Evolving Technology and the Fourth Amendment: The Implications of *Riley v. California*

*Andrew Pincus**

How should constitutional principles take account of changes in technology?

The Supreme Court has faced this question in a variety of contexts: under the First Amendment, as technology advanced from pamphlets and printing presses to broadcast television (with its limited number of channels),[1] to cable systems (with myriad channels),[2] and to the internet;[3] under the Second Amendment, with the Court explaining that although long guns were the self-defense weapon of choice when the amendment was adopted, today "the handgun [is] the quintessential self-defense weapon" and "a complete prohibition of their use is invalid";[4] and under the Commerce Clause, applying the critical phrase "Commerce . . . among the several States" to new forms of transportation and business.[5]

This term's decision in *Riley v. California*[6] charts the course for applying the Fourth Amendment's protection against unreasonable

* Partner, Mayer Brown LLP; counsel of record for briefs submitted for the Center for Democracy and Technology, the Electronic Frontier Foundation, and other parties in *United States v. Jones*; *Riley v. California* and *United States v. Wurie*; and *City of Ontario v. Quon*.

[1] Red Lion Broad. Co. v. FCC, 395 U.S. 367 (1969).

[2] Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622 (1994).

[3] Reno v. ACLU, 521 U.S. 844 (1997).

[4] District of Columbia v. Heller, 554 U.S. 570, 629 (2008).

[5] See, e.g., Gonzales v. Raich, 545 U.S. 1, 16 (2005) (observing that "in response to rapid industrial development and an increasingly interdependent national economy, Congress 'ushered in a new era of federal regulation under the commerce power,'" and that the Court's "understanding of the reach of the Commerce Clause . . . has evolved over time").

[6] 134 S. Ct. 2473 (2014).

government searches and seizures in the context of new technologies. The particular question here was whether the general rule that government agents do not need a warrant or any individualized suspicion to examine documents and other objects found on an individual placed under arrest—which courts have applied to things such as wallets, papers, purses, and cigarette packs—permits the government to examine all of the digitally stored information contained in a cell phone found on an arrestee.

Building upon several prior rulings, the Court refused simply to extend to this new technology the exception to the Fourth Amendment's general requirement of a warrant based on probable cause that had been developed in a pre-digital era. It instead examined the practical, real-world intrusion on long-standing legitimate privacy expectations that would result from taking that step and, finding a significant intrusion, held that the warrant requirement, rather than the less-protective standard developed for the pre-digital environment, should apply.

Riley's analytic framework is likely to be applied in a variety of different contexts, as new technologies collect and preserve personal information previously inaccessible to government agents. It will go a long way toward maintaining the Fourth Amendment's vitality as a bulwark for protecting individuals' privacy against the threat of unjustified government intrusion.

I. Fourth Amendment Background

The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The amendment's origins lie in one of the principal grievances of the Founding generation: "the reviled 'general warrants' and 'writs of assistance' . . ., which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity."[7]

[7] *Id*. at 2494.

General warrants were "not grounded upon a sworn oath of a specific infraction by a particular individual, and thus not limited in scope and application"—they permitted officers of the Crown to search anywhere and anyone they wished.[8]

Although a 1763 court ruling held general warrants unlawful in England,[9] Parliament expressly authorized their continued use in the colonies and "[g]eneral warrants and affiliated methods were still central to colonial search and seizure in 1776."[10] Opposition to these searches

> was in fact one of the driving forces behind the Revolution itself. In 1761, the patriot James Otis delivered a speech in Boston denouncing the use of writs of assistance. A young John Adams was there, and he would later write that "[e]very man of a crowded audience appeared to me to go away, as I did, ready to take arms against writs of assistance." According to Adams, Otis's speech was "the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born."[11]

Many of the states included prohibitions of general warrants in their constitutions, but there was concern following the Constitutional Convention that the new federal government was not subject to such a constraint. "Antifederalists sarcastically predicted that the general, suspicionless warrant would be among the Constitution's 'blessings.' . . . Patrick Henry warned that the new Federal Constitution would expose the citizenry to searches and seizures 'in the most arbitrary manner, without any evidence or reason.'"[12]

The Fourth Amendment "answered these charges" by adding to the Constitution a specific protection against the abuse represented

[8] Maryland v. King, 133 S. Ct. 1958, 1980 (2013) (Scalia, J., dissenting).

[9] Wilkes v. Wood, 98 Eng. Rep. 489, 499 (1763).

[10] William Cuddihy, The Fourth Amendment: Origins and Original Meaning 538 (2009). See generally Brief of Constitutional Accountability Center as Amicus Curiae Supporting Petitioner Riley and Respondent Wurie, Riley v. California, 134 S. Ct. 2473 (2014) (No. 13-132) (detailed discussion of Fourth Amendment's historical origin).

[11] Riley v. California, 134 S. Ct. at 2494.

[12] Maryland v. King, 133 S. Ct. at 1981 (Scalia, J., dissenting).

by general warrants. The amendment "protects individual privacy against certain kinds of governmental intrusion."[13]

The general principle established by the amendment is that government agents may not conduct a search without first obtaining a warrant, issued by a neutral magistrate based on a showing of probable cause to believe that the search will uncover evidence of crime and particularly delineating the scope of the search. But that general rule is subject to a raft of exceptions:

- Some government collections of information or things do not constitute a "search" and therefore do not trigger the amendment's protections,[14]
- Some categories of searches are permissible without any showing of a particularized justification for searching the individual or place, without a warrant, or without both;[15]
- Still other categories of searches may be undertaken on a showing of particularized justification less demanding than probable cause, such as "reasonable suspicion."[16]

This common-law elaboration of the Fourth Amendment's basic protection has been justified by the Supreme Court on the ground that"[t]he touchstone of the Fourth Amendment is reasonableness, and the reasonableness of a search is determined 'by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.'"[17] Faced with a particular factual setting, the Court considers the "totality of the

[13] Katz v. United States, 389 U.S. 347, 350 (1967).

[14] See, e.g., Illinois v. Caballes, 543 U.S. 405 (2005) (dog sniff); Maryland v. Macon, 472 U.S. 463 (1985) (items in plain view).

