouse, *The Supreme Court Justices Have Cellphones, Too*, N.Y. TIMES (June 25, 2014), http://www.nytimes.com/2014/06/26/opinion/linda-greenhouse-the-supreme-court-justices-have-cellphones-too.html [http://perma.cc/UCF7-9NPX].

[25] *Id.* (quoting the government's brief in *Riley*).

[26] Smith v. Maryland, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting).

[27] For example, police officers should still be allowed to use information and documents pertaining to a criminal suspect if that suspect voluntarily surrendered that information to, say, an informant or undercover officer. *See, e.g.*, Hoffa v. United States, 385 U.S. 293, 300–03 (1966) (applying third-party doctrine to endorse the use of government informers against defendants, on the theory that the defendants waived their expectation of privacy in information they divulged to the informers); Lopez v. United States, 373 U.S. 427, 437–40 (1963) (same).

and *Klayman I*. The third-party doctrine as currently defined by *Smith* is too rigid and broad for a modern society in which third parties hold increasing amounts of personal information.[28] *Riley* illuminates the possibility of a more flexible, case-by-case approach, where pervasive and ubiquitous extensions of daily life, such as cell phones, are exempted from the third-party rule.

This article proceeds in five parts. Part I introduces the *Smith* definition of the third-party doctrine and analyzes the strong concerns articulated by the *Smith* dissents. Part II ushers the third-party doctrine into the contemporary legal framework, providing examples of how both state and federal courts are applying it to modern technologies. Part III discusses *Riley*, noting its doctrinal distinction from *Smith* while also emphasizing the theoretical similarities. Part IV argues that *Riley* evokes a philosophical concern with the role technology plays in our everyday lives. It highlights a potential update for the third-party doctrine by reframing modern technologies, such as cell phones, as part of the human self. Part V concludes.

I. *Smith* and the Historical Foundation of the Third-Party Doctrine

Smith v. Maryland*: The Opinion*

Because it has become the touchstone for constitutional defenses of government surveillance and investigations,[29] *Smith* is a logical starting point for a discussion of the third-party doctrine. The reasoning behind *Smith*, as well as the prescient counterarguments raised by its two dissenting opinions, will inform the argument below regarding how the third-party doctrine ought to be updated.

It is perhaps no coincidence that the "bedrock holding"[30] defining the third-party doctrine deals with telephones. *Smith* involved the installation of a pen register (a device used to record phone numbers dialed by a specific telephone line) to monitor outgoing calls made from the home of Michael Lee Smith, a Baltimore man suspected of robbery.[31] The police did *not* obtain a warrant prior to using the pen register, and used the data provided by the telephone company through the register's use to investigate, arrest, and subsequently prosecute Smith.[32] The question for the Supreme Court was

---

[28] *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal L. Rev. 1083, 1089 (2002).

[29] *See* Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 749–50 (S.D.N.Y. 2013); Privacy and Civil Liberties Oversight Board, Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court 116 (2014) [hereinafter PCLOB Report].

[30] *Clapper*, 959 F. Supp. 2d at 749 (describing *Smith*).

[31] *Smith*, 442 U.S. at 737.

[32] *Id.* at 737–38.

whether the Fourth Amendment barred the government's use of pen registers, without a warrant, to monitor the calls of a suspect.[33]

The majority opinion, written by Justice Blackmun, applies a famous test from the 1967 case *Katz v. United States*,[34] in which the Court asked whether the defendant had a "legitimate expectation of privacy" in the numbers he dialed on his phone.[35] *Katz* represented the culmination of a gradual shift in Fourth Amendment jurisprudence. Originally, the Fourth Amendment was thought to protect property interests—personal privacy was not traditionally associated with the prohibition against warrantless search and seizure.[36] After all, the Amendment was originally conceived of as a response to the general warrants practiced by the Crown against the colonies during the American Revolution. *Katz* offered an entirely different view of the Fourth Amendment and what it protects. Just two years after the Court in *Griswold v. Connecticut* found privacy to be a fundamental right guaranteed by the "penumbras" of the Bill of Rights,[37] *Katz* announced that one of those rights—namely the Fourth Amendment—protected *people*, not places.[38]

Applying the *Katz* test to private information divulged to someone else, however, the Court famously declared in *Smith* that "a person has no legitimate expectation of privacy in information"—like phone numbers—that is "voluntarily turn[ed] over to third parties."[39] Because Smith knew, or should have known, that the phone company keeps track of the numbers he dials, he no longer enjoyed a legitimate expectation of privacy in those numbers.

The Problem with a Modernized Third-Party Doctrine: Lessons from the Smith *Dissents*

The rule that a privacy interest in information is forfeited at the moment of conveyance to a third party has survived, virtually unchanged, to today. The *Smith* decision was not particularly controversial; the Court added to a long line of cases that stood for the proposition that by "revealing his affairs to another," a defendant risks that "information will be conveyed by that person to the Government."[40] However, *Smith* involved an individual target, suspected of committing a crime, monitored over a short period of time. Had

---

[33] *Id.*

[34] 389 U.S. 347, 361 (Harlan, J., concurring).

[35] *Smith*, 442 U.S. at 741–42.

[36] *See, e.g.*, United States v. Olmstead, 277 U.S. 438, 464–65 (1928) (holding that because there was no physical invasion of the defendant's property, there was no Fourth Amendment search).

[37] *See* Griswold v. Connecticut, 381 U.S. 479, 481–86 (1965).

[38] 389 U.S. at 351.

[39] 442 U.S. at 743–44.

[40] United States v. Miller, 425 U.S. 435, 443 (1976). *Miller*, decided only three years prior to *Smith*, held that the government could obtain an individual's bank records without a warrant. Whether bank records are as pervasive as cell phones, and should therefore be subject to the same "*Riley*-esque" exception proposed by this paper, is a fascinating question.

the Baltimore Police Department sought a warrant for their use of the pen register, they likely would have had no trouble getting one.

