Article

City of Los Angeles v. Patel: The Upcoming Supreme Court Case No One Is Talking About

Adam Lamparello[1]

I. INTRODUCTION 135

II. A SPLIT AT THE FEDERAL LEVEL 141
A. *ACLU v. Clapper*: The Third-Party Doctrine is Alive and Well in the Digital Era 145
B. Other Decisions at the Federal and State Level 148

III. *CITY OF LOS ANGELES V. PATEL*: THE COURT SHOULD LIMIT *SMITH V. MARYLAND* AND MODIFY THE THIRD-PARTY DOCTRINE 153

IV. CONCLUSION 160

I. INTRODUCTION

The United States Supreme Court recently granted certiorari in *City of Los Angeles v. Patel*[2] to consider whether §41.49 of the Los Angeles Municipal Code violates the Fourth Amendment. Section 41.49 permits law enforcement to conduct warrantless and suspicionless inspections of a hotel owner's guest registry without judicial oversight. A guest registry includes:

---

[1] Assistant Professor of Law, Indiana Tech Law School.
[2] 738 F.3d 1058 (9th Cir. 2013).

> The guest's name and address; the number of people in the guest's party; the make, model, and license plate number of the guest's vehicle if the vehicle will be parked on hotel property; the guest's date and time of arrival and scheduled date of departure; the room number assigned to the guest; the rate charged and the amount collected for the room; and the method of payment.[3]

The Ninth Circuit Court of Appeals correctly held that hotel owners have a reasonable expectation of privacy in their guest registries, and that the lack of judicial oversight could lead to unreasonable infringements on the privacy rights of hotel owners.[4]

But the Ninth Circuit erred when it held that hotel *guests* have no expectation of privacy in the guest registries. The Ninth Circuit based this part of its holding on the third-party doctrine, which states that individuals forfeit privacy protections when they voluntarily submit information to a third party.[5] Federal and state courts are split regarding the continued viability of the third-party doctrine, particularly in an era when technological advances have allowed law enforcement and government officials to track a suspect's location with a GPS device, collect cell phone metadata, and monitor an individual's Google search history, all without a warrant.

This Article argues that the Supreme Court should reject or at least modify the third-party doctrine in *Patel* to reflect threats to privacy posed in the digital era. The Ninth Circuit in *Patel* did not.[6] The Court's holding may have profound implications on the constitutionality of the government's surveillance programs, including its ability to collect cell phone metadata without a warrant or probable cause.[7] Simply put, the constitutionality of section 41.49 can—and should—lead to a principled and much needed shift in favor of stronger privacy protections.

The problem with the third-party doctrine, particularly in the digital era when the line between public and private space is collapsing,

---

[3] *Id.* at 1062.

[4] *Id.* at 1065.

[5] *See, e.g.*, United States v. Miller, 425 U.S. 435, 443 (1976) (holding that individuals have no reasonable expectation of privacy in financial records given to a bank teller); Smith v. Maryland, 442 U.S. 735, 742 (1979) (holding that an individual has no reasonable expectation of privacy in outgoing calls made from a private residence).

[6] 738 F.3d at 1064; *see also* Sherry F. Colby, *Third-Party Searches*, DORF ON LAW (Nov. 12, 2014), http://www.dorfonlaw.org/2014/11/third-party-searches.html, <http://perma.cc/4W29-C489> (discussing the *Patel* case and stating that the third-party doctrine should be reconsidered).

[7] The government's metadata collection program tracks outgoing calls from cell phones, but does not typically record the subscriber's name, address, or other identifying information, which can be accessed only by a showing of reasonable suspicion that the caller is associated with a terrorist group or engaged in criminal conduct. *See* ACLU v. Clapper, 959 F. Supp. 2d 924, 951 (E.D.N.Y. 2013) (stating that "when [the Government] makes a query, it only learns the telephony metadata of the telephone numbers within three "hops" of the "seed." Third, without resort to additional techniques, the Government does not know who any of the telephone numbers belong to. In other words, all the Government sees is that telephone number A called telephone number B.").

is that once an individual voluntarily conveys data to a third party, he or she surrenders *all* privacy protections in that data, regardless of who accesses the data, and irrespective of the purpose for which that access is given. In the pre-digital era, this ordinarily meant that when an individual provided a bank teller with confidential financial information, the individual waived any privacy rights in that information with respect to employees at the bank or government officials who were conducting a criminal or regulatory investigation.[8]

In the digital era, the third-party doctrine means something different, because the scope of the privacy waiver is far more significant. Outgoing cell phone calls can be tracked at any time—without a warrant or any suspicion of wrongdoing—by the government through the subscriber's carrier. Likewise, an individual's search history on Google is subject to monitoring by the government.[9] Thus, the sheer volume of information that the government can uncover in connection with its wide-ranging surveillance program casts doubt on the principle that citizens should lose *all* privacy rights in information merely because they sign a contract with a cell phone service provider or decide to conduct online research.

Admittedly, the administrative search exception to the Fourth Amendment is a well-settled doctrine that allows state and government officials to conduct warrantless searches of records that employers in highly regulated industries are required by law to maintain.[10] This exception is intended to give law enforcement sufficient latitude to ensure that businesses serving the general public, such as restaurants and health care facilities, comply with health and safety codes.[11] When law enforcement searches a hotel guest registry, or when the government tracks cell phone metadata, the purpose is to search for evidence of criminal and terroristic activity, which in most cases requires individualized suspicion. Moreover, these searches are often conducted in a broad and indiscriminate manner. To make matters even worse, they typically reveal the names, location, outgoing call logs, and internet

---

[8] *See Miller*, 425 U.S. at 442–43 (noting that the expressed purpose of the Bank Secrecy Act is to require records to be maintained because they "have a high degree of usefulness in criminal tax, and regulatory investigations and proceedings") (quoting 12 U.S.C. §1829b(a)(1)); *see also* Klayman v. Obama, 957 F. Supp. 2d 1, 33 (D.D.C. 2013) ("The Supreme Court itself has long-recognized a meaningful difference between cases in which a third party collects information and then turns it over to law enforcement, and cases in which the government and the third party create a formalized policy under which the service provider collects information for law enforcement purposes.") (citing *Ferguson v. Charleston*, 532 U.S. 67 (2001).

[9] *See* Catilin Dewey, *The NSA May Be Reading Your Searches But Your Local Police Probably Aren't*, WASH. POST, Aug. 3, 2013, http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/03/the-nsa-might-be-reading-your-searches-but-your-local-police-probably-arent/, <http://perma.cc/G6XF-4NRS>.

[10] *Fourth Amendment—Administrative Searches and Seizures*, 69 J. CRIM. L. & CRIMINOLOGY 552, 553 (1978).

[11] *Id.*

search history of unsuspecting citizens.[12] Together, the third-party doctrine and administrative search exception can easily become a one-two punch that strikes a significant blow at the heart of basic privacy protections.

This is not to say that the third-party doctrine should be abandoned entirely, or that the voluntary disclosure of data to third parties has no legal significance. Rather, it is to say that there should be limits on the type of information third parties can access, the circumstances in which third parties can monitor data that would otherwise be private, and the level of suspicion required before companies such as Verizon or AT&T must surrender their subscribers' call histories, among other things.

After all, limits on the third-party doctrine exist in a variety of contexts. For example, when an individual walks into her neighborhood pharmacy and gives the pharmacist a prescription, the law regulates the circumstances in which the prescription information may be disclosed to third parties.[13] Although state and government officials are permitted by law to inspect a pharmacy's records, including its history of dispensing controlled substances, the purpose of the inspection provisions is to ensure compliance with applicable laws that are designed to prevent prescription drug abuse.[14] Given the documented history of such abuse in the United States and the failure of some pharmacies to comply with federal law, these disclosures further the state's interest in protecting the health and safety of its citizens. Furthermore, warrantless searches of these records are typically limited to circumstances where the government's purpose is to "identify or locate a suspect, fugitive, witness, or missing person,"[15] when a crime is committed on the premises, or when there is a "medical emergency in connection with a crime."[16] Simply put, these laws do not allow government officials to go on a fishing expedition.