[15] See, e.g., Arizona v. Johnson, 555 U.S. 323 (2009) (pat-down of car occupants during a traffic stop permissible without suspicion of criminal activity); Skinner v. R. Labor Exec. Ass'n, 489 U.S. 602 (1989) (drug test of railroad workers following accidents); Payton v. New York, 445 U.S. 573 (1980) (warrant not required in exigent circumstances).

[16] See, e.g., New Jersey v. T.L.O., 469 U.S. 325 (1985) (search in the school context); Terry v. Ohio, 392 U.S. 1 (1968).

[17] United States v. Knights, 534 U.S. 112, 118-19 (2001) (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

circumstances" in determining whether the general Fourth Amendment standard, or some modified version, should apply.[18]

Changes in technology can have a significant impact on the "circumstances" that the Court considers in striking the appropriate balance under the Fourth Amendment. For example, the intrusion on individual privacy may be expanded if government agents use technology not contemplated at the time the Supreme Court determined that a particular factual setting should not be subject to the general warrant-supported-by-probable-cause standard. On the other hand, what is "needed for the promotion of legitimate government interests" can be affected by changes in technology that make it easier for wrongdoers to conceal their criminal activity.

The Court has grappled with these issues in a series of recent decisions, reflecting the dramatic advances in technology that are producing rapid, fundamental changes in every aspect of our lives—our ability to communicate, our work environment, our homes, our leisure. These rulings culminated in this term's decision in *Riley*, which emphatically reaffirmed the Court's determination to preserve the Fourth Amendment's core guarantee: protection against unreasonable government intrusion on individuals' privacy.

II. First Steps in Addressing New Technologies: *Kyllo*, *Jones*, and *King*

The impact of the Court's unanimous ruling in *Riley* cannot be understood without examining the Court's efforts to grapple with the intersection of new technology and the Fourth Amendment in three prior decisions, *Kyllo v. United States*,[19] *United States v. Jones*,[20] and *Maryland v. King*.[21]

A. Kyllo

Growing marijuana indoors generally requires high-intensity lights, which emit substantial amounts of heat. Agent William Elliott

[18] Ohio v. Robinette, 519 U.S. 33, 39 (1996) ("We have long held that the 'touchstone of the Fourth Amendment is reasonableness.' Reasonableness, in turn, is measured in objective terms by examining the totality of the circumstances.").

[19] 533 U.S. 27 (2001).

[20] 132 S. Ct. 945 (2012).

[21] 133 S. Ct. 1958 (2013).

of the U.S. Department of the Interior suspected that Danny Kyllo was growing marijuana in his apartment on Rhododendron Drive in Florence, Oregon. Agent Elliott, sitting in a car across the street from the apartment, scanned the exterior of Kyllo's apartment using a thermal imager, which detects infrared radiation invisible to the naked eye, converting the radiation "into images based on relative warmth—black is cool, white is hot, shades of gray connote relative differences; in that respect, it operates somewhat like a video camera showing heat images."[22] The scan indicated that the roof and wall of Kyllo's apartment were warmer than those of the neighboring apartments; Elliott obtained a search warrant based on that information and found 100 marijuana plants in Kyllo's apartment.

Did the thermal scan—undertaken without a warrant and without probable cause—constitute a search in violation of the Fourth Amendment?

Supreme Court precedent stated that the Fourth Amendment does not "require law enforcement officers to shield their eyes when passing by a home on public thoroughfares. Nor does the mere fact that an individual has taken measures to restrict some views of his activities preclude an officer's observations from a public vantage point where he has a right to be and which renders the activities clearly visible."[23] And that was true even when the "public vantage point" was an aircraft flying 1,000 feet or more over the defendant's property—whether the observation was made by naked eye[24] or a camera.[25]

As in those cases, Agent Elliott neither entered Kyllo's house nor used technology that physically intruded into the house, and four justices found that fact dispositive. Because "[a]ll that the infrared camera did in this case was passively measure heat emitted from the exterior surfaces of [Kyllo's] home," and that "information [was] exposed to the general public from the outside of petitioner's home," the "outside observation" principle could be applied to permit the use of this new technology.[26]

[22] Kyllo v. United States, 533 U.S. at 29–30.

[23] California v. Ciraolo, 476 U.S. 207, 213 (1986).

[24] *Id*. at 213–14.

[25] Dow Chem. Co. v. United States, 476 U.S. 227 (1986).

[26] Kyllo v. United States, 533 U.S. at 42–43 (Stevens, J., dissenting).

The majority, in an opinion by Justice Antonin Scalia, disagreed. Recognizing that it "would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology," the Court framed the question before it as whether there are "limits . . . upon this power of technology to shrink the realm of guaranteed privacy."[27]

With respect to the home, which the Court characterized as the "prototypical" private area that the Fourth Amendment was intended to protect, the Court held that there is a limit: "[w]here, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[28]

Key to this conclusion was the Court's recognition that technology will continue to advance. It pointed out that a "powerful directional microphone" could detect conversations inside a home, and "[t]he ability to 'see' through walls and other opaque barriers is a clear, and scientifically feasible, goal of law enforcement research and development."[29] The dissent's approach "would leave the homeowner at the mercy of advancing technology—including imaging technology that could discern all human activity in the home."[30]

Finally, the Court rejected the government's fallback suggestion of an "intimate details" test: thermal imaging would violate the Fourth Amendment only if personal information was revealed. In the home, the Court emphasized, "*all* details are intimate details, because the entire area is held safe from prying government eyes."[31]

More significantly, an "intimate details" test would not provide law enforcement officers with a "workable" standard. The Court "would have to develop a jurisprudence specifying which home activities are 'intimate' and which are not"; and in any event a government

[27] *Id*. at 33–34 (majority op.).

[28] *Id*. at 40; see also *id*. at 34 (observing that this test "assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted").

[29] *Id*. at 35 & 36 n.3.

[30] *Id*. at 35–36.

[31] *Id*. at 37 (emphasis in original).

agent could not know in advance whether his surveillance would pick up impermissible "intimate" details.[32]

Three elements of *Kyllo*'s analysis set the course for the Court's subsequent Fourth Amendment rulings addressing new technology. First, the refusal to apply mechanically to new technology a Fourth Amendment rule developed before the advent of that technology. The Court squarely rejected the government's attempt to shoehorn thermal imaging under the legal standard for unaided visual observation based on the "no physical intrusion" standard that justified the pre-technology rule.