By endorsing their decision not to do so, the third-party doctrine leads to some troubling implications when pen registers and landline telephones give way, over time, to cell phones and email servers.[41] Even Stephen Sachs, the former Attorney General of Maryland who argued on behalf of the State in *Smith*, believes the modern application of *Smith* "goes far beyond" what Maryland was advocating for (and, indeed, believed it had won) in 1979.[42] The dissents in *Smith*, authored by Justices Stewart and Marshall, identified in 1979 much of what remains alarming about the third-party doctrine today. These dissents recognize a flaw in the Court's privacy rationale, stressing that "[p]rivacy is not a discrete commodity, possessed absolutely or not at all."[43] Yet the Court treats privacy as an on-off switch, flipped off by the mere act of knowingly transmitting a phone call through a telephone company. In his *Smith* dissent, Justice Stewart objected to the majority's interpretation of *Katz*, opining that "[i]t is simply not enough to say, after *Katz*, that there is no legitimate expectation of privacy in the numbers dialed because the caller assumes the risk that the telephone company will disclose them to the police."[44] Whether people *actually make* this assumption is perhaps the fundamental concern with the breadth of the third-party doctrine today. It requires a dangerous logical leap from the increasingly common decision to purchase and use a cell phone to the notion that embedded in that decision is the acquiescence that information contained on that phone will be shared with law enforcement.[45]

Unlike the confidential communications cases on which the majority in *Smith* rely, the risk of government surveillance seems mandatory with respect to telephone communications, "unless a person is prepared to forgo use of what for many has become a personal or professional necessity."[46] The telephone's social and professional importance is still hugely relevant today and evokes the same concerns raised by *Riley* in 2014. The choice to use a phone is different than the choice of to whom to divulge private information because it isn't really a choice at all. Participation in modern society requires the use of a phone—its necessity has arguably become analogous to

---

[41] *See, e.g.*, *1979 Supreme Court Ruling Becomes Focus of NSA Tactics*, NPR (Dec. 21, 2013), http://www.npr.org/2013/12/21/256114227/1979-supreme-court-ruling-becomes-focus-of-nsa-tactics [http://perma.cc/8ZCH-V8VV], transcript available at http://www.npr.org/templates/transcript/transcript.php?storyId=256114227 [http://perma.cc/DJ2B-LY6V].

[42] *Id.* Sachs describes the current state of the third-party doctrine as "really a far cry from the world in 1979. The ubiquity, for example, of cell phones now" informs his belief that government surveillance of cell phone metadata is a "massive intrusion . . . world's [sic] apart from what we argued in 1979." *Id.*

[43] *Smith*, 442 U.S. at 749 (Marshall, J., dissenting).

[44] *Id.* at 747 (Stewart, J., dissenting); *see also id.* at 749 (Marshall, J., dissenting) ("Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes.") (internal citations omitted).

[45] *See, e.g.*, State v. Earls, 70 A.3d 630, 643 (N.J. 2013).

[46] 442 U.S. at 750 (Marshall, J., dissenting).

food and shelter.[47] The perception of cell phones as *necessary* animates this notion that certain devices are virtual extensions of our selves, and the law should consider them accordingly.

The *Smith* dissents highlight other aspects of a broad third-party doctrine that are problematic for privacy purposes. For example, telephone metadata—phone numbers in particular—can "reveal the most intimate details of a person's life" when taken in aggregate.[48] Modern surveillance crystallizes this problem. Through phone numbers or GPS data alone, law enforcement can glean a person's medical history, social interactions, politics, and more. Widespread telephone surveillance, even without actual wiretapping, could have a chilling effect, implicating the First as well as the Fourth Amendment.[49] As the *Smith* dissents make clear, the monitoring of telephone calls, even without the conversations themselves, threatens privacy and liberty interests in ways that other applications of the third-party doctrine do not.

This is not to say that the doctrine as a whole should be abandoned. Confidential communications, for example, ought to be considered fair game for government collection, so long as they are not protected by some other evidentiary privilege (e.g., attorney-client privilege).[50] Phone numbers (*Smith*) and, perhaps, bank records (*Miller*)[51] capture aspects of everyday life that are virtually unavoidable to most people, and are therefore fundamentally different from other, more direct, disclosures of information to third parties. The *Smith* dissents identify this distinction, and the same reasoning informs the argument against applying the third-party doctrine to modern technology in the way it was applied in 1979. Any limits to the modern application of the third-party doctrine ought to derive from concerns proposed by Justices Stewart and Marshall in *Smith*.

Despite these concerns, *Smith* has never been overturned; it is still good law today. As the Foreign Intelligence Surveillance Court noted in a recent

---

[47] This is true even for those with little or no income. *See, e.g.*, Binyamin Appelbaum, *The Vanishing Male Worker: How America Fell Behind*, N.Y. TIMES (Dec. 11, 2014), http://www.nytimes.com/2014/12/12/upshot/unemployment-the-vanishing-male-worker-how-america-fell-behind.html [http://perma.cc/86NG-UG5R] (describing an unemployed Minnesota man who still pays $34 per month for cell phone service despite barely being able to afford monthly rent).

[48] *Smith*, 442 U.S. at 748 (Stewart, J., dissenting). This so-called "mosaic theory," concerning to Justice Stewart in 1979, has even more purchase today—it has been shown that intricate details of people's lives can be inferred purely from analyzing the phone numbers they dial. *See, e.g.*, *Klayman I*, 957 F. Supp. 2d 1, 36 (D.D.C. 2013).

[49] *See Smith*, 442 U.S. at 751 (Marshall, J., dissenting) ("The prospect of unregulated governmental monitoring will undoubtedly prove disturbing even to those with nothing illicit to hide.").

[50] *See generally* cases cited *supra* note 27.

[51] *Miller* and *Smith* are particularly broad applications of the third-party doctrine considering the fact that the third parties in both cases (the bank in *Miller* and the telephone company in *Smith*) are *required*, by law, to maintain the records. *See* Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 454 (2008). Yet the Court still viewed such information as having been "voluntarily conveyed" to third parties and therefore unprotected. United States v. Miller, 425 U.S. 435, 442 (1976).

order, *Smith* "remains controlling" and provides the legal justification for both police investigations and government surveillance programs.[52] The case is often cited simply for its broad declaration that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[53] Indeed, that sentence has defined the third-party doctrine, which now protects the government's warrantless acquisition of cell phone metadata and other forms of personal information.[54] However, as scholars and even some judges are beginning to realize, the digital age is not suited for a theory of privacy that excludes such a large chunk of human activity.[55] As Professor Solove writes, "[w]e are becoming a society of records, and these records are not held by us, but by third parties."[56]

A mechanical application of *Smith* to modern technology like cell phones threatens privacy in ways the dissents forewarned in 1979. Cell phones are ubiquitous—virtually necessary to daily life for many Americans—and their capacity to store and disseminate information is virtually limitless. If there were concerns with the implications of applying the third-party doctrine to a pen register, surely those concerns must be amplified when it comes to cell phones. It is therefore necessary to re-frame the third-party doctrine away from the *Smith* focus on the voluntary transfer of information to third parties, and instead on the *means of transfer*, and how those means have changed. As the subsequent sections illuminate, a selfhood-based approach—one that recognizes the window into personal life that devices like cell phones provide—would be more appropriate.

