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

Adam Lamparello, Indiana Tech Law School
The United States Supreme Court recently granted certiorari in *City of Los Angeles v. Patel* to consider whether §41.49 of the Los Angeles Municipal Code violates the Fourth Amendment. §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:

- 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.

The Ninth Circuit Court of Appeals correctly held that hotels 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. 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. 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

---

1 Assistant Professor of Law, Indiana Tech Law School.
2 738 F.3d 1058 (9th Cir. 2013).
3 *Id.* at 1062.
4 *Id.* at 1065
5 See, e.g., *United States v. Miller*, 425 U.S. 435 (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 (1979) (holding that an individual has no reasonable expectation of privacy in outgoing calls made from a private residence).
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 essay argues that, now that the Supreme Court has granted certiorari in Patel, it should reject or at least modify the third-party doctrine to reflect threats to privacy posed in the digital era. The Ninth Circuit in Patel did not. 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. Simply put, the constitutionality of §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, is the concept 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.

---

6 738 F.3d at 1064; see also Sherry F. Colb, Third-Party Searches, (Nov. 12, 2014), available at: http://www.dorfonlaw.org/2014/11/third-party-searches.html (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 it [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”).

8 See Miller, 425 U.S. 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)) (brackets added); see also Klayman v. Obama, 957 F.Supp.2d 1, 33 (D.D.C. 2013) (“[t]he Supreme Court itself has long-recognized a meaningful difference between cases in which a third party collects
In the digital era, the third-party doctrine means something very 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. Thus, the sheer volume of information that the Government can uncover in connection with its wide-ranging surveillance program casts doubt upon the principle that citizens should lose all privacy rights in information merely because they sign a contract with Verizon or decide to conduct research on Google Chrome.

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. 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. 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. What’s worse, they typically reveal the names, location, outgoing call logs, and internet search history of unsuspecting citizens. It is not difficult to see how the third-

---


11 Id.

party doctrine and the administrative search exception can easily become the one-two punch that strikes a significant blow at the heart of basic privacy protections. In fact, if the Court reverses the Ninth Circuit, that will be the result.

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. It is to say that there should be limits on, among other things, 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 Wireless must surrender its subscribers’ call history.

After all, limits on the third-party doctrine exist in a variety of contexts. For example, when an individual walks into a CVS or Walgreen’s and gives the pharmacist a prescription for Prozac, the law regulates the circumstances within which such 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 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

---

14 Id.
emergency in connection with a crime.” Simply put, these laws do not allow government officials to go on a fishing expedition.

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 just to find a few 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.” 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 our private lives, including where we travel, who we call, and what search for on Google. 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, because the Ninth Circuit expressly stated that the doctrine was still valid law. 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

---

16 Id.
17 Riley, 134 S.Ct. at 2492.
18 See City of Los Angeles, 738 F.3d 1062 (“[t]o be sure, the guests lack any privacy interest of their own in the hotel’s records”).
interest in national security—above privacy rights, therefore sinking the Fourth Amendment further into the sea of irrelevance.

Put bluntly, City of Los Angeles 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 and permits law enforcement officers to march into the Beverly Wilshire hotel and discover the names of its guests, their room and 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 on First Avenue Northeast in Washington, D.C.

This essay argues that the Court should affirm the Ninth Circuit’s decision, invalidating §41.49 on Fourth Amendment grounds, 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 United States v. Jones, which asks whether a particular search exceeds “society’s expectations for how the police would investigate a particular crime.” In so doing, the Court should hold, as it did in Jones and Riley v. California, 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.

---

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.

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 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).
This approach would not require the Court to overrule *Smith v. Maryland*\(^{23}\) and *United States v. Miller*,\(^{24}\) both of which reaffirmed the third-party doctrine, but it would import much-needed limits in situations in which individuals voluntarily convey information to a third party but do not expect that this disclosure will entitle anyone to access and monitor such information. As it stands now, law enforcement officers can walk into a lobby and demand to see the names, room numbers, and license plate numbers of every guest staying at the Beverly Hills Hotel. They can also know when each guest checked in, when they intend to leave, and the people who were staying with them. This makes the Fourth Amendment—and privacy rights—seems like little more than the unpleasant in-laws that you must tolerate during the holidays but discard once the new year begins. The relationship between citizens and their civil liberties should not be so strained.