Second, the importance of examining the practical effect on individuals' privacy interests of the new technology, and of future advances in the area, both in general and in terms of the reduction in the protection of privacy interests that would result from mechanically applying the pre-technology legal standard in this new context. Critical to the Court's decision was its determination regarding the range of previously unavailable information that government agents would be able to obtain through thermal imaging—and other similar technologies, both in existence and under development—if the "no physical intrusion" standard were applied.

Third, the refusal to adopt a Fourth Amendment standard turning on the type of information uncovered by the government search, because that approach would be difficult for law enforcement officers to apply and would have as its practical consequence a significant diminution in the scope of Fourth Amendment protection. The government's "intimate details" test would have opened the door to widespread use of thermal imaging, with its consequent diminution of individuals' ability to maintain a private sphere free from government intrusion. The government simply would have been precluded from utilizing evidence gained from such intrusions on the basis of an after-the-fact "intimacy" analysis.

B. Jones

Following suspects—in the hope that they will take actions that reveal their culpability, or lead police to evidence of crime or to co-conspirators—has long been a staple of law enforcement. Under the principle that "[w]hat a person knowingly exposes to the public . . .

[32] *Id*. at 38–39.

is not a subject of Fourth Amendment protection,"[33] tailing suspects on foot could not implicate the Fourth Amendment's protections.[34]

But what if the government agent's ability to monitor a suspect is augmented by technology? The Supreme Court first addressed that issue in 1983 in the context of a "beeper."[35]

Tristan Armstrong had been purchasing large amounts of chloroform, and police believed he was using the substance to manufacture illegal drugs. They accordingly placed a beeper in a drum of chloroform—with the permission of the seller—and the drum was sold to Armstrong. Following the drum's progress through visual surveillance combined with monitoring the electronic signal emitted by the beeper (including use of a helicopter to find the beeper signal after it was lost), the police traced the drum to a cabin owned by Leroy Knotts. Obtaining a search warrant based in part on the presence of the drum, they found equipment and chemicals sufficient to produce large quantities of amphetamine.

The Court rejected Knotts's argument that the use of the beeper to track the chloroform to his cabin and confirm that the drum had come to rest on his property constituted a search triggering the Fourth Amendment. The critical question was whether the officers' monitoring of the drum's movements intruded on a reasonable expectation of privacy. Holding that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another," the Court stated that traveling over public streets "voluntarily conveyed to anyone who wanted to look the fact that [the driver] was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property."[36]

The use of the beeper did not warrant a different result, because the Fourth Amendment did not "prohibit[] the police from augmenting the sensory faculties bestowed upon them at birth with

[33] Katz v. United States, 389 U.S. at 351.

[34] See United States v. Lee, 274 U.S. 559, 563 (1927) (use of searchlight or binoculars to enhance officer's visual observation does not constitute a search under the Fourth Amendment).

[35] United States v. Knotts, 460 U.S. 276 (1983).

[36] *Id*. at 281–82.

such enhancement as science and technology afforded them in this case."[37] The defendant argued that a ruling in favor of the government would mean "that 'twenty-four hour surveillance of any citizen of this country will be possible, without judicial knowledge or supervision,'" but the Court declined to base its decision on that mere possibility.[38] "[I]f such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."[39]

The Court's ruling in *Knotts* was influenced by the limited impact of the technology—although the beeper enhanced the ability of the police to track the drum, it was far from foolproof: the signal had been lost for approximately one hour. Indeed, the Court compared the beeper to a police officer's use of a searchlight or binoculars. And although the Court wrote broadly in some parts of the opinion, it was careful to limit its ruling to the "enhancement [that] science and technology afforded . . . *in this case*" and to leave open the possibility that "dragnet-type law enforcement practices" could produce a different result.[40]

That circumstance was presented for decision in 2012, when the Court—in *United States v. Jones*—addressed a Fourth Amendment challenge to the use by government agents of a Global Positioning System (GPS) tracking device to monitor with precision the movements of a vehicle over a four-week period.

The principal opinion in *Jones* did not turn on the nature of GPS tracking technology. Instead, the Court held that the physical intrusion on private property resulting from the government's installation of the GPS device on the car constituted a "search" triggering the Fourth Amendment's warrant requirement.

But four justices rejected that rationale, concluding instead that it was the characteristics of GPS technology, as applied in this case, that led to an outcome opposite from *Knotts*. And Justice Sonia Sotomayor agreed with that conclusion as well as the physical-intrusion rationale.

[37] *Id*. at 282.

[38] *Id*. at 283.

[39] *Id*. at 284.

[40] *Id*. at 282 (emphasis added).

As she explained, GPS surveillance is "unique" because it "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. The Government can store such records and efficiently mine them for information years into the future."[41] Moreover, "GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously."[42]

Justice Samuel Alito, in his concurring opinion for himself and Justices Ruth Bader Ginsburg, Stephen Breyer, and Elena Kagan, framed the issue more broadly:

> In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional surveillance for any extended period of time was difficult and costly and therefore rarely undertaken. The surveillance at issue in this case—constant monitoring of the location of a vehicle for four weeks—would have required a large team of agents, multiple vehicles, and perhaps aerial assistance.[43]

For these justices, the critical question was whether—notwithstanding *Knotts*'s conclusion that an individual had no legitimate expectation of privacy in his movements on public roads—the gathering of precise, detailed information about a person's movements, not possible in the pre-computer age, did intrude on such a legitimate expectation. They concluded that it did: "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every

[41] United States v. Jones, 132 S. Ct. at 955–56. Amicus briefs explained that the precise, detailed records produced by GPS tracking, which can be produced around the clock for long periods of time, can be combined with information regarding the businesses at locations visited by the vehicle being tracked, to identify intimate details of a person's life. For example, the fact that a tracked car suddenly began stopping at an oncologist's office several times a month could reveal that a member of the family had cancer. The buildings that a person regularly visits could reveal his or her religious or political affiliations. See, e.g., amicus briefs filed by the Center for Democracy and Technology; ACLU; and Yale Law School Information Society Project Scholars.