On the other hand, indiscriminately collecting metadata, monitoring internet search history, or sifting through hotel guest registries can be just that—a fishing expedition. The government's commonly articulated purpose for collecting such information—national security—is certainly valid, but it should not countenance a government dragnet that delves into the lives of millions of citizens for the sole purpose of finding a few

---

[12] *See* Dewey, *supra* note 9.

[13] *See generally* Sherry L. Green, HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPPA) PRIVACY RULE AND PRESCRIPTION DRUG MONITORING PROGRAMS (PMPS) (Nat'l Alliance for Model State Drug Laws 2010), http://www.namsdl.org/library/80E22BDA-19B9-E1C5-319D10D2D8989B6C/, <http://perma.cc/G3YS-YJVA> (discussing the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and explaining the circumstances when disclosure is mandated by law).

[14] *Id.*

[15] *See FAQ on Government Access to Medical Records*, AMERICAN CIVIL LIBERTIES UNION (May 30, 2003), https://www.aclu.org/technology-and-liberty/faq-government-access-medical-records, <https://perma.cc/9CNR-XJ33> (discussing 45 C.F.R. § 164.512(f)(2002)).

[16] *Id.*

bad apples. The Fourth Amendment's particularity requirement exists for a reason: to prevent the "reviled 'general warrants' and 'writs of assistance' of the colonial era."[17] This is precisely why the third-party doctrine, as currently applied by the courts, is ill-suited to the digital era: it provides law enforcement with almost limitless authority to monitor citizens' private lives, including where we travel, who we call, and what we search for on the internet. Indeed, the scope of the third-party doctrine in the digital age is the issue lurking underneath the surface in *Patel*—and it has the potential to affect privacy rights in a variety of contexts.

Even if the Supreme Court wants to sidestep the third-party doctrine in *Patel*, it will, at the very least, indirectly confront the issue; the Ninth Circuit expressly stated that the doctrine was still valid law.[18] Thus, if the Court's holding is narrow and confined to the hotel owner's expectation of privacy in a guest registry, one can assume that the third-party doctrine remains good law in its current form. If the Court confronts the third-party doctrine directly, the Justices will have the power to strengthen privacy protections by establishing principled limits on the warrantless collection of information, such as cell phone metadata. Conversely, the Court's decision has the potential to place law enforcement's investigatory powers—and the government's interest in national security—above privacy rights. This would lead to a weakening of the Fourth Amendment.

Put bluntly, *Patel* is the case no one is talking about, but the case may—and likely will—affect every citizen, including any Justice of the Supreme Court who decides to stay at a hotel in Los Angeles or call a loved one from a cell phone. After all, if the Court reverses the Ninth Circuit, thereby permitting law enforcement officers to enter hotels and discover the names of hotel guests, their room numbers, their license plate numbers, and the duration of their stay, then the government will almost certainly be permitted to track the outgoing calls from a smartphone.

This Article argues that the Court should partially affirm the Ninth Circuit's decision, which would invalidate section 41.49 on Fourth Amendment grounds,[19] but reverse the portion of its decision reaffirming the third-party doctrine. Specifically, the Court should modify the third-party doctrine by adopting the standard suggested by Justice Alito in

---

[17] *Riley*, 134 S. Ct. at 2492.

[18] *See Patel*, 738 F.3d at 1062 ("To be sure, the *guests* lack any privacy interest of their own in the hotel's records.").

[19] *See* U.S. CONST. amend. IV ("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."). As discussed below, over the years the Court has created numerous exceptions to the warrant and probable cause requirements, thus making it easier for law enforcement to conduct searches and seizures.

United States v. Jones,[20] which asks whether a particular search exceeds society's expectations for how the police would investigate a specific crime.[21] In doing so, the Court should hold, as it did in *Jones* and *Riley v. California*,[22] that factors such as the length and intrusiveness of the search, the quality and quantity of data collected, and the level of suspicion required are all relevant to the societal expectation of privacy.

This approach would not require the Court to overrule *Smith v. Maryland*[23] and *United States v. Miller*,[24] which reaffirmed the third-party doctrine. However, it would import much needed limitations in situations where individuals voluntarily convey information to a third party without the expectation that this disclosure will entitle anyone to access and monitor such information. As it stands now, law enforcement officers can enter a hotel lobby and demand to see the names, room numbers, and license plate numbers of every guest staying at the establishment. They can also seek out information regarding when each guest checked in, when they intended to leave, and the people who were staying with them. This makes the Fourth Amendment—and by extension, privacy rights—seem like little more than an aspirational and unenforced principle. The relationship between citizens and their civil liberties should not be so strained.

Part II of this Article surveys case law, analyzing the constitutionality of the government's metadata collection program and highlighting two recent decisions that arrived at opposite conclusions. In *Klayman v. Obama*,[25] the United States District Court for the District of Columbia invalidated the government's metadata collection program on Fourth Amendment grounds, holding that the third-party doctrine was ill-suited to the digital age.[26] In *ACLU v. Clapper*,[27] the United States District Court for the Southern District of New York reached the opposite result, applying the third-party doctrine to hold that citizens waive any expectation of privacy with respect to information that is voluntarily shared with a third party.[28] These cases, as well as others decided at the state and federal level, reveal deep divisions within the courts that concern the balance between privacy rights and the need to afford the government sufficient flexibility in adopting measures that will prevent acts of terrorism.

Part III analyzes *Patel*, and argues that it provides the Court with an

---

[20] 132 S. Ct. 945 (2012) (holding that the use of a GPS tracking device to monitor a suspect's whereabouts for twenty-eight days violated the Fourth Amendment).

[21] *See id.* at 964 (Alito, J., concurring).

[22] 134 S. Ct. 2473 (2014) (holding that, in the absence of exigent circumstances, law enforcement officers may not search an arrestee's cell phone without a warrant and probable cause).

[23] 442 U.S. 735 (1979).

[24] 425 U.S. 435 (1976).

[25] 957 F. Supp. 2d 1 (D.D.C. 2013).

[26] *Id.* at 37.

[27] 959 F. Supp. 2d 724 (E.D.N.Y. 2014).

[28] *Id.* at 751.

ideal opportunity in which to modify the third-party doctrine to account for the serious threats to privacy posed in the digital era. In addition, Part III sets forth a workable framework within which to protect privacy rights, while giving law enforcement and the Government sufficient flexibility to investigate criminal behavior.

II. A SPLIT AT THE FEDERAL LEVEL

At the federal level, courts are split regarding the continued viability of the third-party doctrine and whether the government's metadata collection program is constitutional. In *Klayman*, for example, the district court held that the NSA's metadata collection program constituted a search under the Fourth Amendment.[29] In doing so, the district court refused to apply *Smith*, emphasizing the differences between pen registers and metadata.[30] In *Clapper*, however, the Eastern District of New York reached the opposite result, applying *Smith*, and held that citizens have no reasonable expectation of privacy in the numbers dialed from a cell phone.[31] *Klayman* and *Clapper* underscore the divergent views that exist among federal courts, the confusion that *Smith* has created among the lower courts, and the need for the Supreme Court to intervene and provide doctrinal guidance.

In *Klayman*, the United States District Court for the District of Columbia held that the National Security Agency's ("NSA") surveillance program, which consisted of the indiscriminate, suspicionless collection of cell phone metadata, likely constituted a search under the Fourth Amendment.[32] The court rejected the rationale in *Smith*, stating that "citizens' phone habits"[33] have become "thoroughly unlike those considered by the Supreme Court thirty-four years ago [in *Smith*]."[34] Indeed, the government's "almost-Orwellian technology"[35] was "unlike anything that could have been conceived in 1979,"[36] when *Smith* was decided. That is precisely the point. Times have changed, and so must the courts. As explained below, *Klayman* embraced a view of privacy—

---

[29] *Klayman*, 957 F. Supp. 2d at 36–37.
[30] *Id.* at 37.
[31] *See Clapper*, 959 F. Supp. 2d at 752.
[32] *See, e.g.*, Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN, June 5, 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order, <http://perma.cc/DF7J-2KXT>. The public became aware of the NSA program from leaks of classified material by Edward Snowden, a former employee of the NSA. Initial media reports suggested that, on April 15, 2013, the Foreign Intelligence Surveillance Court (FISC) issued an order, dated April 25, 2013, ordering Verizon Business Services to produce to the NSA all call detail records for telephone metadata.
[33] *Klayman*, 975 F. Supp. 2d at 31.
[34] *Id.*
[35] *Id.* at 33.
[36] *Id.*

and particularity under the Fourth Amendment—that the pre-digital age precedent could not have foreseen, and that the Supreme Court should adopt.