Part II surveys case law, analyzing the constitutionality of the Government’s metadata collection program and highlights 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. In *ACLU v. Clapper*,\(^{26}\) 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. These cases, and several others decided at the state and federal level, reveal deep divisions within the courts concerning the balance between privacy rights and the need to give the Government sufficient flexibility to adopt measures that will prevent acts of terrorism. Part III analyzes City of *Los Angeles* and argues that it provides the Court with an ideal

---

\(^{23}\) 442 U.S. 735.

\(^{24}\) 425 U.S. 435.

\(^{25}\) 957 F. Supp.2d 1.

\(^{26}\) 959 F.Supp.2d 724 (E.D.N.Y. 2014).
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. Klayman and Clapper underscore the divergent views that exist among federal courts.

A. KLAYMAN V. OBAMA: RE-EXAMINING THE THIRD-PARTY DOCTRINE AND HOLDING THAT METADATA COLLECTION VIOLATES THE FOURTH AMENDMENT

In Klayman, the United States District Court for the District of Columbia held that the National Security Agency’s (NSA) surveillance program,27 which consisted of the indiscriminate, suspicionless collection of cell-phone metadata, likely constituted a search under the Fourth Amendment. The court rejected the rationale in Smith, stating that a “citizens’ phone habits”28 have become “so unlike those considered by the Supreme Court thirty-four years ago [in Smith].”29 Indeed, the Government’s “almost-Orwellian technology”30 was “unlike anything that could have been conceived in 1979,”31 when Smith was decided. That is precisely the point. Times have

---

27 See e.g., Glenn Greenwald, NSA Collecting Phone Records of Millions of Verizon Customers Daily, GUARDIAN (London), June 5, 2013), available at: http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order. The public became aware of the NSA program from leaks of classified material by Edward Snowden, a former employee. 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.
28 Klayman, 975 F.Supp.2d at 17.
29 Id.
30 Id. at 19.
31 Id.
changed, and so must the courts. As explained below, *Klayman* embraced a view of privacy—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 reasoned that, because “people in 2013 have an entirely different relationship with phones than they did thirty-four years ago,” the Government’s “metadata collection and analysis almost certainly does violate a reasonable expectation of privacy.” The court rejected the Government’s argument that *Smith* “squarely control[s].” In *Smith*, the Court held that law enforcement could install a pen register to track the numbers dialed from a suspect’s phone. There was no reasonable expectation of privacy in the dialed numbers because they were “voluntarily transmitted… to his phone company,” and because “it is generally known that phone companies keep such information in their business records.”

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,” have become “so unlike those considered by the Supreme Court thirty-four years ago [in *Smith*].” Put differently, “the Court in *Smith* was not confronted with the NSA’s Bulk Telephony Metadata program,” and could not “have ever imagined [in 1979] how the citizens of 2013 would interact with their phones.”

---

32 *Id.*
33 *Id.*
34 *Id.* at 17.
35 *Id.*
36 *Id.*
37 *Id.*
38 *Id.*
39 *Id.*
40 *Id.* at 19.
41 *Id.*
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.”\textsuperscript{42} Furthermore, in \textit{Smith}, law enforcement installed a pen register to “record the numbers dialed from the [suspect’s] telephone,”\textsuperscript{43} whereas the NSA program collects, “on a daily basis [from telecommunications service providers] electronic copies of call detail records, or telephony metadata.”\textsuperscript{44} In other words, \textit{Smith} involved the targeting of an individual suspect, which “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.”\textsuperscript{45} As the court explained, it is “one thing to say that people expect phone companies to occasionally provide information to law enforcement,”\textsuperscript{46} but “quite another to suggest that our citizens expect all phone companies to operate… a joint intelligence gathering operation with the government.”\textsuperscript{47}