II. The Modern Application of the Third-Party Doctrine

Until recently, federal courts after *Smith* showed little willingness to expand Fourth Amendment protections in the face of rapidly expanding technology. Only actual intrusions into the home, such as the one in *United States v. Kyllo*,[57] tended to rouse concern.[58] However, a few cases, as well as

---

[52] *In re* Fed. Bureau of Investigation for an Order Requiring the Production of Tangible Things, No. BR 14–01, 2014 WL 5463097, at *5 (FISA Ct. Mar. 20, 2014).

[53] *Smith*, 442 U.S. at 743–44.

[54] *See* Rebecca Lipman, *The Third Party Exception: Reshaping an Imperfect Doctrine for the Digital Age*, 8 Harv. L. & Pol'y Rev. 471, 478 (2014) (citing United States v. Suarez-Blanca, No. 1:07–CR–0023–MHS/AJB, 2008 WL 4200156, at *8 (N.D. Ga. Apr. 21, 2008) (listing modern extensions of the third-party doctrine: "(1) bank records; (2) credit card statements; (3) kilowatt consumption from electric utility records; (4) motel registration records; (5) cell phone records; and (6) employment records")).

[55] *See* Solove, *supra* note 28, at 1089; Cate, *supra* note 51, at 456.

[56] Solove, *supra* note 28, at 1089.

[57] 533 U.S. 27 (2001). *Kyllo* rejected the use of thermal imaging technology to investigate a suspected grower of marijuana. The Court focused primarily on the technology's intrusion into the defendant's home—therefore, the case is not directly relevant to the third-party doctrine question. But the Court did ask more broadly "what limits there are upon [the] power of technology to shrink the realm of guaranteed privacy." *Id.* at 34.

[58] *See* Cate, *supra* note 51, at 460 ("[W]ith the sole exception of physical searches into the home, the Court has proven more likely to reduce, rather than preserve (much less expand), Fourth Amendment protections.").

Edward Snowden's recent revelations regarding the government's widespread surveillance programs,[59] suggest that there may be room to buck this trend.

The Importance of Necessity: United States v. Warshak

For example, in *United States v. Warshak*, the Sixth Circuit held that the warrantless seizure of a defendant's emails violated the Fourth Amendment, even though the government obtained the emails through the defendant's Internet Service Provider (ISP).[60] In so doing, *Warshak* limited the broad third-party doctrine as defined by *Smith*. The court's justification for this limit was simple: "[T]he Fourth Amendment must keep pace with the inexorable march of technological progress, or its guarantees will wither and perish."[61] Emails, the "technological scion of tangible mail,"[62] have become an essential means of communication, and must therefore share the rigorous Fourth Amendment protections that snail-mail enjoys.

The Sixth Circuit's commentary in *Warshak* on the pervasiveness and necessity of email in the modern era is reminiscent of Justice Marshall's argument regarding the use of the telephone in *Smith*. Email, therefore, could function as an additional candidate for the selfhood-based technological update to the third-party doctrine discussed in Part IV. The fact that people send email through an ISP does not suggest a voluntary transmission of information to a third party just as permitting the Post Office to convey a letter does not signify the sender's willingness for the mail carrier to read her missive. The ISP, crucially, was "not the intended recipient of the emails."[63] When a third party "carries, transports, or stores property for another," like the Post Office does with mail, and ISPs do with email, the third party is involved only "because it is essential to the customer's interests."[64] Modern communication—that which takes place outside the confines of in-person conversation—requires, by definition, the participation of third parties to function. *Warshak* excludes from the rigidities of *Smith* the necessary means we must employ in order to communicate with each other.

The Return of the "Mosaic Theory": United States v. Jones

Beyond the *necessary* involvement of third parties in technological communication, as emphasized by *Warshak*, there is a further concern about the pervasiveness of technology and the expansive picture of individual lives

---

[59] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 5, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [http://perma.cc/GJ43-7FHQ].

[60] 631 F.3d 266, 282 (6th Cir. 2010).

[61] *Id.* at 285.

[62] *Id.* at 286.

[63] *Id.* at 288.

[64] Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored Email*, U. CHI. LEGAL F. 121, 165 (2008).

technological data mining can paint. As Justice Sotomayor opined in her concurrence to the Supreme Court's opinion in *United States v. Jones*, 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."[65] *Jones* involved the warrantless GPS-tracking of the movements of a suspect's car. The case presented an opportunity to curb the absurd applications of the third-party doctrine, but while the Court did invalidate the search, it did so while skirting entirely the third-party doctrine (and arguably even strengthening it).[66] Recognizing the dangers implicit in the Court's opinion, Justice Sotomayor penned a concurrence that reads more like a dissent. Citing Justice Marshall's concern in *Smith* that "[p]rivacy is not a discrete commodity, possessed absolutely or not at all,"[67] Justice Sotomayor's *Jones* concurrence questions this "on-off" switch theory that is used to support the third-party doctrine's extension to technologies like cell phones. Privacy interests are not binary, and a sliding scale approach, as supported by the reasoning in *Riley*, would be wiser than a rigid "on-off" third-party analysis. Adopting an "on-off" approach to the third-party doctrine yields troubling results: all phone numbers dialed, web sites accessed, and email addresses contacted can be acquired by the government without a warrant, simply because such information was disclosed to a third party.[68] A doctrine that allows for warrantless acquisition of personal information ought to only cover discrete, targeted data. Without a substantive limit, the "on-off" conception of the third-party doctrine is capable of invading the very core of personal privacy. Focusing on *how* data is generated, as the *Riley* court did with respect to cell phones, could provide this substantive limit.

Information currently subject to the third-party doctrine is not a mere snapshot, but rather a wide-open window onto people's everyday lives. The D.C. Circuit identified this problem in *United States v. Maynard*, the case that led to the Supreme Court's decision in *Jones*.[69] This type of data unearths whether a person "is a weekly church goer, a heavy drinker, a regular at the gym, a faithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but *all* such facts."[70] *Maynard* and *Jones* involved the GPS-aided tracking of defendants' movements. The same concerns exist for

---

[65] 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

[66] The *Jones* majority reverted to a property-based approach for analyzing the Fourth Amendment implications of the police use of a GPS tracking device. Because the police had attached the device to the suspect's car, this represented a *physical intrusion* onto his personal property, a *per se* search under the Fourth Amendment. *See id.* at 949–54. It did not address the privacy implications of the GPS tracking itself, focusing instead on the physical intrusion of the device onto the defendant's car.

[67] Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting).

[68] *See Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

[69] *See* United States v. Maynard, 615 F.3d 544, 555–68 (D.C. Cir. 2010), *aff'd sub nom.*, United States v. Jones, 132 S. Ct. 945 (2012).