[42] United States v. Jones, 132 S. Ct. at 956.

[43] *Id*. at 963.

single movement of an individual's car for a very long period"—and four weeks exceeded the permissible period.[44]

The analysis employed by these justices, and by Justice Sotomayor, paralleled the Court's approach in *Kyllo*. They refused the government's invitation simply to extend *Knotts* to this new and very different technology and instead reviewed the characteristics of GPS technology and assessed the impact of the government's use of that technology on individuals' privacy expectations pre-dating the development of the new technology. In view of the significant intrusion on those expectations, they concluded that the use of the technology constituted a search.

Indeed, the difference in result between *Jones* and *Knotts* rests principally on the different real-world impact of the two technologies. Justice Alito's opinion in *Jones* expressly recognizes that the detailed, long-term surveillance that GPS makes "easy and cheap" would "have been exceptionally demanding" to accomplish using a beeper. [45] For example, "[t]he signal had a limited range and could be lost if the police did not stay close enough"—limitations inapplicable to GPS.[46]

The Court's next decision involving new technology and the Fourth Amendment, *Maryland v. King*, confirms this conclusion. The Court followed the course charted in *Kyllo* and the *Jones* concurring opinions, but the government side prevailed because the Court's assessment of the real-world impact of the new technology found little or no erosion of legitimate, pre-existing privacy interests.

C. King

DNA technology plays an important role in identifying those responsible—and not responsible—for crime. The Supreme Court has acknowledged its "unparalleled ability both to exonerate the wrongly convicted and to identify the guilty. It has the potential to

[44] *Id*. at 964. See also *id*. at 956 (Sotomayor, J., concurring) ("I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on").

[45] *Id*. at 964 & 963 n.10.

[46] *Id*. at 963 n.10.

significantly improve both the criminal justice system and police investigative practices."[47]

To help realize these benefits, the federal government has sponsored creation of a nationwide database of DNA profiles provided by local, state, and national laboratories based on samples collected from convicted offenders and, in some circumstances, from arrestees. The question in *Maryland v. King* was whether the Fourth Amendment permits the collection and analysis of DNA samples from arrestees in the absence of a warrant based on individualized probable cause.

The Court divided 5-4 on the issue, with Justice Scalia writing an emphatic dissent on behalf of himself and Justices Ginsburg, Sotomayor, and Kagan. The majority, applying the general standard of reasonableness—"weigh[ing] 'the promotion of legitimate governmental interests' against 'the degree to which [the search] intrudes upon an individual's privacy'"[48]—concluded that a warrant is not required and that collecting and analyzing arrestees' DNA does not violate the Fourth Amendment.

On the government interest side of the ledger, the Court cited the "need for law enforcement officers in a safe and accurate way to process and identify the persons and possessions they must take into custody."[49] And "a suspect's criminal history is a critical part of his identity that officers should know when processing him for detention," which is why fingerprints are routinely obtained and compared with databases of known criminals and unsolved crimes.[50] "[T]he only difference between DNA analysis and the accepted use of fingerprint databases is the unparalleled accuracy DNA provides."[51]

By comparison, "the intrusion of a cheek swab to obtain a DNA sample is a minimal one" and "[t]he expectations of privacy of an individual taken into police custody 'necessarily [are] of a diminished scope.'"[52] Moreover, the processing of the DNA sample was structured to prevent disclosure of the arrestee's genetic traits, and

[47] Dist. Attorney's Office v. Osborne, 557 U.S. 52, 55 (2009).

[48] Maryland v. King, 133 S. Ct. at 1970 (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

[49] *Id.*

[50] *Id.* at 1971.

[51] *Id.* at 1972.

[52] *Id.* at 1977, 1978.

statutory protections barred use of a sample for purposes other than identifying individuals. The Court specifically observed that use of samples "to determine an arrestee's predisposition for a particular disease or other hereditary factors not relevant to identity" would "present additional privacy concerns not present here."[53]

In these circumstances, the Court concluded, obtaining the DNA sample from an arrestee "is, like fingerprinting and photographing, a legitimate police booking procedure that is reasonable under the Fourth Amendment."[54]

The difference in outcome between this case and *Kyllo* and *Jones* stems directly from the Court's analysis of the nature of the information gained through DNA analysis. Because the new technology was simply a more accurate means of ascertaining the arrestee's identity and prior criminal history—and did not reveal other types of personal information—the Court concluded that additional Fourth Amendment protection was not warranted.

III. *Riley* Reaffirms the Fourth Amendment's Vitality

The Supreme Court has long held that the Fourth Amendment permits government agents to search individuals placed under arrest without first obtaining a warrant and without probable cause to believe that the search would uncover evidence of crime. This "search incident to arrest" exception has been applied by courts to permit a search of the arrestee's person and of the area within the arrestee's immediate control.[55]

That is, if documents or other objects are discovered on the arrestee's person or within his or her control, the police are permitted to examine them. As the Supreme Court explained in upholding the search of a cigarette pack found in the course of a search incident to arrest, "[h]aving in the course of a lawful search come upon the crumpled package of cigarettes, [the officer] was entitled to inspect it."[56]

[53] *Id.* at 1979.

[54] *Id.* at 1980.

[55] Riley v. California, 134 S. Ct. at 2483–84. See also Arizona v. Gant, 556 U.S. 332, 343 (2009); United States v. Robinson, 414 U.S. 218, 235–36 (1973); Chimel v. California, 395 U.S. 752, 762–63 (1969).

[56] United States v. Robinson, 414 U.S. at 236.

But what if the object discovered on the arrestee's person is not a wallet or a cigarette pack, but instead a smartphone or a tablet or a thumbdrive? May the government "inspect" all of the digitally stored information, without obtaining a warrant, by invoking the search-incident-to-arrest exception? That is the question that the Court addressed this term in *Riley*. And the answer is a resounding "no."

The Court granted review in two cases presenting the same question regarding cell phone searches. David Riley was arrested on a firearms offense; an officer searched him incident to the arrest and found a cell phone in his pocket. Accessing the phone's digital memory, the officer found words that he believed stood for a criminal gang. During a subsequent examination of the phone at the police station, a detective found photographs of Riley standing in front of a car that had been involved in a shooting.