The court in *Klayman* reasoned that, because "people in 2013 have an entirely different relationship with phones than they did thirty-four years ago,"[37] the Government's "metadata collection and analysis almost certainly does violate a reasonable expectation of privacy."[38] The court rejected the government's argument that *Smith* "squarely control[s]"[39] cell phone searches. In *Smith*, the Court held that law enforcement could install a pen register to track the numbers dialed from a suspect's phone.[40] There was no reasonable expectation of privacy in the dialed numbers because they were "voluntarily transmitted . . . to his phone company"[41] and because "it is generally known that phone companies keep such information in their business records."[42]

The collection of cell phone metadata, however, involves novel issues that could not have been contemplated by courts decades ago. To begin with, the government's surveillance capabilities, coupled with "citizens' phone habits, and the relationship between the NSA and telecom companies,"[43] have become "unlike those considered by the Supreme Court thirty-four years ago [in *Smith*]."[44] Put differently, "the Court in *Smith* was not confronted with the NSA's Bulk Telephony Metadata program,"[45] and could not "have ever imagined [in 1979] how the citizens of 2013 would interact with their phones."[46]

For example, unlike a pen register, which was "operational for only a matter of days," the "NSA telephony metadata program . . . involves the creation and maintenance of a historical database for *five years'* worth of data."[47] Furthermore, in *Smith*, law enforcement installed a pen register to "record the numbers dialed from the [suspect's] telephone,"[48] whereas the NSA program collects "*on a daily basis* [from telecommunications service providers] electronic copies of call detail records, or telephony metadata."[49] In other words, *Smith* involved the targeting of an individual suspect, which "in no way resembles the daily, all-encompassing, indiscriminate dump of phone metadata that the NSA

---

[37] *Id.* at 36.
[38] *Id.* at 32.
[39] *Klayman*, 975 F. Supp. 2d at 30 (internal quotation marks omitted).
[40] *Id.*
[41] *Id.*
[42] *Id.*
[43] *Id.* at 31.
[44] *Id.*
[45] *Klayman*, 975 F. Supp. 2d at 32.
[46] *Id.*
[47] *Id.* (emphasis in original).
[48] *Id.*
[49] *Id.* (internal quotation marks omitted) (emphasis in original).

now receives as part of its . . . Metadata Program."[50] As the court explained, it is "one thing to say that people expect phone companies to occasionally provide information to law enforcement"[51] but "quite another to suggest that our citizens expect all phone companies to operate . . . a joint intelligence gathering operation with the government."[52]

To be sure, the "almost-Orwellian technology that enables the Government to store and analyze the phone metadata of every telephone user in the United States is unlike anything that could have been conceived in 1979."[53] As the court recognized, "[t]he notion that the Government could collect similar data on hundreds of millions of people . . . for a five-year period . . . was at best, in 1979, the stuff of science fiction."[54] To make matters worse, the government uses "the most advanced twenty-first century tools,"[55] to "proceed surreptitiously,"[56] thus circumventing the "ordinary checks that constrain abusive law enforcement practices."[57]

Lastly, "not only is the Government's ability to collect, store, and analyze phone data greater now than it was in 1979, but the nature and quantity of the information contained in . . . metadata is much greater."[58] The court held as follows:

> Cell phones have also morphed into multi-purpose devices. They are now maps and music players . . . . They are cameras . . . . They are even lighters that people hold up at rock concerts . . . . They are ubiquitous as well. Count the phones at the bus stop, in a restaurant, or around the table at a work meeting or any given occasion. Thirty-four years ago [when *Smith* was decided], *none* of those phones would have been there . . . . [Instead], city streets were lined with pay phones . . . when people wanted to send "text messages," they wrote letters and attached postage stamps.[59]

Of course, while metadata itself has not changed over time,[60] it can, unlike thirty-four years ago, "reveal the user's location."[61]

Also, the "ubiquity of [cell] phones has dramatically altered the

---

[50] *Klayman*, 975 F. Supp. 2d at 33.
[51] *Id.*
[52] *Id.*
[53] *Id.*
[54] *Id.*
[55] *Id.*
[56] *Klayman*, 975 F. Supp. 2d at 33 (internal citation omitted).
[57] *Id.*
[58] *Id.* at 33–34.
[59] *Id.* at 34–35 (internal citations omitted).
[60] *Id.* at 35.
[61] *Id.* at 35 n.57.

quantity of information that is now available and . . . what the information can tell the Government about people's lives."[62] For example, people "send text messages now that they would not (really *could not*) have made or sent back when *Smith* was decided."[63] In fact, text messaging has become "so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification."[64] This reflects a "rapid and monumental shift towards a cell-phone-centric culture,"[65] in which metadata from each person's phone reveals "a wealth of detail about her familial, political, professional, religious, and sexual associations."[66] As the Supreme Court held in *City of Ontario v. Quon*,[67] this "might strengthen the case for an expectation of privacy."[68] That expectation is compromised when "the Government, without any basis whatsoever to suspect them of any wrongdoing, collects and stores for five years their telephony metadata for purposes of subjecting it to high-tech querying and analysis without case-by-case judicial approval."[69]

Klayman's analysis is significant in several respects. First, the individual's expectation of privacy was predicated on the scope, breadth, and duration of the government's intrusion, not whether the place itself was public or private, or whether the information was sufficiently personal to establish an objective expectation of privacy. In *Jones*, the Supreme Court adopted a similar view, holding that law enforcement's use of a "GPS device to track a suspect's movement for nearly a month violated Jones's reasonable expectation of privacy."[70] The *Jones* Court explained that, while "relatively short-term monitoring of a person's movements on public streets"[71] is permissible, "the use of longer-term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[72] Although, in *United States v. Maynard*,[73] the District of Columbia Circuit held that, while a person "traveling in an automobile on public thoroughfares has no reasonable expectation of

---

[62] *Klayman*, 957 F. Supp. 2d at 35–36 (emphasis in original).
[63] *Id.* at 36 (emphasis in original).
[64] *Id.* (quoting City of Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010)).
[65] *Klayman*, 957 F. Supp. 2d at 3621.
[66] *Id.* (quoting United States v. Jones, 132 S. Ct. 945 at 955–56 (2012) (Sotomayor, J., concurring)).
[67] 130 S. Ct. 2619 (2010).
[68] *Id.* at 2630.
[69] *Klayman*, 957 F. Supp. 2d at 22.
[70] *Id.* at 17 (citing *Jones*, 132 S. Ct. at 955–56 (Sotomayor, J., concurring)); *cf. Jones*, 132 S. Ct. at 962 (Alito, J., concurring) (stating that advances in technology may require individuals to "reconcile themselves" to the "inevitable diminution of privacy that new technology entails").
[71] *Jones*, 132 S. Ct. at 964 (Alito, J., concurring).
[72] *Id.* (internal citations omitted). The plurality and concurring opinions in *Jones* highlight the Justices' preferences for either a "reasonable expectation of privacy" theory, or a trespass theory. Thus, several Justices in *Jones* followed Fourth Amendment construct that was based on physical space. *Id.*
[73] 615 F.3d 544 (D.C. Cir. 2010).

privacy in his movements from one place to another,"[74] it does not mean that "such a person has no reasonable expectation of privacy in his movements whatsoever, without end, as the Government would have it."[75]

In addition, *Klayman* implicitly recognized that voluntary disclosure of information to a third party does not automatically extinguish an individual's expectation of privacy, nor does it render the government's sweeping surveillance program exempt from Fourth Amendment scrutiny.[76] Although citizens consciously decide to transmit personal information via a cell phone and know that it can be shared with third parties, they do so because of the ubiquity, affordability, and efficiency of this highly advanced method of communication. They do not simultaneously give the government consent to monitor their outgoing calls for whatever reason it pleases and for however long it desires.[77]

It should not matter that the government's metadata program consists only of reviewing outgoing call logs and does not reveal the user's identity. The government has the power—with no warrant and no suspicion of criminal activity—to review telephone numbers and make subjective determinations concerning which numbers create reasonable suspicion that an individual may be associated with terrorist activity. When that determination is made, the government need only have a magistrate sign off on an order that will reveal the user's identity. It is far too easy for the government to circumvent Fourth Amendment protections, in the same manner that section 41.49 gives law enforcement officers *carte blanche* to discover the names of every guest staying at hotels in Los Angeles.[78]

A. *ACLU v. Clapper:* The Third-Party Doctrine is Alive and Well in the Digital Era

In *Clapper*, the district court came to the opposite conclusion, relying largely on the third-party doctrine to hold that "individuals have no 'legitimate expectation of privacy' regarding the telephone numbers they dial because they knowingly give that information to telephone

---

[74] *Id.* at 557.