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.”\textsuperscript{48} 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.”\textsuperscript{49} To make matters worse, the Government uses “the most advanced twenty-first century tools,”\textsuperscript{50} to “proceed surreptitiously,”\textsuperscript{51} thus circumventing the “ordinary checks that constrain abusive law enforcement practices.”\textsuperscript{52}

\textsuperscript{42} Id. (emphasis in original).
\textsuperscript{43} Id.
\textsuperscript{44} Id. (emphasis in original).
\textsuperscript{45} Id.
\textsuperscript{46} Id.
\textsuperscript{47} Id.
\textsuperscript{48} Id.
\textsuperscript{49} Id. at 20.
\textsuperscript{50} Id.
\textsuperscript{51} Id.
\textsuperscript{52} Id.
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. 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.

Of course, while metadata itself has not changed over time, it can, unlike thirty-four years ago, “reveal the user’s location.”

Also, the “ubiquity of [cell] phones has dramatically altered the quantity of information that is now available and… what the information can tell the Government about people’s lives.”

For example, people “send text messages now that they would not (really could not) have made or sent back when Smith was decided.” 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.” This reflects a “rapid and monumental shift towards a cell-centric culture,” in which metadata from each person’s phone reveals “a wealth of detail about her familial, political, professional, religious, and sexual associations.” As the Supreme Court held

---

53 Id.
54 Id.
55 Id.
56 Id. at 21.
57 Id. at 21 n.57.
58 Id. at 21.
59 Id.
60 Id. (quoting City of Ontario v. Quon, 130 S.Ct. 2619, 2630 (2010)).
61 Klayman, 957 F.Supp.2d at 21.
62 Id. (quoting Jones, 132 S.Ct. at 955-56 (2012)) (Sotomayor, J., concurring).
in *City of Ontario v. Quon*,63 “[t]hat might strengthen the case for an expectation of privacy.”64 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.”65

*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.”66 The *Jones* Court explained that, while “relatively short-term monitoring of a person’s movements on public streets”67 is permissible, “the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.”68 Likewise, in *United States v. Maynard*,69 the District of Columbia Circuit held that, while a person “traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another,”70 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.”71

63 130 S.Ct. at 2619.
64 Id. at 2630.
65 *Klayman*, 957 F.Supp.2d at 22.
66 *Id.* at 17 (citing *Jones*, 132 S.Ct. at 955-56 (Sotomayor, concurring)); cf. *Jones*, 132 S.Ct. at 962 (Alito, J., concurring) (advances in technology may require individuals to “reconcile themselves” to the “inevitable diminution of privacy that new technology entails”).
67 *Jones*, 132 S.Ct. at 964 (Alito, J., concurring).
68 *Id.* The plurality and concurring opinions in *Jones* highlighted 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.
69 615 F.3d 544 (D.C. Cir. 2001).
70 *Id.* at 557.
71 *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).
In addition, Klayman implicitly recognized that voluntary disclosure of information to a third party does not automatically extinguish an individual’s expectation of privacy or render the Government’s sweeping surveillance program exempt from Fourth Amendment scrutiny. 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.\textsuperscript{72}

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 at all—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 §41.49 gives law enforcement officers carte blanche to discover the names of every guest staying at Hotel Shangri La in Santa Monica.

B. \textit{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 companies when they dial a number.”73 The district court held that “an individual has no legitimate expectation of privacy in information provided to third parties,”74 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.”75

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.”76

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

73 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”).
74 Clapper, 959 F.Supp.2d at 749.
75 Id. at 750 (quoting Smith, 442 U.S. at 737, 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).
76 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)).
suicide, addiction to gambling or drugs, experience with rape, grappling with sexuality, or support for particular political causes.”

The court stated:

First, without additional legal justification—subject to 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.

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.” 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.”

---

77 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”).

78 Clapper, 959 F.Supp.2d at 750-51.

79 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 Quon, 130 S.Ct. at 2632) (citing Vernonia School Dist. 47 J v. Acton, 515 U.S. 646 (1995)) (internal quotation marks and citations omitted).