[70] *Id.* at 562 (emphasis added).

data-only digital surveillance—where intimate details of an individual's life can be easily interpreted just on the basis of metadata.[71]

Telephone Metadata: Klayman v. Obama

Indeed, it was the government's bulk collection of telephone metadata ("non-content" surveillance, or so goes the government's argument)[72] that provoked a federal judge to proclaim in *Klayman I* that the third-party doctrine as announced in *Smith* ought not be applied to "almost-Orwellian technology."[73] *Klayman I* is the first, and only, federal case to invalidate the government's telephony metadata program on constitutional grounds. It stands in direct opposition to other challenges to the program that have been rejected, such as in *Clapper*.[74] *Klayman I* relied on the same concerns raised by the *Smith* dissents and Justice Sotomayor's concurrence in *Jones* to refuse to extend the third-party doctrine to a technology it was not designed to reach. *Klayman I* beckoned to the vast gulf separating the Baltimore Police Department's use of the pen register to monitor Michael Lee Smith's phone calls for a few days, and the U.S. government's widespread and indefinite collection of cell phone metadata.[75] Because the two have "so many significant distinctions between them," Judge Richard Leon wrote in *Klayman I*, "I cannot navigate these uncharted Fourth Amendment waters using as my North Star a case that predates the rise of cell phones."[76]

State Courts and the Third-Party Doctrine

In order for a technological update to the third-party doctrine to become law, a court, likely the Supreme Court, will have to declare it so. The *Clapper* court appeared to entertain the possibility of updating the doctrine before rejecting it as the exclusive purview of the Supreme Court, not the lower courts.[77] In the meantime, it may be instructive to note that several *state* courts have already recognized the danger in a third-party doctrine as broad and absolute as the one announced in *Smith*. As Professor Stephen Hender-

---

[71] This type of data-only surveillance is to be distinguished from, for example, wiretapping, where telephone conversations are actually recorded and eavesdropped.

[72] The government distinguishes its metadata program—which records only the dates, times, and phone numbers of placed calls—from "content" surveillance, which actually monitors the conversations themselves. The statute that authorizes the metadata program does not authorize wiretapping, *see generally* USA PATRIOT Act, Pub. L. No. 107–56, § 215, 115 Stat. 272 (2001), and the government cites this for why the program is constitutional.

[73] *Klayman I*, 957 F. Supp. 2d 1, 33 (D.D.C. 2013).

[74] *Clapper* declared that "[t]he collection of breathtaking amounts of information unprotected by the Fourth Amendment does not transform that sweep into a Fourth Amendment search." Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 752 (S.D.N.Y. 2013).

[75] *See Klayman I*, 957 F. Supp. 2d at 32–37.

[76] *Id.* at 37.

[77] *See Clapper*, 959 F. Supp. 2d at 752 ("[T]he Supreme Court has instructed lower courts not to predict whether it would overrule a precedent even if its reasoning has been supplanted by later cases.").

son reports, eleven states have formally rejected the third-party doctrine, with ten more indicating they might do so in the future.[78] Below are a few examples of states that formally grappled with the technological implications of the third-party doctrine, absent any U.S. Supreme Court guidance on the subject.

Hawaii, for example, has formally rejected the third-party doctrine in both the telephone (*Smith*) and bank records contexts (*Miller*).[79] In *Walton*, decided in 2014, the Hawaii Supreme Court overruled a prior case, *State v. Klattenhoff*,[80] which had adopted the U.S. Supreme Court's decision in *Miller*, finding that both *Klattenhoff* and *Miller* were inconsistent with the Hawaii Constitution.[81] The *Walton* reasoning highlights similar concerns with the binary nature of the third-party doctrine. The court identifies "rapid changes in technology" which have created "a dissonance between a mechanical application of the expectation of privacy test and its core meaning."[82] This is reminiscent of Justice Marshall's complaint that privacy is not an on-off switch, "possessed absolutely or not at all."[83] *Walton* rejects this inflexible approach, relying in large part on Justices Stewart's and Marshall's dissents in *Smith* and Justice Sotomayor's concurrence in *Jones*.[84] It instead opts for a case-by-case analysis that asks whether a defendant had "a legitimate expectation that such information would not be shared with others."[85] Such a view is perhaps more faithful to the original *Katz* test than the third-party doctrine as held by *Smith* and *Miller*. Factors to consider include whether a subjective privacy expectation existed, whether the information in question reveals "intimate details of a person's life," and whether the release of information to a third party was necessary and without realistic alternative.[86] All of these criteria would build a more flexible third-party doctrine, appropriate for a technological society replete with information sharing.

Other states, even ones that have not formally rejected the federal third-party doctrine, are sympathetic to the case-by-case approach proposed by Hawaii in *Walton*. Professor Henderson commends Indiana for its "nuanced, context-specific" approach, which he describes as "essential in the modern world."[87] Specifically within the realm of cell phones, the New Jersey Supreme Court recently noted that "[p]eople buy cell phones to communicate with others, to use the Internet," and increasingly for other reasons—but

---

[78] *See* Stephen Henderson, *Learning From All Fifty States: How to Apply the Fourth Amendment and its State Analogs to Protect Third Party Information From Unreasonable Search*, 55 CATH. U. L. REV. 373, 376, 396–400 (listing table of states that have rejected, or indicated they might reject, the third-party doctrine).

[79] *See* State v. Rothman, 779 P.2d 1, 7–8 (Haw. 1989) (declining to adopt *Smith*); State v. Walton, 324 P.3d 876, 906–07 (Haw. 2014).

[80] 801 P.2d 548 (Haw. 1990).

[81] *See Walton*, 324 P.3d at 906–07.

[82] *Id.* at 908.

[83] Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting).

[84] *See Walton*, 324 P.3d at 903–06.

[85] *Id*. at 907.

[86] *See id.* (quoting *Smith*, 442 U.S. at 748 (Stewart, J., dissenting)).

[87] Henderson, *supra* note 78, at 422.

nobody buys cell phones with the assumption that these activities will be shared with the police.[88] The Massachusetts Supreme Judicial Court further limited the rigidity of its third-party doctrine in 2014, declaring that the "digital age has altered dramatically the societal landscape from the 1970s, when *Miller* and *Smith* were written."[89]

An evolving landscape requires an evolving doctrine. The above cases are just a few of many examples of how the states have been grappling with the third-party doctrine in the light of rapid technology growth. They embody the need to tie the collection of personal data to the characteristics of both the data itself and the mechanisms through which the data is being retrieved, rather than the old-fashioned focus on to whom it was being disseminated. As Professor Henderson rightly argues, "[o]btaining different types of information from different types of third parties should require different quanta of suspicion and different processes."[90] A scaled, flexible approach would respond to these concerns with technology without eviscerating the third-party doctrine entirely. The extension of a categorical rule would dangerously ignore the particular privacy concerns that cell phones and other technologies implicate.