[75] *Id.* (distinguishing United States v. Knotts, 460 U.S. 276 (1983)) (holding that the use of a tracking beeper did not constitute a search where an individual was traveling from one place to another on a public thoroughfare).

[76] *See Klayman*, 957 F. Supp. 2d at 9.

[77] *See generally* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005 (2010) (discussing the particularity requirement in the context of internet searches).

[78] L.A., CAL., MUN. CODE § 41.49 (2008).

companies when they dial a number."[79] The district court held that "an individual has no legitimate expectation of privacy in information provided to third-parties,"[80] and relied on *Smith* to reject the notion that citizens retain any privacy interest in records voluntarily disclosed to third parties;

> The privacy concerns at stake in *Smith* were far more individualized . . . . *Smith* involved the investigation of a single crime and the collection of telephone call detail records collected by the telephone company at its central office, examined by the police, and related to the target of their investigation, a person identified previously by law enforcement. . . . Nevertheless, the Supreme Court found there was no legitimate privacy expectation because "[t]elephone users . . . typically know that they must convey numerical information to the telephone company; that the telephone company has facilities for recording this information; and that the telephone company does in fact record this information for a variety of legitimate business purposes."[81]

Much like a hotel registry, cell phone metadata records "are created and maintained by the telecommunications provider . . . that distinction is critical because when a person voluntarily conveys information to a third party, he forfeits his right to privacy in the information."[82]

The district court also rejected the notion that the government's analysis of metadata can "reveal a person's religion, political associations, use of a telephone-sex hotline, contemplation of suicide, addiction to gambling or drugs, experience with rape, grappling with sexuality, or support for particular political causes."[83] The court stated:

> First, without additional legal justification—subject to

---

[79] *Clapper*, 959 F. Supp. 2d at 749 (quoting *Smith*, 442 U.S. at 742) (stating that "telephone customers have no subjective expectation of privacy in the numbers they dial because they convey that information to the telephone company knowing that the company has facilities to make permanent records of the numbers they dial").

[80] *Id.* (referencing generally, *Smith*, 442 U.S.).

[81] *Id.* at 750 (referencing *Smith*, 442 U.S. at 743 (citing United States v. Reed, 575 F.3d 900, 914 (9th Cir. 2009) ("[Because] data about the 'call origination, length, and time of call'. . . is nothing more than pen register and trap and trace data, there is no Fourth Amendment 'expectation of privacy.'")) (internal citations omitted).

[82] *Clapper*, 959 F. Supp. 2d at 751 (holding that "the Government's . . . querying of . . . telephony metadata does not implicate the Fourth Amendment any more than a law enforcement officer's query of the FBI's fingerprint or DNA databases to identify someone. In the context of DNA querying, any match is of the DNA profile and like telephony metadata additional investigative steps are required to link that DNA profile to an individual"). *Id.* at 751–52 (citing Maryland v. King, 133 S. Ct. 1958, 1963–64 (2013)).

[83] *Clapper*, 959 F. Supp. 2d at 750 (quoting Decl. of Edward Felten, Professor of Computer Science and Public Affairs, Princeton University, ¶ 42 (ECF No. 27)); *see also* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012) (discussing the mosaic theory, which "considers whether a set of nonsearches aggregated together amount to a search because their collection and subsequent analysis creates a revealing mosaic").

> rigorous minimization procedures—the NSA cannot even query the telephony metadata database. Second, when it makes a query, it only learns the telephony metadata of the telephone numbers within three "hops" of the "seed." Third, without resorting to additional techniques, the Government does not know who any of the telephone numbers belong to. In other words, all the Government sees is that telephone number A called telephone number B. It does not know who subscribes to telephone numbers A or B. Further, the Government repudiates any notion that it conducts the type of data mining the ACLU warns about in its parade of horribles.[84]

The district court acknowledged that "less intrusive means to collect and analyze telephony metadata could be employed," but noted that the Supreme Court has "repeatedly refused to declare that only the 'least intrusive' search practicable can be reasonable under the Fourth Amendment."[85] Furthermore, the district court was unmoved by the sheer breadth of the Government's metadata collection program, holding that "the collection of breathtaking amounts of information unprotected by the Fourth Amendment does not transform that sweep into a Fourth Amendment search."[86]

Likewise, the district rejected the argument that the Court's decision in *United States v. Jones*, which held that law enforcement's use of a GPS tracking device to monitor a vehicle's location for four weeks, violated the Fourth Amendment and implicated the government's metadata collection policies. Noting that "the Supreme Court did not overrule *Smith*,"[87] the district court stated that "the 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."[88] To be sure, the majority's holding was based on a trespass theory, because by placing the GPS device on the vehicle, "[t]he Government physically occupied private property for the purpose of obtaining information."[89]

---

[84] *Clapper*, 959 F. Supp. 2d at 750–51.

[85] *Id.* at 751 (stating that "judicial-Monday-morning-quarterbacking 'could raise insuperable barriers to the exercise of virtually all search-and-seizure powers,' because judges engaging in after-the-fact evaluations of government conduct 'can almost always imagine some alternative means by which the objectives might have been accomplished'") (quoting City of Ontario, Cal. v. Quon, 130 S. Ct. 2619 at 2632 (citing Vernonia School Dist. 47J v. Acton, 115 S. Ct. 2386, 2396 (1995)) (internal quotations and citations omitted).

[86] *Clapper*, 959 F. Supp. 2d at 752 (citing United States v. Dionisio, 410 U.S. 1, 13 (1973)) (holding that, where a grand jury subpoena did not constitute unreasonable seizure, it was not rendered unreasonable simply because many citizens were "subjected to the same compulsion"); In re Grand Jury Proceedings: Subpoenas Duces Tecum, 827 F.2d 301, 305 (8th Cir. 1987) (holding that a grand jury "'dragnet' operation" does not necessarily violate the Fourth Amendment) (internal citation omitted).

[87] *Clapper*, 959 F. Supp. 2d at 752.

[88] *Id.* (quoting Agostini v. Felton, 521 U.S. 203, 237 (1997)).

[89] *Id.* (quoting *Jones*, 132 S. Ct. at 949 ("Such a physical intrusion would have been considered a

With respect to metadata, the issue does not concern a physical intrusion or even implicate the Fourth Amendment because "a subscriber has no legitimate expectation of privacy in telephony metadata created by third parties."[90]

Finally, the district court rejected the reasoning in *Klayman*, holding that, "[w]hile people may 'have an entirely different relationship with telephones than they did thirty-four years ago' . . . their relationship with their telecommunications providers has not changed and is just as frustrating."[91] Furthermore, "what metadata is has not changed over time," and the information being collected by the Government is limited to "[tele]phone numbers dialed, date, time, and the like."[92] Thus, although cell phones "have far more versatility now than when *Smith* was decided,"[93] it does not undermine "the Supreme Court's finding that a person has no subjective expectation of privacy in telephony metadata."[94] Ultimately, the district's decision came down to a single proposition: "Because *Smith* controls, the NSA's bulk telephony metadata collection program does not violate the Fourth Amendment."[95]

B. Other Decisions at the Federal and State Level

The majority of courts at the federal and state levels have upheld the constitutionality of the government's metadata collection program on the grounds than an individual has no expectation of privacy in cell phone metadata. In *United States v. Skinner*,[96] the Sixth Circuit held that a defendant had no reasonable expectation of privacy "in the data given off by his voluntarily procured pay-as-you-go cell phone."[97] The court also emphasized the fact that the defendant voluntarily disclosed the cell phone data on a public highway.[98]

'search' within the meaning of the Fourth Amendment when it was adopted.")).