Riley was charged under California law in connection with the shooting and the charge included an enhancement based on his alleged involvement with a criminal street gang. He moved to suppress the evidence obtained in the searches of his phone, but the motion was denied on the ground that the warrantless search was permissible under the search-incident-to-arrest exception. The California appellate court affirmed that determination on the basis of a California Supreme Court decision holding that the digital content of a cell phone could be examined as part of a search incident to arrest.[57]

Brima Wurie, the defendant in the second case, was arrested on a drug charge, and the police seized two cell phones. One of the phones received calls from a source that the phone's screen identified as "my house." The officers opened the phone, accessed its call log, identified the phone number associated with "my house," and—using an online directory—ascertained its location. Upon arriving at the building, they saw through a window a woman who resembled someone in a photograph on Wurie's phone. Based on this information, the police obtained a warrant authorizing a search of the apartment; they seized illegal drugs, firearms, and drug paraphernalia.

Wurie was charged with drug and firearms violations and moved to suppress the evidence obtained in the search of the apartment on

[57] People v. Riley, No. D059840, 2013 WL 475242 (Cal. App. 4th Dist. Feb. 8, 2013).

the ground that it was the product of an unconstitutional search of his cell phone. The trial court denied the motion, but the U.S. Court of Appeals for the First Circuit reversed, holding that the search of a cell phone could not be justified under the search-incident-to-arrest exception.

The Supreme Court began its analysis by observing that a "mechanical application" of the search-incident-to-arrest principle could justify the searches in these cases. But, the Court said, "neither of its rationales has much force with respect to digital content on cell phones."[58]

Searches incident to arrest are justified by the interest in police safety, but "[d]igital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer. . . . Once an officer has secured a phone and eliminated any potential physical threats, . . . data on the phone can endanger no one."[59]

The second interest justifying the exception is preventing destruction of evidence. Again, however, "[o]nce law enforcement officers have secured a cell phone, there is no longer any risk that the arrestee himself will be able to delete incriminating data from the phone."[60]

The Court observed, however, that the search-incident-to-arrest exception also rests on "an arrestee's reduced privacy interests upon being taken into police custody. . . . [A] patdown of [the arrestee's] clothing and an inspection of the cigarette pack found in his pocket constituted only minor additional intrusions compared to

[58] Riley v. California, 134 S. Ct. at 2484.

[59] *Id*. at 2485.

[60] *Id*. at 2486. California and the United States argued strenuously that the threat of remote wiping—receipt by the phone of a signal erasing the stored data—justified an immediate search to prevent destruction of evidence. But the Court pointed out that this argument was distinct from the concern expressed in prior cases, because it did not relate to the potential acts of the arrestee but rather "turns on the actions of third parties who are not present at the scene of arrest." *Id*. Moreover, there was no evidence that the problem is prevalent; it was not clear that permitting searches at the time of arrest would address the problem, because officers preoccupied with securing the arrestee and the scene would be delayed in turning their attention to the contents of a cell phone; and a phone could be turned off or isolated from radio waves (through placement in a "Faraday bag"—a simple aluminum bag or wrapping named for the scientist William Faraday). *Id*. at 2486–87.

the substantial government authority exercised in taking [him] into custody."[61]

That diminished privacy interest did not mean that "the Fourth Amendment falls out of the picture entirely."[62] The Court had previously held that an arrest does not permit a warrantless search of the arrestee's home, because it could not "join in characterizing the invasion of privacy that results from a top-to-bottom search of a man's house as 'minor.'"[63]

The government argued that a search of the data stored on a cell phone was "materially indistinguishable" from the search of a wallet, address book, or purse when the latter are found on an arrestee. But the Court squarely rejected that mechanistic approach:

> Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse. A conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom.[64]

The Court then turned to the inquiry that was dispositive in *Kyllo* and in the *Jones* concurrences: whether extending an existing legal rule (here, the search-incident-to-arrest exception) to encompass a new technology would undermine previously existing, legitimate privacy expectations. It surveyed the characteristics of digital information stored on cell phones—based in large part on discussions in amicus briefs submitted by organizations with expertise in technology and privacy.[65]

The Court focused principally on cell phones' "immense storage capacity."[66] Before the development of digital storage technology, "a search of a person was limited by physical realities and tended as

[61] *Id*. at 2488.

[62] *Id*.

[63] Chimel v. California, 395 U.S. at 766–67 n.12.

[64] Riley v. California, 134 S. Ct. at 2488–89.

[65] See, e.g., amicus curiae briefs filed by the Center for Democracy and Technology and Electronic Frontier Foundation; the Electronic Privacy Information Center, et al.; the National Association of Criminal Defense Lawyers et al.; and the ACLU et al.

[66] Riley v. California, 134 S. Ct. at 2489.

a general matter to constitute only a narrow intrusion on privacy. Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read."[67]

Digital storage means that "the possible intrusion on privacy is not [so] physically limited."[68] Cell phones have the capacity to store "millions of pages of text, thousands of pictures, or hundreds of videos"; moreover, the types of information preserved can include "photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on."[69]

The Court found that these capabilities had "several interrelated consequences for privacy":

- "[A] cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal more in combination than any isolated record" and a large volume of even one type of information will "convey more than previously possible" about the individual;
- The information "can date back to purchase of the phone, or even earlier"—"[a] person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone";
- Digitally stored information has "an element of pervasiveness" that does not characterize physical records, because "[p]rior to the digital age, people did not typically carry a cache of sensitive information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception";
- Some types of data stored on phones are "qualitatively different" from physical records: internet browsing history, which can "reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease"; GPS-generated location data, which "can reconstruct someone's specific movements down to the minute, not only around town but also within a

[67] *Id.*

[68] *Id.*

[69] *Id.*

> particular building"; and mobile applications, which "together can form a revealing montage of the user's life."[70]

"Allowing the police to scrutinize such records on a routine basis," the Court said, "is quite different from allowing them to search a personal item or two in the occasional case."[71] Indeed, the Court pointed out that its search-incident-to-arrest precedent distinguished between an impermissible warrantless search of the arrestee's house and a permissible warrantless search of what might be found in the arrestee's pockets, because of the significantly reduced intrusion on privacy in the latter situation. But if "the arrestee's pockets contain a cell phone, that is no longer true."[72] The Court explained that

> a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.[73]

In light of this very substantial difference in the impact on legitimate privacy expectations, compared with the effect of the search-incident-to-arrest exception as applied to physical records, the Court held—unanimously—that the exception does not apply to digitally stored information contained in a device seized in the course of an arrest, and that government agents must obtain a warrant to conduct such a search.