The law evolves with technology all the time. The temporal and technological gulf between *Smith* and today is ample reason to limit the extension of the third-party doctrine to the use of technologies like cell phones. The differences between pen registers and cell phones, cited in depth by Judge Leon in *Klayman I*, are vast. These differences are discussed in a different legal context by the Supreme Court in *Riley*. *Riley* focuses on how data is generated and stored on cell phones, articulating a sense that they have become central to our personhood. Concerns about the depths of human selfhood and privacy—fundamental principles protected by the Fourth Amendment—animate the mood of *Riley*, and provide a new technological framework for the third-party doctrine.

III. *RILEY V. CALIFORNIA*

On its face, *Riley* has nothing to do with the third-party doctrine. It is about searches and seizures incident-to-arrest, another exception to the warrant requirement of the Fourth Amendment, which is justified by concern for the safety of arresting officers and the preservation of evidence.[91] This is distinguishable from the justifications for the third-party doctrine, which is justified by the notion that information given to third parties assumes the

---

[88] State v. Earls, 70 A.3d 630, 643 (N.J. 2013).

[89] Commonwealth v. Augustine, 4 N.E.3d 846, 859 (Mass. 2014). To be fair, *Augustine* was limited to an analysis of cell tower data, rather than the telephony metadata addressed above. Still, it is a useful discussion of technology more broadly, and how a categorical third-party rule is no longer viable.

[90] Henderson, *supra* note 78, at 423.

[91] *See* Chimel v. California, 395 U.S. 752, 762–63 (1969).

risk that it will subsequently end up in the hands of the government.[92] *Riley* declines to extend the incident-to-arrest exception to cell phones, holding instead that "officers must generally secure a warrant before conducting . . . a search" of an arrestee's phone.[93] In so doing, the Court references the third-party doctrine only once, in passing, to reject the government's argument that *Smith* allowed police officers unlimited discretion to search a cell phone's call log.[94] It is important to understand, therefore, that *Riley* is doctrinally distinct from *Smith* and the third-party doctrine.

However, the Court in *Riley* evokes precisely the same concerns with the role of technology in modern society as *Warshak* and *Klayman I* expressed. In a way, *Riley* is a comment on culture as much as a legal decision. These underpinnings of the *Riley* opinion can easily be applied to the third-party context in the search for technology- and privacy-facing limits.

First, *Riley* announces a test for the incident-to-arrest doctrine that balances its justifications, as expounded by *Chimel v. California*, with "this particular category of effects."[95] This simple rule articulation represents an important doctrinal update. (Balancing the old doctrine, and its justifications, with "this particular category of effects," is *precisely* the type of doctrinal update this paper seeks for the third-party doctrine. *Riley* provides the blueprint.) In *United States v. Robinson*,[96] the Court announced a bright-line rule: incident-to-arrest searches are reasonable regardless of "the probability in a particular arrest situation that weapons or evidence would in fact be found."[97] This rigid *Robinson* rule can be understood as a corollary to *Smith* for the incident-to-arrest context: a rigid rule the inflexibility of which *Riley* recognizes. In the face of thirty years of technological developments since *Robinson*, *Riley* refuses to extend the rule to searches of data on cell phones.[98] *Riley* recognizes that a rigid rule from the 1970s should not be blindly applied to a society that has evolved beyond the speculation of the rule's advocates. Even Stephen Sachs, the attorney who argued *Smith* for the State of Maryland at the Supreme Court in 1979, opposes the current appli-

---

[92] *See* Smith v. Maryland, 442 U.S. 735, 745 (1979).

[93] Riley v. California, 134 S. Ct. 2473, 2485 (2014).

[94] *Id.* at 2492–93. After all, the Court reasoned, the entire premise of *Smith* and the third-party doctrine is that information accessed after it has been provided to a third party is *not* a Fourth Amendment search. *Id.* at 2492. Here, there was no question that the officers' activity was both a *search* and *seizure* of the defendants' phone—the contents of which were not necessarily provided to third parties. *Id.* at 2492–93. The question was whether such a search was excepted by the incident-to-arrest doctrine. *Id.* at 2484.

[95] *Id.* at 2485.

[96] 414 U.S. 218 (1973).

[97] *Id.* at 235.

[98] *Riley*, 134 S. Ct. at 2485. Even if *Riley* is read to simply carve out an exception for cell phones, and only cell phones (a rather narrow reading of the opinion), it still resonates for its willingness to adapt an old legal doctrine to modern technology.

cation of the third-party doctrine, which he says "*certainly* wasn't contemplated by those involved in *Smith*."[99]

In addition to establishing a more flexible rule for incident-to-arrest, *Riley* discusses the function and pervasiveness of cell phones in society. Cell phones of the sort that exist today were "unheard of ten years ago," let alone when *Robinson* and *Smith* were decided—nowadays, they are possessed by "a significant majority of American[s] . . . ."[100] *Riley* recognizes that a "search of the information on a cell phone bears little resemblance" to the type of search conducted in *Robinson* (or, for that matter, *Smith*).[101] Applying categorical rules from three decades ago to incomparable facts "is like saying a ride on horseback is materially indistinguishable from a flight to the moon."[102] Searches of digital data, specifically that contained on cell phones, present new, challenging implications.

For instance, *Riley* explains, cell phones have "immense storage capacity"—while people are physically unable to carry around all of their mail, photographs, or reading material, they can easily do so with cell phones.[103] Privacy concerns abound. "The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions."[104] It would be nonsensical to apply a categorical allowance for incident-to-arrest searches in the face of such broad factual distinctions.

The concern in *Riley* with the piecing together of an individual's life through cell phone searches cuts at the heart of what the Fourth Amendment is trying to protect: our individual, physical selves. To be fair, the privacy implications animating *Riley* are especially stark because the contents of the physical phone are at stake. But quick analysis of just the data generated from cell phone usage can easily create a simulacrum of human experience. This so-called "mosaic theory" is alarming, because it directly contradicts the notion that metadata, for example, is "non-content" and therefore not intrusive.[105] This jump from data to a conceptual picture of a life is getting easier. Increased cell phone capacity has led to dramatically increased usage—2.3 trillion voice minutes were spent on cell phones in 2012, an increase from 62.9 billion in 1997.[106] Metadata alone, government capture of which *Smith* provides blanket authorization for, reveals "a vibrant and con-

---

[99] David Kravets, *How a Purse Snatching Led to the Legal Justification for NSA Domestic Spying*, WIRED (Oct. 2, 2013), http://www.wired.com/2013/10/nsa-smith-purse-snatching/ [http://perma.cc/LM3H-2GCR] (emphasis added).

[100] *Riley*, 134 S. Ct. at 2484 (citing AARON SMITH, PEW RESEARCH CTR., SMARTPHONE OWNERSHIP—2013 UPDATE (2013)).