80 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).
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 the next four weeks violated the Fourth Amendment, implicated the Government’s metadata collection policies. Noting that “*Jones* did not overrule *Smith*,”81 the district court stated, “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.”82 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.”83 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.”84

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.”85 Furthermore, “metadata is has not changed over time,” and the information being collected by the Government is limited to “[t]elephone numbers dialed, date, time, and the like.”86 Thus, although cell phones “have far more versatility now than when *Smith* was decided,”87 it does not undermine “the Supreme Court's finding that a person has no subjective

81 *Clapper*, 959 F.Supp. 2d at 752.
83 *Clapper*, 959 F.Supp. 2d at 752 (quoting *Jones*, 132 S.Ct. at 949 (“such a physical intrusion would have been considered a ‘search’ within the meaning of the Fourth Amendment when it was adopted”).
84 *Clapper*, 959 F.Supp. 2d at 752 (citing *Smith*, 442 U.S. at 744–45).
85 *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).
86 *Clapper*, 959 F.Supp. 2d at 752 (quoting *Klayman*, 957 F.Supp.2d at 35).
87 *Clapper*, 959 F.Supp. 2d at 752.

16
expectation of privacy in telephony metadata.” Ultimately, the district’s decision came down to a single proposition: “[b]ecause Smith controls, the NSA’s bulk telephony metadata collection program does not violate the Fourth Amendment.”

C. 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, 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.” The Sixth Circuit also emphasized the fact that the defendant voluntarily disclosed the cell phone data on a public highway.

On the other hand, the Sixth Circuit recognized that the Government’s argument was “strengthened by the fact that the authorities sought a court order to obtain information on [the suspect’s] location from the GPS capabilities of his cell phone.” Likewise, in In re Smartphone Geolocation Data Application, 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.

It 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

88 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.”) (brackets in original)
89 Clapper, 959 F.Supp. 2d at 752.
90 690 FR.3d 772 (6th Cir. 2012).
91 Id. at 777.
92 Id. at 781.
93 Id. at 779.
94 977 F. Supp.2d 129.
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…. Individuals 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.\(^\text{95}\)

In *United States v. Caraballo*,\(^\text{96}\) 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.”\(^\text{97}\) 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.’”\(^\text{98}\) Thus, the district court distinguished *Smith* and *Miller* because pinging was not “part and parcel of the provision of cellular phone service.”\(^\text{99}\) 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 pinging,\(^\text{100}\) because the Government’s conduct fell within the exigent circumstances exception.

In *In re Application of the Federal Bureau of Investigation*,\(^\text{101}\) 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

\(^{95}\) *Id.* at 143-44; see also *In re Application of the United States of America for Historical Cell Site Data*, 724 F.3d 600, 611-13 (5th Cir. 2013) (overruling *In re Application of the United States for Historical Cell Site Data*, 747 F.Supp.2d 827 (S.D. Tex. 2010)).

\(^{96}\) 963 F.Supp.2d 341, 360 (D. Vermont 2013).

\(^{97}\) *Id.*

\(^{98}\) *Id.*

\(^{99}\) *Id.*

\(^{100}\) *Id.*

\(^{101}\) No. BR 14-01, 2014 WL 5463097 (Foreign Intell. Surveillance Ct., March 20, 2014).
information he voluntarily turns over to third parties.”

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.”

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.”

The court also emphasized that the cell phone data does not reveal “subscribers’ names or addresses or other identifying information,” and 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.”

Consequently, these safeguards undermine the assertion that metadata collection is sufficiently intrusive to raise Fourth Amendment concerns.

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, which emphasized the physical space where the search occurred. In Knotts, for example, the Supreme Court held that the use of a beeper to monitor a suspect’s location and activities did not violate the Fourth Amendment. The surveillance in Knotts “amounted principally to the following of an automobile on public streets and highways,” where an individual has a diminished expectation of privacy. By the same token, the Knotts Court acknowledged that the

---

102 Id. at *6.
103 Id. (quoting Smith, 442 U.S. at 744) (in turn quoting Miller, 425 U.S. at 443).
104 2014 WL 5463097 at *7.
105 Id. at *8.
106 Id.
107 Id.
109 Id. at 281.
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 on his automobile.\textsuperscript{110} As the Court held in \textit{United States v. Karo},\textsuperscript{111} “the monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment.”\textsuperscript{112}