The Court distinguished its prior decision in *King* by pointing to the recognition in that case that "when 'privacy-related concerns are

[70] *Id*. at 2488–89. The Court pointed out another attribute of cell phones: a cell phone user may not know whether information being accessed through the phone is stored on the device or on a remote server. Thus, although the government conceded that the search-incident-to-arrest doctrine could not be used to search files stored remotely, "officers searching a phone's data would not typically know whether the information they are viewing was stored locally at the time of arrest or has been pulled from" a remote server. *Id*. at 2491. It concluded that "[t]he possibility that a search might extend well beyond papers and effects in the physical proximity of an arrestee is yet another reason that the privacy interests here dwarf those" in prior cases. *Id*.

[71] *Id*. at 2490.

[72] *Id*. at 2491.

[73] *Id*. (emphasis in original).

weighty enough' a 'search may require a warrant notwithstanding the diminished expectations of privacy of the arrestee.'"[74] The vast quantity and numerous different types of personal information revealed by searching the digital contents of a cell phone were dramatically different from the one kind of information—identity—revealed by the DNA sample.

The Court rejected a number of arguments advanced by the federal government and the State of California, reaffirming the conclusion that the substantial and varied information contained in cell phones (and other devices with digital storage capability) renders inapplicable legal standards developed in other contexts.

For example, the federal government urged the Court to import into the cell phone context a Fourth Amendment rule governing searches of automobiles, which permits officers to search an automobile incident to an arrest if it is "'reasonable to believe evidence relevant to the crime of arrest might be found in the vehicle.'"[75] That rule, however, was expressly tied to "circumstances unique to the vehicle context"—in particular "'a reduced expectation of privacy' and 'heightened law enforcement needs' when it comes to motor vehicles," due to their mobility.[76]

Not only do "cell phone searches bear neither of these characteristics," but such a rule would provide "no practical limit at all when it comes to cell phone searches" because of the comprehensive nature of the data stored on them, compared with the relatively limited material likely to be found in a car.[77] It therefore "would in effect give 'police officers unbridled discretion to rummage at will among a person's private effects.'"[78]

California argued that officers should be permitted to search cell phone data when they would have been able to examine a physical counterpart: because an address book found on the arrestee could be searched, the theory went, the police should be able to search a digital phone book. But that argument ignored the comprehensive nature of digitally stored data: "the fact that a search in the pre-digital

[74] *Id.* at 2488.

[75] Arizona v. Gant, 556 U.S. at 343.

[76] Riley v. California, 134 S. Ct. at 2492.

[77] *Id*.

[78] *Id*.

era could have turned up a photograph or two in a wallet does not justify a search of thousands of photos in a digital gallery."[79] Moreover, such a standard would lead to difficult line-drawing by police and judges: "Is an e-mail equivalent to a letter? Is a voicemail equivalent to a phone message slip?"[80]

The Court recognized its ruling would hamper to some degree government's ability to fight crime. But "[p]rivacy comes at a cost."[81]

Of course the Court's decision did not ban searches of digitally stored information, but only required government agents to obtain a warrant. Advances in technology have made that process easier for the police, with requests sent via email and processed electronically by judges.

Finally, other exceptions to the warrant requirement—such as the rule that police may proceed without a warrant when confronting particular "exigent circumstances"—will enable government agents to search a cell phone if necessary to "prevent the imminent destruction of evidence in individual cases, to pursue a fleeing suspect, and to assist persons who are seriously injured or are threatened with imminent injury."[82] Critically, however, the police will have to establish that "an emergency justified a warrantless search in each particular case"[83]—a significant difference from the across-the-board exemption that would have resulted from extension of the search-incident-to-arrest rule to digitally stored information.

The Court ended its opinion with a flourish, revisiting the Fourth Amendment's origins; in particular, the general warrants that outraged the Founding generation. Modern cell phones, the Court said, "hold for many Americans 'the privacies of life,'" and permitting government agents to search them without a warrant would allow government to exercise the very arbitrary authority that the amendment was intended to prevent.[84] "The fact that technology now allows an individual to carry such information in his hand does not

[79] *Id*. at 2493.

[80] *Id*.

[81] *Id*.

[82] *Id*. at 2494.

[83] *Id*.

[84] *Id*. at 2494–95.

make the information any less worthy of the protection for which the Founders fought."[85]

Riley establishes a clear paradigm for application of the Fourth Amendment to new technology:

- Courts should not mechanically extend exemptions from the warrant requirement recognized in the pre-digital era to encompass information resulting from new technology.
- Instead, a court must (1) determine whether the rationale justifying the rule developed with respect to physical information makes sense in the context of the new technology; and (2) examine the real-world effect on individuals' privacy expectations of extending the rule to the new technology.
- If the rationale makes no sense or the impact on privacy expectations would be substantial, then the exemption should not be extended and government agents should be required to obtain a warrant.
- New exclusions from the warrant requirement that lack significant constraints on officer discretion, and would give government agents access to significant amounts of personal information previously protected by the warrant requirement, should not be recognized.

By refusing to accept the very substantial erosion of protection against government power that would have resulted from turning a blind eye to the real-world impact of reflexively combining old legal rules with new technologies, the Court's decision lays an excellent foundation for ensuring that the Fourth Amendment's protections remain real and vital in our age of advancing technology.

IV. What's Next?

Riley addressed digitally stored information on a cell phone, but it is difficult to see how a different result could possibly apply to searches incident to arrest of the contents of tablets, laptops, or thumb

[85] *Id*. at 2495.

drives. All share the characteristics relied on by the *Riley* Court, and a warrant therefore should be required to conduct such searches.[86]

Moreover, we will not have to wait long to see how *Riley*'s approach will be applied outside the search-incident-to-arrest context. Federal and state governments have argued in a variety of other contexts that other exemptions from the warrant requirement should be applied to permit searches of digital information. Most of those arguments are likely to suffer the same fate as they did in *Riley*, as lower courts follow the Supreme Court's lead and focus broadly on practical realities and not simply on legal tests developed in the pre-digital era. Three examples demonstrate *Riley*'s impact.