[101] *Id.* at 2485.

[102] *Id.* at 2488.

[103] *See id.* at 2489.

[104] *Id.*

[105] *See supra* note 48 and accompanying text.

[106] *See Klayman I*, 957 F. Supp. 2d 1, 36 (D.D.C. 2013) (citing CTIA, *Wireless Quick Facts*, http://www.ctia.org/your-wireless-life/how-wireless-works/wireless-quick-facts [http://perma.cc/85NS-38RS]).

stantly updating picture of [a] person's life," virtually unforeseeable in 1979.[107] If anything, our legitimate expectation of privacy should expand, not contract, with the implications of technology.[108]

In addition to increased capacity for personal information, *Riley* also identifies a pervasiveness of cell phones that raises privacy concerns. The opinion's quip that a Martian visitor might believe phones to be a human body part[109] is farther from hyperbole than it seems. Many cell phone users report being within arm's reach of their phones at most times.[110] Cell phones allow for the convenient maintenance of digital records, *on one's person*, "of nearly every aspect of [life]—from the mundane to the intimate."[111] The Court has identified the pervasive nature of cell phones before, noting in *City of Ontario v. Quon* that they are "so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification."[112] Judge Leon applied these concerns directly to the third-party context in *Klayman I*, noting that, while the definition of telephony metadata has not changed, the ubiquity, quantity, and breadth of metadata has changed dramatically.[113]

In both doctrinal contexts—incident-to-arrest and third-party—it would be foolish, therefore, to simply ignore these changes in society attributable to cell phones, in favor of a rigid, outdated doctrinal rule. The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[114] Cell phones, obviously, are not included in the enumerated list—had the Framers been supernaturally prescient, perhaps they would have been. In many ways, the modern cell phone is as much a feature of our *selves* as anything, more even than our homes.[115] An analogy to human anatomy is therefore apt. Cell phones speak directly at the core of the Fourth Amendment—they are reflections of our individualism, and therefore deserve the strictest protection.

---

[107] *Id.*

[108] *See id.*

[109] *Riley*, 134 S. Ct. at 2484.

[110] *See id.* at 2490 (citing HARRIS INTERACTIVE, 2013 MOBILE CONSUMER HABITS STUDY (2013)).

[111] *Id.*

[112] City of Ontario v. Quon, 560 U.S. 746, 760 (2010).

[113] *See Klayman I*, 957 F. Supp. 2d 1, 35–36 (D.D.C. 2013).

[114] U.S. CONST. amend. IV.

[115] *See Riley*, 134 S. Ct. at 2491 (stating that "a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house"); *Quon*, 560 U.S. at 760 (stating that "some persons may consider [cell phones] to be essential means or necessary instruments for self-expression, even self-identification").

IV. Re-Thinking the Third-Party Doctrine: Self, Body, and Technology

Riley does not overrule *Smith*. What it *does* do is offer a different way to think about the human experience interacting with devices, and the impact of those devices on data generation. The devices that generate data, and the often automatic mechanisms by which those devices transmit data, are far more relevant for Fourth Amendment privacy concerns than just the fact that the data was given to a third party. This section outlines a new path for the third-party doctrine, as embodied by the discussion in *Riley*. It clarifies how *Smith* is still good law, but focuses on criteria of selfhood and individuality that might help to update the doctrine.

In their recently filed brief to the D.C. Circuit, Plaintiff Larry Klayman and his co-plaintiffs declared that *Riley* "invalidate[d]" *Smith* in the case at hand.[116] This misses the point. *Riley* provides, more than anything, a cultural reflection on why the third-party doctrine needs a technological update. If the nine Supreme Court Justices, all of whom are older than the average cell phone user, are aware of the pervasiveness and ubiquity of cell phones and how that ought to impact legal analysis, surely the country is similarly aware.[117] Mr. Klayman's amici in the D.C. Circuit appeal, the American Civil Liberties Union and the Electronic Frontier Foundation, took a more realistic and nuanced approach with respect to the relationship between *Riley* and the third-party doctrine. *Riley*, the amici argued, simply reiterated what the Supreme Court and D.C. Circuit have already held: that "earlier Fourth Amendment cases cannot be blindly applied in the digital age . . . ."[118] But it is crucial to emphasize that *Smith* is still good law, and with the exception of Judge Leon's opinion in *Klayman I*, it continues to support even the most widespread forms of government surveillance.[119]

The third-party doctrine, as defined by *Smith*, focuses on the information or data sought by the government, and the means by which it can be obtained. In other words, if the source of the relevant data is anyone other than the defendant (e.g., a cell phone provider), the third-party test under *Smith* is satisfied. The evolution of technology has diluted the purchase of this test by creating exponentially more information, stored primarily in hands other than the information's original source.[120]

---

[116] Brief for Plaintiffs-Appellees at 8, *Klayman II*, 800 F.3d 559 (D.C. Cir. 2015) (Nos. 14-5004, 14-5005, 14-5016, 14-5017).

[117] *See* Greenhouse, *supra* note 24.

[118] Brief for the Electronic Frontier Foundation, the American Civil Liberties Union, and the ACLU of the Nation's Capital as Amici Curiae Supporting Plaintiffs-Appellees at 26, *Klayman II*, 800 F.3d 559 (D.C. Cir. 2015) (Nos. 14-5004, 14-5005, 14-5016, 14-5017).

[119] *See* PCLOB Report, *supra* note 29, at 114; Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 752 (S.D.N.Y. 2013) ("Because *Smith* controls, the NSA's bulk telephony metadata collection program does not violate the Fourth Amendment.").

[120] *See* Solove, *supra* note 28, at 1089.

The *Smith* analysis is backward looking: how did the government come to possess information? A *Riley*-based update to the doctrine would start from the inception of the data, and ask which *sources* of information ought the government be able to access. As Chief Justice Roberts warned, cell phones are becoming figuratively, if not literally, attached to our bodies.[121] Internally, our devices contain an increasingly high percentage of our personal information. Externally, they account for the lion's share of our daily communications. By distinguishing cell phones from other items found in an arrestee's car, *Riley* offers a way to recognize the increasingly close relationship between our devices and our selves. This acknowledges the different media through which we *generate* data, as opposed to the ways in which that data can be accessed by the government. Importing the *Riley* rationale to the third-party doctrine context would target the core of what the Fourth Amendment protects: "[t]he right of the people to be secure in their *persons*."[122]

Cell phones have become extensions of our selves, and should be included in this "right" to be "secure" in our "persons." Data generation and storage capability are helpful criteria for building this framework of technological selfhood. Others might include proximity to the body and frequency of use. Writing separately in *Riley*, Justice Alito notes the discrepancy between the sheer quantity of digital data contained in our persons and what people would be able to carry in hard copy.[123] *Riley* identifies perhaps two additional characteristics that justify this "technological anatomy" update to the third-party doctrine: pervasiveness and necessity.[124] The prescient *Smith* dissents again resonate: that which is ubiquitous and necessary to human interaction in society, business, and everyday life exposes too much self to be exempted from Fourth Amendment scrutiny.[125]

The Historical Legacy of Updating the Fourth Amendment to Respond to Changing Technology

This would not be the first time that Fourth Amendment doctrine has had to adapt to changing technology. Over the course of the twentieth century, the Fourth Amendment evolved from protecting only physical intrusions onto physical property to acknowledging a more personal right to privacy.[126] The shift in doctrine, from *United States v. Olmstead* to *Katz*,

---

[121] *See* Riley v. California, 134 S. Ct. 2473, 2484 (2014).