The Court’s decisions in \textit{Jones} and \textit{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. \textit{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 \textit{Jones} casts doubt on the district courts holding in \textit{Clapper} that “the collection of breathtaking amounts of information unprotected by the Fourth Amendment does not transform that sweep into a Fourth Amendment search.”\textsuperscript{113} As the \textit{Jones} Court noted, a relatively brief period of surveillance does not implicate Fourth Amendment protections,\textsuperscript{114} but the duration of that surveillance can transform a perfectly lawful search into one that infringes on privacy rights. As such, \textit{Jones} undercuts the Court’s statement in \textit{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.”\textsuperscript{115}

Moreover, in \textit{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.\textsuperscript{116} These items, which constitute the “papers and

\begin{footnotes}
\item[110] \textit{Id.} at 282.
\item[112] \textit{Id.} at 707.
\item[113] \textit{Clapper}, 959 F.Supp. 2d at 751.
\item[114] \textit{Jones}, 132 S.Ct. 945.
\item[115] \textit{Knotts}, 460 U.S. at 281-282.
\item[116] 134 S.Ct. at 2483.
\end{footnotes}
effects” that the Fourth Amendment historically protected, did not receive less protection merely because an individual was traveling on a public highway.\footnote{Id. at 2488.} Although the Government’s collection of metadata does not collect 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,\footnote{214 N.J. 564 (2013); see also In re 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).} the New Jersey Supreme Court held that cell phone users had a reasonable expectation of privacy in data disclosing their location and noted that “[m]odern cell phones… blur the historical distinction between public and private areas because cell phones emit signals from both places.”\footnote{70 A.3d 630, 642 (N.J. 2014).} Thus, Jones and Riley indicate that factors such as the length and intrusiveness of the surveillance, as well as the quality \textit{and} quantity of the information collected, bear directly on 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.”\footnote{In re Application of Federal Bureau of Investigation, 2014 WL 5463097 at *8.} 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”\(121\) is no longer valid. Furthermore, at least one other court has applied \textit{Jones} to the Government’s metadata collection program, holding that the continuous monitoring of cell phone location data violates the Fourth Amendment.\(122\)

Simply put, the third-party doctrine, and the concept of voluntary disclosure, must be re-examined. Although \textit{Smith} and \textit{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 \textit{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 \textit{Jones}, \textit{Riley}, and \textit{In re Application of Federal Bureau of Investigation} is whether the search “exceeded society’s expectations for how the police would investigate a particular crime.”\(123\)

\textsuperscript{121} \textit{Id.} (quoting \textit{Smith}, 442 S.S. at 744) (in turn quoting \textit{Miller}, 425 U.S. at 443).


\textsuperscript{123} \textit{Jones}, 132 S.Ct. at 964 (Alito, J., concurring).
In *City of Los Angeles*, the outcome should not be in doubt because law enforcement can learn the identity of every guest in a hotel, including their 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 *City of Los Angeles*, 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 *City of Los Angeles* was applied to reject any contention that hotel guests have an expectation of privacy in, among other things, their name, room number, and length of stay. This is problematic, and demonstrates that the time has arrived to reconsider the third-party doctrine. After all, §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.\(^\text{124}\)

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.

\(^{124}\) See *Los Angeles Municipal Code* §41.49.
The answer to those questions should be yes, but the sixty-four thousand dollar question—and the proverbial elephant in the room—is whether hotel occupants and cell phone users forfeit their privacy rights simply because they check into the Beverly Hills Hotel or call their significant others from a Smart Phone on the Santa Monica Freeway. 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 subscriber’s—is where the rubber meets the constitutional road.

The issue lurking in the background of *City of Los Angeles*—and in the back of most citizens’ minds—transcends hotel owners, highly regulated industries, and Holiday Inns. It is about whether the third-party doctrine, which was created during the disco era when rotary telephones were in vogue, adequately protects privacy rights in the digital era. 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 law enforcement officers from the Los Angeles Police Department will be able to march into the lobby of the Beverly Hills Hotel without a warrant—or any suspicion whatsoever—and know if a Supreme Court Justice is staying in the Sunset Suite.