A. Email Messages

Americans conduct personal business using email accounts provided by a third party: an employer; a school; or an email service provider, such as Gmail, Hotmail, or Yahoo. All of these third parties reserve the right to access the content of emails sent by their users. Does that mean that the government may obtain any email messages that it wishes, without obtaining a warrant?

The answer depends on the scope of a Fourth Amendment principle known as the "third-party doctrine," which holds that "'[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.'" The Supreme Court in 1976 applied this principle to conclude that an individual has no legitimate expectation of privacy with respect to checks, account statements, and other financial information in the possession of his banks, because it was "information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business. . . . The [customer] takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[87]

[86] Information-collecting sensors—one example is the increasingly ubiquitous "Fitbit" device that monitors an individual's movements and could, for example, record data indicating that the wearer was likely involved in a physical altercation—should fall within the same category. Government prosecutors might try to argue that sensors collecting a single category of information should not be encompassed under *Riley*'s rationale, but the comprehensive nature of that information, and the fact that it previously has been unavailable to government agents, fit well within *Riley*, as well as the approach taken by *Kyllo* and the *Jones* concurrences.

[87] United States v. Miller, 425 U.S. 435, 442–43 (1976).

Three years later, the Court held that the same rationale precluded Fourth Amendment protection for telephone numbers dialed by an individual: "When he used his phone, [the individual] voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed."[88]

Government lawyers have been arguing that this rationale precludes Fourth Amendment protection for the content of email messages because the email provider—whether employer, commercial service, or otherwise—always reserves the right to access messages to detect abuse of the service or other wrongful activity and, sometimes, for other purposes.

Yet the Supreme Court has refused one invitation to extend the third-party doctrine to digital messages. *City of Ontario v. Quon*,[89] decided in 2010, involved a suit under 42 U.S.C. § 1983 alleging that the plaintiffs—police officers employed by the city—suffered a violation of their Fourth Amendment rights when their supervisors read messages sent via a city-provided pager and disciplined the officers for use of the pager for inappropriate personal messages. The court of appeals held that the officers had a reasonable expectation of privacy in the text messages and that the city's review of the messages violated the Fourth Amendment.

The city and the federal government urged the Supreme Court to hold that the Fourth Amendment did not apply at all, because the officers had no legitimate expectation of privacy in the messages on the ground that the city's policy stated that pager messages were not private and could be accessed by city officials. The Court declined to rest its decision on that ground, because "[a] broad holding concerning employees' privacy expectations vis-à-vis employer-provided technological equipment might have implications for future cases that cannot be predicted."[90] It therefore assumed that the employees had a reasonable expectation of privacy, but held that the warrantless search fell within a previously recognized exception to

[88] Smith v. Maryland, 442 U.S. 735, 744 (1979).

[89] 560 U.S. 746 (2010).

[90] *Id*. at 760.

the warrant requirement based on the "special needs" of the government workplace.[91]

The Court explained its decision by pointing to "[r]apid changes in the dynamics of communication and information transmission" affecting "what society accepts as proper behavior."[92] For example, "many employers expect or at least tolerate personal use of such equipment by employees because it often increases worker efficiency" and "some States have recently passed statutes requiring employers to notify employees when monitoring their electronic communications."[93] "At present," the Court said, "it is uncertain how workplace norms, and the law's treatment of them, will evolve."[94]

Justice Sotomayor made the same point in her concurring opinion in *Jones*, stating that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach 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" such as sending emails or visiting websites.[95]

More fundamentally, inviting friends into my home does not vitiate my expectation of privacy vis-à-vis government agents. They still must obtain a warrant if they wish to search the premises. Why then should sharing my private information with individuals or businesses that I select vitiate my expectation of privacy as against the government? To be sure, those individuals or businesses could choose to provide government with the information voluntarily—my decision to share the information creates that risk (just as an individual invited into my home could choose to describe its contents, or events transpiring there, to government agents). But the decision to share the information should not relieve the government of the need to obtain a warrant if neither I nor the individuals I have taken into my confidence are willing to provide it to the government voluntarily.

One court of appeals addressed this issue—pre-*Riley*—in the email message context, and concluded that a warrant is required to permit

[91] *Id*.

[92] *Id*. at 759.

[93] *Id*.

[94] *Id*.

[95] United States v. Jones, 132 S. Ct. at 957.

the government to access the content of email messages. The Sixth Circuit's analysis in *United States v. Warshak*[96] largely anticipated the Supreme Court's approach in *Riley*.

The court of appeals first observed that—in the absense of consent or some other generally applicable exception—the government is obliged to obtain a warrant in order to access the content of old-technology private communications, in the form of telephone conversations and letters. Failing to extend the warrant requirement to email communications would mean that "the Fourth Amendment would prove an ineffective guardian of private communications, an essential purpose it has long been recognized to serve. As some forms of communication begin to diminish, the Fourth Amendment must recognize and protect nascent ones."[97] In the terms used by the Supreme Court in *Riley*, failing to recognize a reasonable expectation of privacy would significantly erode the privacy protection previously provided by the Fourth Amendment, in light of the then-existing technology.

The Sixth Circuit went on to reject the government's reliance on the third-party doctrine—which was based on the internet service provider's right to access the email messages. It held that a right of access is insufficient to eliminate a reasonable expectation of privacy, pointing out that tenants have a privacy expectation in their apartments notwithstanding the landlord's reservation of a right of access. And the bank records case was distinguishable in that the information was "conveyed to the bank so that the bank could put [it] to use 'in the ordinary course of business,'" while the internet service provider was "an *intermediary*, not the intended recipient of the emails."[98]

As in *Riley*, the court of appeals rejected a mechanical application of the pre-existing standard, focusing instead on whether the rationale underlying the third-party principle applied in this very different context. Concluding that it did not, and that applying the third-party principle would significantly intrude on legitimate expectations of privacy, the court instead concluded that the general requirement of a warrant should govern.