[122] U.S. CONST. amend. IV (emphasis added).

[123] *Riley*, 134 S. Ct. at 2496 (Alito, J., concurring) ("Many cell phones now in use are capable of storing and accessing a quantity of information, some highly *personal*, that no person would ever have had on his person in hard-copy form.") (emphasis added).

[124] *See id.* at 2484 (describing cell phones as "pervasive and insistent").

[125] *See* Smith v. Maryland, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting).

[126] *Compare* Olmstead v. United States, 277 U.S. 438, 464–65 (1928) (holding that because there was no physical invasion of the defendant's property, there was no Fourth Amendment search), *with* Katz v. United States, 389 U.S. 347, 351 (1967) ("[T]he Fourth Amendment protects *people*, not places." (emphasis added)).

correlates with rapid technological development in general, and in particular with the growing pervasiveness of one type of technology: telephone communications. Whereas *Olmstead* declared that the "United States takes no such care of telegraph or telephone messages as of mailed sealed letters,"[127] *Katz* focused not on the telephone, but on the individual using it.[128] *Katz* recognized that society had developed certain expectations while using the telephone: a (now famous) reasonable expectation of privacy.[129]

Katz ushered in a new era of Fourth Amendment jurisprudence, one that focused on privacy rather than property.[130] *Smith* is a product of that trend. It excludes from Fourth Amendment protection third-party information on the basis that people do not have a legitimate expectation of privacy for information they have shared.[131] In the three decades since *Smith*, the capacity of telephonic communication has expanded exponentially more than it did in the four decades between *Olmstead* and *Katz*. Cell phones have wholly different functionalities, such as text messaging and calendar applications, than their pre-cellular counterparts. They have a broader, and more primary place in the daily human experience than they did in 1979—the same sort of evolution that took place between *Olmstead* and *Katz*—only more stark. Expectation of privacy (*Katz*) and whether information has been shared (*Smith*) are no longer effective proxies for more fundamental Fourth Amendment concerns.

"An Important Feature of Human Anatomy"

Extending *Riley* to the third-party doctrine would refocus Fourth Amendment analysis on the devices that possess the information sought by the government, rather than whether that information was transmitted to a third party. This is perhaps an ironic homage to the traditional property conception of the Fourth Amendment analysis. These particular types of property are so pervasive, and so capacious in their capacity to generate, transmit, and store personal information, that our concern about "physical intrusion" should be at its peak. The crucial leap is to include the data itself—some of which can be collected even without physically interfering with the device—in the scope of this device-centric analysis. The data, inextricable aspects of the physical devices, caused cell phones to evolve from widespread tools of communication to extensions of human anatomy.

Even the term "cell phone" is inherently misleading. They are, more accurately, "minicomputers that also happen to have the capacity to be used as a telephone."[132] Their capacity, both to store and to send, is unparalleled

---

[127] *Olmstead*, 277 U.S. at 464.
[128] *See Katz*, 389 U.S. at 351–52.
[129] *See id.* at 360 (Harlan, J., concurring).
[130] *See*, *e.g.*, Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-First Century*, 65 IND. L.J. 549, 557–59 (1990).
[131] *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979).
[132] Commonwealth v. Stem, 96 A.3d 407, 412–13 (Pa. Super. Ct. 2014) (quoting Riley v. California, 134 S. Ct. 2473, 2489 (2014)).

in human history—and they sit within arm's reach for the majority of our daily lives.[133] Not only are they parts of our selves—they are infinitely voluminous parts. Therefore our analysis of their Fourth Amendment implications should begin with the devices themselves, and the personal information they generate, as opposed to a backward-looking *Smith* conception of what we did with that data once it was created.

Cell phones, as *Riley* illustrated, "differ in both a quantitative and a qualitative sense from other objects" that might be the subject of a government search.[134] These differences—their pervasiveness, ubiquity, storage and transmission capacity—transform cell phones into something greater than the sum of their parts. Applying the same level of Fourth Amendment scrutiny to cell phones as we did to telephones and pen registers in 1979 is illogical. *Smith* prefers to analyze a cell phone's relationship with a service provider while *Riley* analyzes their relationship with their owners.

The digital age has already transformed the Fourth Amendment landscape. From GPS tracking in *Jones* to cell phone metadata collection in *Clapper* and *Klayman I*, courts are grappling with new Fourth Amendment questions every year. At this point, the general claim "that settled Fourth Amendment precedent may [not] apply . . . in the context of digital searches" is almost a truism.[135] The existence of massive amounts of easily disseminated electronic information directly implicates the fear of general warrants,[136] the historic foundation of the Fourth Amendment.[137]

However, the practical impact *Riley* will have is still an open question. In 2013, the Fifth Circuit upheld an application of the Stored Communications Act[138] that targeted historical cell site location data.[139] Relying on *Smith* and the third-party doctrine, the *Historical Cell Site* opinion reasoned that cell phone users "understand that their service providers record their location information when they use their phones at least to the same extent that the landline users in *Smith* understood that the phone company recorded the numbers they dialed."[140] It noted further that because "[t]he Government does not require a member of the public to own or carry a phone," the use of cell phones is "entirely voluntary."[141] In other words, *Historical Cell Site* interpreted the third-party doctrine exactly the same way *Smith* did—broadly

---

[133] *See Riley*, 134 S. Ct. at 2490.

[134] *Id.* at 2489.

[135] *See* United States v. Lustyik, 57 F. Supp. 3d 213, 229 n.12 (S.D.N.Y. 2014).

[136] During the American Revolution, warrants would be issued to permit British soldiers to inspect the homes of American colonists, without any subject-matter or time limitations. These so-called "general warrants" were the basis for the Fourth Amendment at the Constitutional Convention.

[137] *See* United States v. Galpin, 720 F.3d 436, 447 (2d Cir. 2013); United States v. Comprehensive Drug Testing, Inc., 621 F.3d 1162, 1176 (9th Cir. 2010) (noting the "serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant").