Law enforcement will also be able to know the make, model, and license plate number of the Justice’s vehicle, the length of time the Justice has been staying there (including the Justice’s departure date), the Justice’s room number, and how many people are in the Justice’s room. Incredibly, the 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.126

125 *See Miller,* 425 U.S. 435.

126 *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”).
To make matters worse, if the hotel operator at the Beverly Hills Hotel 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.\footnote{See id. (a violation of §41.49 is a misdemeanor, “punishable by up to six months in jail and a $1000”)} Something is very wrong—and unreasonable—with this picture. And reasonableness is the touchstone of the Fourth Amendment.\footnote{See Riley 134 S.Ct. at 2482 (“the ultimate touchstone of the Fourth Amendment is reasonableness,” (quoting Brigham City v. Stuart, 547 U.S. 398, 403 (2006)); Patel, 738 F.3d at 1061 (“[t]he “papers” protected by the Fourth Amendment include business records like those at issue here”).}

The point, of course, is that §41.49, like the placement of a GPS tracking device on a car, the Government’s indiscriminate collection of metadata, and the monitoring of internet search history, affects all citizens.\footnote{See Brian Owsey, 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”).} The threat to core privacy protections cannot be gainsaid, 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.\footnote{See Patel, 738 F.3d at 1062.}

Thus, regardless of whether this Court reverses or affirms the Ninth Circuit, \textit{if it says nothing about the third-party doctrine} then one can assume that the Ninth Circuit’s assumption was correct. The likely impact will be that the Government will continue tracking outgoing calls from citizens everywhere, including those who call their significant others from a cell phone on First Street NE or who perform a Google search from a laptop computer on the Metro in Washington, D.C. 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 the Hollywood Hills Hotel.

Think about it: 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 what principle would stop the Government from collecting cell phone metadata, which typically reveals outgoing phone calls but does not typically disclose the user’s identity?131 Nothing.

The time has arrived “to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.”132 As part of this inquiry, the Court should refine its approach to determining 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 level of suspicion required to obtain the information.133

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.”134 We do not live in a world of pen registers and plastic

---

131 See In re Application of the Federal Bureau of Investigation, 2014 WL 5463097 at *8 (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”).

132 See Jones, 132 S.Ct. at 957 (Sotomayor, J., concurring); see also Smith, 442 U.S. at 749 (Marshall, J., dissenting) (“[t]hose 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”).

133 See, e.g., Jones 132 S.Ct. 945 (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, 134 S.Ct. at 2488 (“cell 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 [pin cite needed] (2013) (Scalia, J., dissenting) (expressing concern that, “because 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”) (brackets added).

134 Jones, 132 S.Ct. at 957 (Sotomayor, J., concurring).
containers anymore. 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, although “technology now allows an individual to carry … [private] information in his hand” it does not make the information any less worthy of the protection for which the Founders fought. To be sure, it “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.” 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.”

A citizen who signs a contract with Verizon Wireless in the digital era is not analogous 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. It is quite another to hold that calling your wife, husband, or partner from an cell phone on First Street NE in Washington, D.C. can 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.

\[\text{135 See Smith, 442 U.S. 735; United States v. Robinson, 414 U.S. 218 (1973) (holding that law enforcement may search the contents of a crumpled cigarette pack found on an arrestee’s person).}\\
\text{136 Riley, 132 S.Ct. at 2492 (brackets added).}\\
\text{137 Klayman, 975 F.Supp.2d at 19.}\\
\text{138 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”).}\\
\text{139 See Miller, 425 U.S. at 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)) (brackets added).}\\
\text{140 See Klayman 957 F.Supp.2d at 33 (“[t]he 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}
the search of a hotel guest registry or the collection of metadata collection 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.” To be sure, “[b]oth are ways of getting from point A to point B, but little else justifies lumping them together.”

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. 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 no answer to rely on the Government to establish procedures that ensure compliance with the Fourth Amendment.

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 the location from which those numbers are dialed. In fact, the lower courts’ reliance on the third-party 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

---

141 Riley, 134 S.Ct. at 2488; Klayman, 957 F.Supp.2d at 37 (“the 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”).