[96] 631 F.3d 266 (6th Cir. 2010).

[97] *Id*. at 286.

[98] *Id*. at 288 (emphasis in original).

Warshak's analysis seems likely to be accepted, not simply for email service providers, but also for personal information in email accounts provided by employers, schools, and others—at least in the absence of an extraordinarily clear warning by the account provider that the email account may not be used for personal purposes. And it is also likely to apply to other categories of information stored by increasingly ubiquitous cloud service providers; for example, calendars, documents, and photographs.

B. Cell Phone Location Information

Cell phone service providers maintain "cell site location information"—a record of calls made by the customer and of the particular cell tower that carried the call to or from the customer. Because the cell tower used will normally be the one closest to the customer, and the location information often includes the customer's location vis-à-vis the tower, it is possible to use this information to identify the customer's movements over a long period of time.

Several courts of appeals have addressed whether the government must obtain a warrant in order to access this information, reaching conflicting results.[99] All of these decisions pre-date *Riley*, however.

Under a *Riley* analysis, the threshold question is whether an individual has a legitimate expectation of privacy in information regarding his location. The concurring opinions in *Jones* indicate that the answer to that question is likely "yes." Although the cell tower information is not as accurate as GPS tracking, it nonetheless provides a highly detailed picture of an individual's movements—the very information that the concurring justices found protected in *Jones*.

In the cell tower context, however, the government argues that this location information has been "shared" with the cell phone service provider—indeed, it is embodied exclusively in the service provider's records—and that the third-party doctrine therefore precludes protection under the Fourth Amendment. But the overwhelming majority of customers are unaware that these data are collected and maintained by cell companies; a customer therefore "has not voluntarily

[99] See United States v. Davis, 754 F.3d 1205 (11th Cir. 2014); In re Application of the United States, 724 F.3d 600, 615 (5th Cir. 2013); In re Application of the United States, 620 F.3d 304 (3d Cir. 2010).

disclosed his cell site location information to the provider in such a fashion as to lose his reasonable expectation of privacy."[100]

Given the ubiquity of cell phones, a contrary result would give government agents an easy way to obtain comprehensive location information regarding virtually any American—something that government agents could not do before the advent of this technology. In the terms used in *Riley*, failing to recognize a legitimate expectation of privacy would produce a very substantial diminution of the privacy protection that Americans previously enjoyed.

As Professor Orin Kerr has pointed out, however, recognizing a protectable Fourth Amendment interest in this information collected by a private party is not compelled by any existing Supreme Court decision.[101] Here, however, the customer plays an essential role in enabling collection of the information (the customer's phone sends the signal to the tower)—and that involvement should supply the essential link.

One final issue: a federal statute (the Stored Communications Act) requires the government to obtain an order from a magistrate based upon a showing of reasonable grounds to believe that the information is relevant and material to an ongoing criminal investigation.[102] Although this standard is less demanding than probable cause, it does impose a limit on law enforcement officers.

Justice Alito in both *Jones* and *Riley* expressed the view that determinations by Congress and state legislatures regarding the appropriate standards for reconciling privacy interests and law enforcement needs would be more appropriate than leaving those questions "primarily to federal courts using the blunt instrument of the Fourth Amendment."[103]

[100] United States v. Davis, 754 F.3d at 1215–16.

[101] O. Kerr, DoJ Petitions for Rehearing in Eleventh Circuit Cell-Site Case, The Volokh Conspiracy (Aug. 1, 2014), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/08/01/doj-petitions-for-rehearing-in-eleventh-circuit-cell-site-case.

[102] 18 U.S.C. § 2703(d) (2011).

[103] Riley v. California, 134 S. Ct. at 2497; see also United States v. Jones, 132 S. Ct. at 963–64.

C. Border Searches of Digitally Stored Information

Another area of Fourth Amendment controversy involving digitally stored information involves searches at the border. As a general matter, the federal government has extremely broad authority to conduct searches of people and things entering the United States:

> Since the founding of our Republic, Congress has granted the Executive plenary authority to conduct routine searches and seizures at the border, without probable cause or a warrant, in order to regulate the collection of duties and to prevent the introduction of contraband into this country. [The Supreme] Court has long recognized Congress' power to police entrants at the border. . . . "'Import restrictions and searches of persons or packages at the national border rest on different considerations and different rules of constitutional law from domestic regulations. The Constitution gives Congress broad comprehensive powers "[t]o regulate Commerce with foreign Nations." Historically, such broad powers have been necessary to prevent smuggling and to prevent prohibited articles from entry.'"[104]

Does that mean that a customs officer may search all of the digitally stored data on the cell phone, tablet, or laptop computer of an individual entering the country without a warrant and without any individualized suspicion?

The U.S. Court of Appeals for the Ninth Circuit addressed that question in *United States v. Cotterman* and rejected the government's argument that no individualized suspicion was required to justify such a search at the border.[105] It held, however, that the Fourth Amendment requires only a showing of "reasonable suspicion," as opposed to the probable cause generally needed to justify a search.

The Supreme Court has applied a reasonable suspicion requirement in the context of the extended detention *of an individual*.[106] It has not been receptive to limits on the government's authority with respect to property, rejecting the argument that a reasonable suspicion showing was necessary to permit the government to remove a car's gas tank.[107]

[104] United States v. Montoya de Hernandez, 473 U.S. 531, 537–38 (1985).

[105] 709 F.3d 952 (9th Cir. 2013) (en banc).

[106] United States v. Montoya de Hernandez, 473 U.S. at 540–41.

[107] See, e.g., United States v. Flores-Montano, 541 U.S. 149 (2004).

For these reasons, it is not clear whether the significant impact on privacy interests recognized in *Riley* will be sufficient to require a showing of individualized suspicion for border searches of digitally stored information.

* * *

Evolving technology is certain to provide courts with a steady diet of questions regarding the appropriate scope of Fourth Amendment rules developed in earlier eras. With its decision in *Riley*, the Supreme Court has charted a course for addressing these questions that promises to ensure that this vital protection remains meaningful, continuing to safeguard Americans' privacy against arbitrary invasion through abuse of government power.