[138] 18 U.S.C. §§ 2701–2712 (2012).

[139] *See In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013).

[140] *Id.* at 613.

[141] *Id.*

and without limitation—despite recognizing "that technological changes can alter societal expectations of privacy."[142] The changing social landscape scored no points in the face of firm Supreme Court precedent.

The next year, the Supreme Court decided *Riley*. Soon thereafter, the Fifth Circuit upheld *Historical Cell Site*, finding that *Riley* overruled neither it nor *Smith*.[143] In *United States v. Guerrero*, the Fifth Circuit punted on the academic question of how technology is interacting with societal concerns about privacy in favor of the doctrinal trump card: whether the Supreme Court has spoken on the issue.[144] This is a common, albeit perhaps frustrating, approach for an appellate court to take. Without a clear Supreme Court doctrinal shift, the third-party doctrine is set in stone (or in *Smith*). And, as *Guerrero* aptly notes, the academic jury is still out as to what impact *Riley* will have on the Supreme Court's third-party jurisprudence.[145]

For those concerned about cell phones, and the broader threat technology poses to privacy, the answer seems clear: in order to curb the continued robotic application of *Smith* we need a new doctrine. *Riley* offers a path, not in its limited incident-to-arrest holding, but in the cultural zeitgeist it evokes. Cell phones are inextricable extensions of the human body. They are used often, and by many.[146] They are *not* voluntary frivolities, as *Historical Cell Site* suggests. They are necessary for many people (and not just the wealthy or business-oriented).[147] As Professor Solove notes, *Riley* suggests that "[w]hat matters [now] is the data involved and how much it reveals about a person's private life."[148] Cell phones are more than the data they store or the

---

[142] *See id.* at 614 (citing United States v. Jones, 132 S. Ct. 962 (2012) (Alito, J., concurring)).

[143] *See* United States v. Guerrero, 768 F.3d 351, 359–60 (5th Cir. 2014).

[144] *See id.* at 361 ("[W]e do not read tea leaves to predict possible future Supreme Court rulings, but only decide whether an issued Supreme Court decision has 'unequivocally' overruled our precedent.").

[145] *Compare* Daniel Solove, The U.S. Supreme Court's 4th Amendment and Cell Phone Case and Its Implications for the Third Party Doctrine, CONCURRING OPINIONS (June 25, 2014), http://concurringopinions.com/archives/2014/06/the-u-s-supreme-courts-4th-amendment-and-cell-phone-case-and-its-implications-for-the-third-party-doctrine.html [http://perma.cc/R2FG-4YKH] ("Although the case involves searches incident to arrest and not other areas of the Fourth Amendment, the Court recognizes some key points about privacy and technology that harbinger a change in some other Supreme Court doctrines [such as the third-party doctrine]."), *with* Barry Friedman, How the Supreme Court Changed America This Year, POLITICO MAGAZINE (July 1, 2014), http://www.politico.com/magazine/story/2014/07/how-the-supreme-court-changed-america-this-year-108497_Page3.html [http://perma.cc/E5FD-VLVG] ("First, the *Riley* majority didn't touch the issue that's really on everyone's digital mind, the 'third party' doctrine . . . . That's where the real digital action is, but a footnote in *Riley* said the court was not going near the question. Those who believe the justices will leap from *Riley* to overturning the third party doctrine are dreaming.").

[146] *See* Riley v. California, 134 S. Ct. 2473, 2484 (2014) ("[A] significant majority of American adults now own [smart] phones.") (citing AARON SMITH, PEW RESEARCH CTR., SMARTPHONE OWNERSHIP—2013 UPDATE (2013)); *id.* at 2490 ("[M]ore than 90% of American adults who own a cell phone keep on their person a *digital record of nearly every aspect of their lives – from the mundane to the intimate*.") (citing City of Ontario v. Quon, 560 U.S. 746, 760 (2010) (emphasis added)).

[147] *See* Appelbaum, *supra* note 47.

[148] Solove, *supra* note 145.

metadata they transmit. They are windows onto the human experience, at least as revealing, if not more so, than any of the papers and effects the Fourth Amendment explicitly protects. Chief Justice Roberts's "proverbial visitor from Mars" would be correct in its conclusion: cell phones have become "an important feature of human anatomy."[149]

V. Conclusion

Riley v. California provokes a serious discussion about the growing role of technology in the lives of human beings, and whether this trend demands a similar evolution in our legal doctrine. Law enforcement still needs the third-party doctrine—sting operations and police informants depend on it. But its value to law enforcement can no longer justify its absolute application to *any* information conveyed to a third party,[150] because in our modern society that simply captures too much. Without eviscerating the third-party doctrine entirely, it is imperative to decline to extend it to the widespread use of technology like cell phones and other internet-based devices.[151]

Applying a case involving a single pen register recording the phone numbers of a single landline to the realm of cell phones is, indeed, "like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together."[152] *Riley* represents a significant updating of the incident-to-arrest doctrine, recognizing that evolving technology demands evolving law. The third-party doctrine, still alive and well, needs a similar update.

Riley provides the beginnings of that update. To force cell phone usage into the third-party doctrine is like fitting a square peg in a round hole. Our phones say too much about our selves to exclude them from Fourth Amendment protection pursuant to the rigid application of an outdated rule. Cell phones are, for better or for worse, extensions of the self. They can be filled with as much information as humans have to give up, and their use is as voluntary as participation in society is voluntary. Even cell phone metadata, distinguished by defenders of government surveillance from the "content" of the telephone conversations themselves, can construct a clear "mosaic" of individual lives.[153] That mosaic can show medical history, sexual orientation,

---

[149] *Riley*, 134 S. Ct. at 2484.

[150] *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

[151] This paper has focused on cell phones, because of the direct connection to *Riley*. But the theory would apply to devices like iPads, Apple Watches, and the like.

[152] *Riley*, 134 S. Ct. at 2488.

[153] *See* Jonathan Hafetz, *Bulk Data Collection and the Mosaic Theory: A More Balanced Approach to Information*, Just Security (Jan. 17, 2014, 9:00 AM), https://www.justsecurity.org/5758/guest-post-bulk-data-collection-mosaic-theory [http://perma.cc/R2Q4-F3WW] ("The mosaic theory provides an opportunity to adopt the Fourth Amendment to the privacy intrusions accompanying rapid technological change.").

political preference, and more.[154] Such a technological deconstruction of privacy, on the grounds of an outmoded legal architecture, is, as *Smith* oral advocate Stephen Sachs himself believes, "a bridge too far."[155]

[154] *See* United States v. Jones, 132 S. Ct. 945, 955–57 (2012) (Sotomayor, J., concurring).
[155] Kravets, *supra* note 99.