[90] *Id.* (citing *Smith*, 442 U.S. at 744–45).

[91] *Clapper*, 959 F. Supp. 2d at 752 (quoting *Klayman*, 957 F. Supp. 2d at 36); *see also Reed*, 575 F.3d at 914 (finding that because "data about the 'call origination, length, and time of call . . . . is nothing more than pen register and trap and trace data, there is no Fourth Amendment 'expectation of privacy'") (internal citation omitted).

[92] *Clapper*, 959 F. Supp. 2d at 752 (quoting *Klayman*, 957 F. Supp. 2d at 35).

[93] *Id.*

[94] *Id.* (citing *Smith*, 442 U.S. at 745) ("The fortuity of whether or not the [tele]phone company in fact elects to make a quasi-permanent record of a particular number dialed does not . . . make any constitutional difference. Regardless of the [tele]phone company's election, petitioner voluntarily conveyed to it information that it had facilities for recording and that it was free to record.").

[95] *Id.*

[96] 690 F.3d 772 (6th Cir. 2012).

[97] *Id.* at 777.

[98] *Id.* at 781.

On the other hand, the Sixth Circuit recognized that the government's argument was "strengthened by the fact that the authorities sought court orders to obtain information on [the suspect's] location from the GPS capabilities of his cell phone."[99] Likewise, in *In re Smartphone Geolocation Data Application*,[100] the Eastern District of New York held that an individual has no expectation of privacy regarding cell phone data because of the knowledge that such data may be disclosed to third parties:

> [I]t is clearly within the knowledge of cell phone users that their telecommunications carrier, smartphone manufacturers and others are aware of the location of their cell phone at any given time. After all, if the phone company could not locate a particular cell phone, there would be no means to route a call to that device, and the phone simply would not work. Given the notoriety surrounding the disclosure of geolocation data . . . cell phone users cannot realistically entertain the notion that such information would (or should) be withheld from federal law enforcement agents searching for a fugitive. . . . [I]ndividuals who do not want to be disturbed by unwanted telephone calls at a particular time or place simply turn their phones off, knowing that they cannot be located.[101]

In *United States v. Caraballo*,[102] the United States District Court for the District of Vermont suggested that an individual's expectation of privacy in cell phone data location may hinge on whether the disclosure of such data occurred "in the ordinary course of providing cellular phone service."[103] In *Caraballo*, the data was obtained by "pinging" the defendant's cell phone, which was a "special, surreptitious procedure not available to the general public, initiated solely by law enforcement, [and] without notice or any other volitional activity by the Defendant other than having his phone in the 'on mode.'"[104] Thus, the district court distinguished *Smith* and *Miller* because pinging was not "part and parcel of the provision of cellular phone service."[105] The court declined, however, to resolve the "thorny question of whether an individual *generally* maintains a subjective expectation of privacy in his or her real-time location data where that information is obtained exclusively through

---

[99] *Id.* at 779.
[100] 977 F. Supp. 2d 129.
[101] *Id.* at 146; *see also* Application of the United States of America for Historical Cell Site Data, 724 F.3d 600, 611–13 (5th Cir. 2013) (noting that by expressly agreeing to provider's privacy policies, cell phone users cede any expectation of privacy for cell cite data).
[102] 963 F. Supp. 2d 341, 360 (D. Vt. 2013).
[103] *Id.*
[104] *Id.*
[105] *Id.*

pinging,"[106] because the government's conduct fell within the exigent circumstances exception.

In *In re Application of the Federal Bureau of Investigation*,[107] the United States Foreign Surveillance Court upheld the government's metadata collection program and reaffirmed the third-party doctrine's core principle that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[108] The doctrine applies regardless of the "disclosing person's assumptions or expectations with respect to what will be done with the information following its disclosure."[109]

Furthermore, the disclosing party has no "reasonable expectation with respect to how the government will use or handle the information after it has been divulged by the recipient."[110] The court also emphasized that the cell phone data does not reveal "subscriber[s'] names or addresses or other identifying information,"[111] and can only be "accessed for analytical purposes after [the] NSA has established a reasonable articulable suspicion . . . that the number to be used to query the data—the 'seed'—is associated with one of the terrorist groups listed in the Order."[112] Consequently, these safeguards undermine the assertion that metadata collection is sufficiently intrusive to raise Fourth Amendment concerns.[113] The court held that *Jones* was largely irrelevant because the Court's decision was predicated on a trespass theory and never discussed the issue of whether individuals have a reasonable expectation of privacy in terms of cell phone metadata.

These decisions rely not only on the third-party doctrine, but on cases such as *United States v. Knotts*,[114] which emphasized the physical space in which the search occurred.[115] In *Knotts*, the Supreme Court held that the use of a beeper to monitor a suspect's location and activities did not violate the Fourth Amendment, because the form of surveillance was akin to "following of an automobile on public streets and highways,"[116] where an individual has a diminished expectation of privacy. By the same token, the *Knotts* Court acknowledged that the owner of the cabin where the defendant was traveling did have an expectation of privacy within the cabin, thus limiting law enforcement's surveillance to the period when the defendant was traveling in his automobile.[117] Similarly,

---

[106] *Id.*
[107] No. BR 14-01, 2014 WL 5463097 (Foreign Intell. Surveillance Ct., March 20, 2014).
[108] *Id.* at *6 (quoting Smith, 442 U.S. at 743–44).
[109] *Id.* (quoting *Smith*, 442 U.S. at 744).
[110] *Id.* at *7.
[111] *Id.* at *8.
[112] *Id.*
[113] *Id.*
[114] 460 U.S. 276 (1983).
[115] *Id.* at 287.
[116] *Id.* at 281.
[117] *Id.* at 282.

the Court held in *United States v. Karo*,[118] "the monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment."[119]

The Court's decisions in *Jones* and *Riley*, however, undercut the pre-digital era distinction between private and public space and called into question the continuing vitality of the third-party doctrine. *Jones* recognized that the length of time within which the surveillance is conducted, and possibly the number of individuals affected, may impact the constitutionality of the search. This aspect of *Jones* casts doubt on the district court's holding in *Clapper* that "the collection of breathtaking amounts of information unprotected by the Fourth Amendment does not transform that sweep into a Fourth Amendment search."[120] As the *Jones* Court noted, a relatively brief period of surveillance does not implicate Fourth Amendment protections,[121] but the duration of that surveillance can transform a perfectly lawful search into one that infringes on privacy rights. As such, *Jones* undermines the Court's statement in *Knotts* that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[122]

Moreover, in *Riley*, the Supreme Court acknowledged that cell phones store uniquely private information, such as confidential documents, financial records, photographs, and letters that in the pre-digital era were located in a home.[123] These items, which constitute the "papers and effects" that the Fourth Amendment has historically protected, did not receive less protection merely because an individual was traveling on a public highway.[124] Although the government's collection of metadata does not include such information, the point in *Riley* was that the focus on physical space was less relevant to the reasonableness of the search, particularly in the digital era. Likewise, in *State v. Earls*, the New Jersey Supreme Court held that cell phone users had a reasonable expectation of privacy over data disclosing their location[125] and noted that "[m]odern cell phones . . . blur the historical distinction between public and private areas because cell phones emit signals from both places."[126] Thus, *Jones* and *Riley* indicate that factors such as the length and intrusiveness of the surveillance, as well as the quality *and* quantity of the information collected, bear directly on

---

[118] 468 U.S. 705 (1984).
[119] *Id.* at 707.
[120] *Clapper*, 959 F. Supp. 2d at 751.
[121] *Jones*, 132 S. Ct. at 945.
[122] *Knotts*, 460 U.S. at 281–82.
[123] *Riley*, 134 S. Ct. at 2483.
[124] *Id.* at 2488.
[125] State v. Earls, 214 N.J. 564, 569 (2013); *see also U.S. ex rel. Order Pursuant to 18 U.S.C. Section 2703(d)*, 2012 WL 4717778 (S.D. Tex. September 26, 2012) (Owsley, M.J) (invalidating the government's warrantless search of cell phone metadata).
[126] *Earls*, 214 N.J. at 586.

whether an individual had an expectation of privacy in the information subject to a search.