142 Riley, 134 S.Ct. at 2488.

143 See Clapper, 959 F.Supp.2d at 752 (“metadata 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).

144 See Riley, 134 S.Ct. at 2492 (“the Founders did not fight a revolution to gain the right to government agency protocols”).

145 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 familial, political, professional, religious, and sexual associations”); Patel, 738 F.3d at 1062-63 (“[t]hat 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)).
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 considered one of life’s luxuries. 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.\textsuperscript{146} Given this fact, the Court should hold that, before the Government can indiscriminately collect metadata, it must have a lawful basis to do so.\textsuperscript{147}

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.”\textsuperscript{148} Such practices resemble the “reviled ‘general warrants’ and ‘writs of assistance’ of the colonial era,”\textsuperscript{149} and in an era where technological advances have enabled the Government to conduct unprecedented surveillance over its citizens, the threat that these searches pose to privacy cannot be underestimated.\textsuperscript{150}

For these reasons, \textit{Patel} presents the Court with an ideal opportunity to modify the third-party doctrine and apply the brakes on investigatory practices that run roughshod over Fourth Amendment freedoms. Indeed, the constitutionality of Los Angeles Municipal Code §41.49 is the

\textsuperscript{146} \textit{Riley}, 134 S.Ct. at 2482.

\textsuperscript{147} See \textit{Minnesota v. Dickerson}, 508 U.S. 366 (1993) (“if 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”).

\textsuperscript{148} \textit{Riley}, 134 S.Ct. at 2492.

\textsuperscript{149} Id. (quoting \textit{Boyd v. United States} 116 U.S. 616, 626 (1886)).

\textsuperscript{150} Id. at 2492-93; see also \textit{Olmstead v. United States} 277 U.S. 438 (1928) (Brandeis, J., dissenting) (“[t]he progress of science in furnishing the Government with means of espionage is not likely to stop with wiretapping”); \textit{Florida v. Jardines}, 133 S.Ct. 1409 (2013) (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); \textit{Skinner v. Railway Labor Executives Association} 489 U.S. 602, 635 (1989) (Marshall, J., dissenting) (“[h]istory teaches that grave threats to liberty often come in times of urgency, when constitutional rights seem too extravagant to endure”).
tip of a very large iceberg that can—and should—lead to a doctrinal shift in favor of stronger privacy protections. Specifically, the Court should the Court 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.” 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 the Chateau Marmont or a Motel 6, it must provide reasonable, articulable facts upon which to conclude that an individual at a particular hotel may be engaged in criminal conduct. 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, without any suspicion of criminal activity, and with an erroneous belief about the law(s) the citizen is believed to have violated. 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.” That is a tradeoff that no citizen—or this Court—should find worthwhile.

---

151 See Patel, 738 F.3d at 1060.
152 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).
153 See Terry v. Ohio, 392 U.S. 1 (1968) (requiring law enforcement to have reasonable suspicion of criminal conduct before stopping a suspect); see also Skinner, 690 F.3d at 779 (noting that the Government’s argument was “strengthened by the fact that the authorities sought court order to obtain information on [the suspect’s] location from the GPS capabilities of his cell phone”); Stored Communications Act, 18 U.S.C. §2703(d) (requiring the Government to set forth “specific and articulable facts that there are reasonable grounds to believe [that the records] sought, are relevant and material to an ongoing criminal investigation”) (brackets in original).
155 132 S.Ct. at 962 (Alito, J., concurring).
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.156 It should not matter that an individual’s expectation of privacy in his or her name and whereabouts is less important at the Holiday Inn than in a home, or that the Holiday Inn 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.157

City of Los Angeles v. Patel may be the case no one is taking about, but it raises the question that is on everyone’s mind: whether the third-party doctrine, which was 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 used to protect its people. If the Court confronts the third-party doctrine in City of Los Angeles, it should ask whether society

156 See Riley, 134 S.Ct. at 2488 (“[t]he fact that an arrestee has diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely”).
157 Riley, 134 S.Ct. at 2488.
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.