The Foreign Surveillance Court's decision, although upholding the government's metadata collection program, suggested that the intrusiveness of the search, and the requirement that the government establish reasonable suspicion before accessing information beyond the numbers called, impacted its constitutionality. Specifically, the court emphasized that "the non-content metadata at issue here is particularly limited in nature and subject to strict protections that do not apply to run-of-the-mill productions of similar information in criminal investigations."[127] Thus, if the intrusiveness of the search degree of individualized suspicion is relevant, then the notion that individuals, after disclosing information to a third party, have no expectation of privacy "with respect to what will be done with the information following its disclosure"[128] is no longer valid. Furthermore, at least one other court has applied *Jones* to the government's metadata collection program, holding that the continuous monitoring of cell phone location data violates the Fourth Amendment.[129]

Simply put, the third-party doctrine, and the concept of voluntary disclosure, must be reexamined. Although *Smith* and *Miller* need not be overruled, the Court should limit the third-party doctrine by holding that the disclosure of information to third parties does not constitute a blanket waiver of all expectations of privacy to anyone who may access the information and use it for whatever reason. After all, cell phones have become ubiquitous in society and store a virtual warehouse of information, much of which is private. In addition, cell phones are used for a variety of purposes, such as to check email, hold conference calls, download books and videos, and store confidential information. The fact that the government's metadata collection program, like an inspection of a hotel guest registry, can only monitor outgoing calls and location does not mean that the search is *per se* reasonable; it depends on factors such as the quantity of information being collected, the length of time in which a particular caller is being monitored, and the ease with which the Government can go the extra step and discover the identity of the caller. In short, the relevant question, and one that would take into account the factors discussed in *Jones*, *Riley*, and *In re Application of Federal Bureau of Investigation*, is whether the search "exceeded society's

---

[127] Application of Federal Bureau of Investigation, 2014 WL 5463097 at *8.

[128] *Id.* (quoting *Smith*, 442 S.S. at 744).

[129] United States v. Powell, 943 F. Supp. 2d 759, 776 (E.D. Mich. 2013) (holding that long-term monitoring of an individual via a cell phone was invalid absent probable cause, although the evidence was admissible because the government relied on the defective warrant in good faith); *but see* Application of the United States of America for an Order Pursuant to 18 U.S.C. 2703(c) Directing AT&T, Sprint/Nextel, T-Mobile, Metro PCS and Verizon Wireless to Disclose Cell Tower Log Information, No. M-50, WL 4388397 (S.D.N.Y. 2014) (holding Fourth Amendment does not preclude government form requiring cell phone service providers to disclose cell site data).

expectations for how the police would investigate a particular crime."[130]

In *Patel*, the outcome should not be in doubt because law enforcement can learn the identity of every guest in a hotel, including the guest's room and license plate numbers, without any suspicion or pre-compliance judicial review. Even the government, in its metadata program, cannot go to such lengths without prior judicial approval. The critical question is whether the Court will limit the scope of the third-party doctrine. If it does, the impact on the government's surveillance efforts will be substantial.

III. *CITY OF LOS ANGELES V. PATEL*: THE COURT SHOULD LIMIT *SMITH V. MARYLAND* AND MODIFY THE THIRD-PARTY DOCTRINE

In *Patel*, the Court should do what it did in *Riley*: recognize that some pre-digital era doctrines are no longer workable. This includes the third-party doctrine, which in *Patel* was applied to reject any contention that hotel guests have an expectation of privacy in their name, room number, and length of stay. This is problematic, and demonstrates that third-party doctrine is in need of Supreme Court review. Indeed, section 41.49 gives law enforcement the power to discover the following information about every guest in a hotel:

- the guest's name, room, and license plate number;
- the make and model of the guest's car;
- the number of people staying in the guest's hotel room; and
- the arrival and departure dates.[131]

Given that law enforcement is not subject to any judicial oversight whatsoever, focusing solely on whether a hotel owner has a reasonable expectation of privacy in a guest registry ignores the critical issue that underscored Justices Sotomayor and Alito's opinions in *Jones*: whether the third-party doctrine is appropriate in the digital era. To limit the inquiry to hotel owners is akin to asking only whether Verizon Wireless has a reasonable expectation of privacy in its customer lists. The answer to those questions should be yes, but the issue that is missed within such a narrow inquiry is whether hotel *occupants* and cell phone *users* forfeit their privacy rights simply upon checking into a hotel, or making a call from a smart phone. In other words, a hotel owner's expectation of privacy in a guest registry is the tip of the iceberg. The hotel guests' privacy rights—just like the cell phone user's and the internet

---

[130] *Jones*, 132 S. Ct. at 964 (Alito, J., concurring).

[131] *See* L.A., CAL. MUN. CODE ch. IV, art. 1, §41.49 (2008).

subscriber's—is where the rubber meets the constitutional road.

The issue lurking in the background of *Patel* transcends hotel owners, highly regulated industries, and Holiday Inns. It is about whether the third-party doctrine, created during the disco era when rotary telephones were in vogue, adequately protects privacy rights in the digital era.[132] The answer to this question should be no. If the answer to this question is yes, and the third-party doctrine remains intact in its current form, then a hotel owner must provide all of this information to law enforcement officers regardless of whether the officers have probable cause, reasonable suspicion, or even a hunch that criminal activity is afoot. All of this happens without any judicial oversight whatsoever.[133] To make matters worse, if the hotel operator refuses law enforcement's demand, he or she may spend the night in the Los Angeles County Jail awaiting a trial on charges that can result in six months' imprisonment and a stiff fine.[134]

This scenario should be found unreasonable under the Fourth Amendment. As Chief Justice Roberts stated in *Riley*, "the ultimate touchstone of the Fourth Amendment is 'reasonableness.'"[135] In *Riley*, Chief Justice Roberts explained that the reasonableness standard involves "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."[136] The Court's "reasonableness balancing"[137] test derives from the Fourth Amendment's text, which prohibits "unreasonable searches and seizures,"[138] and the Court's precedent, which does not impose a categorical warrant requirement on law enforcement. The reasonableness test is beneficial in some respects because it ensures that a suspect's privacy interests, not merely the asserted interests of law enforcement, will factor into the determination of whether a particular search is constitutional.

On the other hand, arriving at a workable definition of reasonableness, or identifying standards to guide the reasonableness analysis, can prove difficult. As such, the reasonableness standard risks importing subjectivity into the decision-making process, and may result in case-by-case decision-making that fails to produce a cohesive jurisprudence in this area. Notwithstanding, the fact that the Court is willing to balance privacy rights against governmental interests reveals

---

[132] *See Miller*, 425 U.S. 435, 443.

[133] *See Patel*, 738 F.3d at 1064 ("As presently drafted, §41.49 provides no opportunity for pre-compliance judicial review of an officer's demand to inspect a hotel's guest records.").

[134] *See id.* (stating a violation of §41.49 is a misdemeanor, "punishable by up to six months in jail and a $1000") (citing L.A., CAL., MUN. CODE ch. I, art. 1 § 11.00(m) (2004)).

[135] *Riley*, 134 S. Ct. at 2482 (quoting Brigham City v. *Stuart*, 547 U.S. 398, 403 (2006)); *see also Patel*, 738 F.3d at 1061 ("The 'papers' protected by the Fourth Amendment include business records like those at issue here.").

[136] *Riley*, 134 S. Ct. at 2484 (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

[137] Case Comment, *Fourth Amendment: Riley v. California*, 128 HARV. L. REV. 251 (2014).

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

that the government's justifications alone, even if legitimate, must also be sufficiently compelling to outweigh a citizen's privacy rights, or at least be no broader than necessary to achieve the asserted interest.

In the context of section 41.49, the authority given to law enforcement is patently unreasonable. Warrantless searches of hotel guest registries, like the placement of a GPS tracking device on a car, the government's collection of metadata, or the monitoring of internet search history, indiscriminately affects all citizens.[139] The threat to core privacy protections cannot be denied, and the remedy lies in modifying the third-party doctrine. In its opinion, the Ninth Circuit relied on Supreme Court precedent and assumed without discussion that the third-party doctrine was still good law.[140]

Thus, regardless of whether this Court reverses or affirms the Ninth Circuit, one can assume that the Ninth Circuit's assumption was correct if it says nothing about the third-party doctrine. The likely impact will be that the government will continue tracking outgoing calls from citizens everywhere. After all, it would be difficult to argue that motorists have a greater expectation of privacy in the numbers dialed from an automobile than they would have in their name and location at a hotel in Los Angeles. In fact, if the Fourth Amendment were interpreted to permit law enforcement to obtain the names and room numbers of every guest in a hotel in Los Angeles County without a warrant or scintilla of suspicion, then there would be no controlling principle stopping the government from collecting cell phone metadata, which typically reveals outgoing phone calls but does not typically disclose the user's identity.[141]

The time has arrived "to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[142] As part of this inquiry, the Supreme Court should refine its approach to determining whether searches like those at issue here violate the Fourth Amendment. The Court should consider, *inter alia*, the length and intrusiveness of a search, the quantity and quality of data collected, the amount of time that data is kept, and the

---

[139] *See* Brian Owsley, *Trigger Fish, Sting Rays, and Fourth Amendment Fishing Expeditions*, 66 HASTINGS L. J. 183, 224 (2014) (discussing *Jones*, 132 S. Ct. 945, and noting that, at oral argument, "Chief Justice Roberts appeared to address the reasonable expectation of privacy as it relates to him . . . the reason for this expectation could arguably be based on the personal nature of one's vehicle and travels.").

[140] *See Patel*, 738 F.3d at 1062.

[141] *See* Application of the Fed. Bureau of Investigation, No. BR 14-01, 2014 WL 5463097 at *8 (FISA Ct. Mar. 20, 2014) (emphasizing that the cell phone data collected does not reveal "subscribers names or addresses or other identifying information." Such information can only be "accessed for analytical purposes after the NSA has established a reasonable articulable suspicion . . . that the number used to query the data—the 'seed'—is associated with one of the terrorist groups listed in the Order.").

[142] *See Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring); *see also* Smith v. Maryland, 442 U.S. 735, 749 (1979) (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.").

level of suspicion required to obtain the information.[143]

In so doing, the Court would recognize that 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."[144] We no longer live in a world of pen registers and plastic containers.[145] The principle that individuals have no reasonable expectation of privacy "with respect to how the Government will use or handle the information after it has been divulged by the recipient" fails to consider that "technology now allow[ing] an individual to carry . . . [private] information in his hand does not make the information any less worthy of the protection for which the Founders fought."[146] To be sure, it is "one thing to say that people expect phone companies to occasionally provide information to law enforcement," but "quite another to suggest that our citizens expect all phone companies to operate . . . a joint intelligence gathering operation with the government."[147] More specifically, monitoring calls from a single suspect's residence "in no way resembles the daily, all-encompassing, indiscriminate dump of cell phone metadata that the NSA now receives as part of its . . . Metadata Program."[148]

A citizen who signs a contract with a cell phone service provider in the digital era is not analogous to the person in the pre-digital era who hands over confidential records to a bank teller. It is one thing for customers to know that the bank teller may disclose such information to the government in connection with criminal and regulatory investigations.[149] It is quite another to hold that an outgoing call may be part of a vast and suspicionless government dragnet that relies on "national security" to justify a much less supportable—and far more intrusive—version of the sobriety checkpoint.[150] Comparing the search

---

[143] *See, e.g.*, *Jones*, 132 S. Ct. at 945 (finding that the Fourth Amendment violation was based in substantial part on the length of search—twenty-eight days—not merely on the use of a GPS tracking device to monitor a suspect's whereabouts); Riley v. California, 134 S. Ct. 2473, 2488 (2014) ("[C]ell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person."); Maryland v. King, 133 S. Ct. 1958, 1989 (2013) (Scalia, J., dissenting) (expressing concern that, "because as an entirely predictable consequence of today's decision [allowing law enforcement to take a DNA sample from an arrestee], your DNA can be taken and entered into a national database if you are ever arrested, rightly or wrongly, and for whatever reason").

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

[145] *See Smith*, 442 U.S. at 735; United States v. Robinson, 414 U.S. 218, 236 (1973) (holding that law enforcement may search the contents of a crumpled cigarette pack found on an arrestee's person).

[146] *Riley*, 132 S. Ct. at 2492 (brackets added).

[147] Klayman v. Obama, 975 F. Supp. 2d at 1, 33. (D.D.C. 2013).

[148] *Id.*; *see also Riley*, 132 S. Ct. at 2482 (holding that "[o]ne of the most notable distinguishing features of modern cell phones is their immense storage capacity," which is not "limited by physical realities").

[149] *See* United States v. Miller, 425 U.S. at 435, 442–43 ("The expressed purpose of [the Bank Secrecy Act] is to require records to be maintained because they "have a high degree of usefulness in criminal tax, and regulatory investigations and proceedings.'") (quoting 12 U.S.C. §1829b(a)(1)).

[150] *See Klayman*, 957 F. Supp. 2d at 33 ("The Supreme Court itself has long-recognized a

of a hotel guest registry or the collection of metadata to a pen register or a crumpled cigarette pack is "like saying a ride on horseback is materially indistinguishable from a flight to the moon."[151] To be sure, "[b]oth are ways of getting from point A to point B, but little else justifies lumping them together."[152]

Furthermore, it is not sufficient to say that the government's collection of metadata, unlike the searches of hotel guest registries, does not reveal a person's name.[153] What matters is that the government has the power to monitor *every* citizen's outgoing call history, and if it uncovers a few calls to Pakistan or Yemen, the government can seek an order that will disclose a motorist's identity and location. Moreover, it is not sufficient to rely on the government to establish procedures that ensure compliance with the Fourth Amendment.[154] Admittedly, the government should be given sufficient latitude to investigate threats to national security, and the interest in preventing a terrorist attack is certainly of the highest order. But this does not, and should not, mean that the government can do that which the Fourth Amendment prohibits, or simply be trusted to comply with constitutional demands when legitimate Fourth Amendment questions are raised. The purpose of the Fourth Amendment is to prohibit arbitrary and unreasonable intrusions by the government on personal privacy. Giving the government the means to define the limits of this power—when it is in the government's interest to have no limits whatsoever—would all but ensure that privacy rights would evaporate in the name of national security. Such an approach would also lend credence to Justice Thurgood Marshall's statement that "grave threats to liberty often come in times of urgency, when constitutional rights seem too extravagant to endure."[155]

In addition, giving the government such broad latitude ignores the fact that citizens do have at least some expectation of privacy in the numbers they dial, particularly in the location from which those numbers are dialed.[156] In fact, the lower court's reliance on the third-party

---

meaningful difference between cases in which a third party collects information and then turns it over to law enforcement, and cases in which the government and the third party create a formalized policy under which the service provider collects information for law enforcement purposes.") (internal citation omitted)); *see also* Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 447 (1990) (upholding a sobriety checkpoint against a Fourth Amendment challenge).

[151] *Riley*, 134 S. Ct. at 2488; *see also Klayman*, 957 F. Supp. 2d at 37 ("[T]he *Smith* pen register and the ongoing NSA Bulk Telephony Metadata Program have so many significant distinctions between them that I cannot possibly navigate these uncharted Fourth Amendment waters using as my North Star a case that predates the rise of cell phones.").

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

[153] *See Clapper*, 959 F. Supp. 2d at 752 ("what metadata is has not changed over time," and the information being collected by the Government is limited to "[tele]phone numbers dialed, date, time, and the like") (brackets in original).

[154] *See Riley*, 134 S. Ct. at 2491 ("[T]he Founders did not fight a revolution to gain the right to government agency protocols.").

[155] Skinner v. Railway Labor Execs. Ass'n, 489 U.S. 602, 635 (1989) (Marshall, J., dissenting).

[156] *See Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring) ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her

doctrine in *Patel*, as in the context of metadata collection, rather than on the lack of an expectation of privacy in metadata itself, suggests that citizens would have an expectation of privacy in this information if it has not initially been disclosed to a third party. The expectation of privacy in metadata is strengthened by the fact that cell phones are not a rare technological luxury. Rather, cell phones are a routine part of daily life for millions of citizens; they are a repository for the type of private information that would have historically been located in a home, and are used for a variety of purposes other than merely communicating with third parties.[157] Given this fact, the Court should hold that, before the government can indiscriminately collect metadata, it must have a lawful basis to do so.[158]

The bottom line is that law enforcement and the government should not be permitted to use modern technology as a means to rummage through hotel guest registries and call logs for the same reason they cannot "rummage through homes in an unrestrained search for evidence of criminal activity."[159] The Founders drafted the Fourth Amendment to avoid the "reviled 'general warrants' and 'writs of assistance' of the colonial era,"[160] which permitted British officers to search any area of a home regardless of whether evidence relating to the crime under investigation could be found there. Plainly, once officers had probable cause to believe that someone had committed a crime, they had *carte blanche* to search anywhere in the person's home for incriminating evidence that could be used at a subsequent trial. The Fourth Amendment's particularity requirement prohibited this practice by confining searches to areas where evidence of the specific crime(s) identified in the warrant, and giving rise to the suspicion, could be found. As such, the particularity requirement minimized the invasion of a citizen's privacy.[161] Prior to *Riley*, warrantless cell phone searches were the digital era's version of the general warrant because they gave law enforcement the unfettered authority to search any area of a cell phone incident to arrest. In doing so, officers could—and did—discover the most intimate details about an arrestee's private life.

---

familial, political, professional, religious, and sexual associations."); *Patel*, 738 F.3d at 1062–63 ("That the inspection may disclose 'nothing of any great personal value' to the hotel—on the theory, for example, that the records contain 'just' the hotel's customer list—is of no consequence" because "[a] search is a search, even if it happens to disclose nothing but the bottom of a turntable.") (quoting *Arizona v. Hicks*, 480 U.S. 321, 325 (1987)).

[157] *Riley*, 134 S. Ct. at 2482.

[158] *See* Minnesota v. Dickerson, 508 U.S. 366 (1993) ("[I]f police are lawfully in a position from which they view an object, if its incriminating character is apparent, and if the officers have a lawful right of access to the object, they may seize it without a warrant.").

[159] *Riley*, 134 S. Ct. at 2494.

[160] *Id.* (quoting Boyd v. United States, 116 U.S. 616, 626 (1886)).

[161] *See, e.g.*, Berger v. State of New York, 388 U.S. 41, 55 (1967) ("The Fourth Amendment commands that a warrant issue not only upon probable cause supported by oath or affirmation, but also '*particularly* describing the place to be searched, and the persons or things to be seized.'") (emphasis added).

In an era where technological advances have enabled the government to conduct unprecedented surveillance over its citizens, such searches posed threats to privacy that could not be underestimated.[162] Yet, this is precisely what the third-party doctrine enables; it strips citizens of any expectation of privacy in data or objects being searched, simply because they provided that information to a third party for a limited purpose. For this and other reasons, *Patel* presents the Court with an ideal opportunity to modify the third-party doctrine and apply the brakes to investigatory practices that run roughshod over Fourth Amendment freedoms. Indeed, the constitutionality of Los Angeles Municipal Code section 41.49 is the tip of an iceberg that can—and should—lead to a doctrinal shift in favor of stronger privacy protections.[163]

Specifically, the Court should reexamine the third-party doctrine. It should shift the focus from whether an individual has an expectation of privacy in a guest registry or in cell phone metadata, and instead inquire whether a search "exceeded society's expectations for how the police would investigate a particular crime."[164] In *Jones*, for example, several Justices appeared to focus less on whether the suspect had a subjective expectation of privacy in data revealing his location, and more on whether *society* would collectively expect that such information would be protected from warrantless intrusion by law enforcement. Justice Alito stated in his concurrence that "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 single movement."[165] Likewise, Justice Sotomayor discussed in her concurrence the "existence of a reasonable societal expectation of privacy in the sum of one's public movements."[166]

Of course, regardless of whether the Court elects to reexamine the third-party doctrine, it should hold that, before law enforcement can discover whether someone is staying at a hotel, it must provide reasonable, articulable facts upon which to conclude that an individual at a particular hotel may be engaged in criminal conduct. A similar standard

---

[162] *See Riley*, 134 S. Ct. at 2492–93; *see also* Olmstead v. United States, 277 U.S. 438 (1928) (Brandeis, J., dissenting) ("The progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping."); Florida v. Jardines, 133 S. Ct. 1409 (2013) (holding that the use of a trained dog to sniff for narcotics on a homeowner's front porch is a search and therefore requires a warrant and probable cause); Skinner v. Railway Labor Execs. Ass'n, 489 U.S. 602, 635 (1989) (Marshall, J., dissenting) (pointing out that "[h]istory teaches that grave threats to liberty often come in times of urgency, when constitutional rights seem too extravagant to endure").

[163] *See Patel*, 738 F.3d at 1060.

[164] *Jones*, 132 S. Ct. at 964 (Alito, J., concurring); *see also* Katz v. United States, 389 U.S. 347 (1967) (extending First Amendment protection to areas where an individual has a reasonable expectation of privacy).

[165] *Jones*, 132 S. Ct. at 964 (Alito, J., concurring).

[166] *Id.* at 956 (Sotomayor, J., concurring).

was adopted in *Terry v. Ohio*,[167] where the Court held that, "in justifying the particular intrusion the police officer must be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion."[168] Likewise, 18 U.S.C. §2703(d) (the Stored Communications Act), although quite lenient in its threshold warrant requirement, at least requires the government to set forth "specific and articulable facts showing that there are reasonable grounds to believe [that the particular records] sought, are relevant and material to an ongoing criminal investigation."[169] Put bluntly, the reasonable suspicion standard will ensure the stamp of judicial approval is made of something other than rubber.

After all, imagine a world in which law enforcement officers could obtain any citizen's name and location without a warrant, with *only* an erroneous belief about the law(s) the citizen is believed to have violated.[170] We are one decision away from that world. In *Jones*, Justice Alito stated that "even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable."[171] That is a tradeoff no citizen—or this Court—should find worthwhile.

IV. CONCLUSION

Enforcing the Fourth Amendment's protections has become akin to walking through a dark tunnel toward a bright light while trying to avoid carefully placed landmines. Citizens should not be forced to travel through such treacherous terrain to enforce basic privacy protections, and law enforcement should not have such an easy path to act on a mere hunch—or no hunch at all.[172] It should not matter if an individual's expectation of privacy with regards to his or her name and whereabouts is less important at a hotel than in a home, or that the hotel in which they stay is part of a highly-regulated industry. What matters is that law enforcement's ability to uncover this information is, for all intents and purposes, entirely unregulated.[173]

City of Los Angeles v. Patel may be the case no one is talking about, but it raises a foundational question in modern-day Fourth Amendment jurisprudence: whether the third-party doctrine, which was

---

[167] 392 U.S. 1, 21 (1968).
[168] *Id.* at 21.
[169] 18 U.S.C. 2703(d) (brackets added).
[170] *See* Heien v. North Carolina, 135 S. Ct. 530 (2014).
[171] 132 S. Ct. at 962 (Alito, J., concurring).
[172] *See Riley*, 134 S. Ct. at 2488 ("The fact that an arrestee has diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely.").
[173] *Riley*, 134 S. Ct. at 2488.

established in the pre-digital era, is appropriately suited to an era in which law enforcement can sift through guest registries on a whim, and the government can indiscriminately track cell phone metadata. The answer to this question should be no. As Justice Sotomayor wrote in *Jones*, privacy rights should evolve to account for the new threats posed by advances in technology and by the unprecedented manner in which law enforcement and the government monitor their citizens.

Part of that evolution should, as Justice Alito stated in *Jones*, recognize that the expectations of society matter, because societal expectations influence the public's perception of government conduct and the fairness of the methods the government uses to protect its people. If the Court confronts the third-party doctrine in *Patel*, it should ask whether society would find reasonable the proposition that once you disclose information to a third party, you thereby disclose it to the world. The answer will surely be no.