No. 13-1175

IN THE
SUPREME COURT OF THE UNITED STATES

CITY OF LOS ANGELES,
Petitioner,

v.

NARANJIBHAI PATEL, ET AL.
Respondents.

On Writ of Certiorari to the
United States Court of Appeals for the Ninth Circuit

BRIEF OF *AMICI CURIAE* – PROFESSORS ADAM LAMPARELLO AND CHARLES E. MACLEAN IN SUPPORT OF THE RESPONDENT

Jim Berles
Counsel of Record
Adam Lamparello & Charles E. MacLean
Assistant Professors of Law
Indiana Tech Law School
1600 E. Washington Blvd.
Fort Wayne, IN 46803
1-855-TECHLAW

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Constitutional Provisions

Statutes and Regulations

Municipal Codes

Secondary Authorities

INTEREST OF *AMICI CURIAE*

Amici Curiae Adam Lamparello and Charles E. MacLean[1] are assistant professors of law at Indiana Tech Law School in Fort Wayne, Indiana. They teach and write in the areas of criminal and constitutional law, and have an interest in the principled development of the law in this area. Professors Lamparello and MacLean respectfully submit that the Court's decision in this case will affect citizens' privacy rights in a variety of contexts and have implications for the continuing viability of the third-party doctrine.

Together or separately, *Amici* have written numerous articles in the area of Fourth Amendment jurisprudence, including: Adam Lamparello, *City of Los Angeles v. Patel: The Upcoming Supreme Court Case No One is Talking About,* 20 TEX. J. C.R. & C.L. (forthcoming 2015); Adam Lamparello, *The Internet is the New Marketplace of Ideas: Why Riley v. California Supports Net Neutrality*, 25 DEPAUL J. ART, TECH. & INTELL. PROP. L. (forthcoming 2015);

---

[1] Counsel for Petitioner City of Los Angeles consented to the filing of this brief. Counsel for respondents Naranjibhai Patel, *et al.* did not respond to our request for consent, although counsel for both parties submitted written consent to the filing of briefs in support of either party or neither party. No counsel for any party authored this brief in whole or in part, and no counsel or party made a monetary contribution intended to fund the preparation or submission of this brief. No person other than the amici curiae, their law school, or their counsel made a monetary contribution to its preparation or submission.

Charles E. MacLean, *Katz on a Hot Tin Roof: The Reasonable Expectation of Privacy Doctrine is Rudderless in the Digital Age Unless Congress Continually Resets the Privacy Bar*, 24 ALB. L.J. SCI. & TECH. 47 (2014); Charles E. MacLean & Adam Lamparello, *Abidor v. Napolitano: Suspicionless Cell Phone and Laptop "Strip" Searches at the Border Compromise the Fourth and First Amendments*, 108 NW. U. L. REV. ONLINE 280 (2014); Charles E. MacLean & Adam Lamparello, *Riley v. California: The New Katz or Chimel?*, 21 RICHMOND J.L. & TECH. 1 (2014); Adam Lamparello & Charles E. MacLean, *Back to the Future: Returning to Reasonableness and Particularity under the Fourth Amendment*, 99 IOWA L. REV. BULL. 101 (2014); and Charles E. MacLean, *But Your Honor, A Cell Phone is Not a Cigarette Pack: An Immodest Call for a Return to the Chimel Justifications for Searches of Cell Phone Memories Incident to Lawful Arrest*, 6 FED. CTS. L. REV. 37 (2012).

SUMMARY OF ARGUMENT

In Los Angeles, if the owner of the Beverly Hills Hotel refuses to allow law enforcement to inspect the hotel's guest registry, he or she may spend a few nights in the Los Angeles County Jail awaiting trial on charges that can result in six months' imprisonment and a stiff fine. *See Patel v. City of Los Angeles*, 738 F.3d 1060, 1062 (9th Cir. 2013) (a violation of Los Angeles Municipal Code Section 41.49 is a misdemeanor "punishable by up to six months in jail and a $1000 fine") (citing L.A. Mun. Code § 11.00(m)).

If a hotel *guest* objected, law enforcement officers would simply say, "sorry, but you checked your Fourth Amendment rights at the door." The officers would be correct. The third-party doctrine, which states that individuals forfeit all privacy protections upon disclosing information to a third-party, prohibits the hotel guests from asserting any expectation of privacy in their personal information. And Section 41.49 gives law enforcement officers the authority—without any judicial oversight whatsoever—to march into the lobby of the Beverly Hills Hotel without a warrant and discover, *inter alia*, the names, room and license plate numbers, and arrival and departure dates of every guest in the hotel's 208 luxurious rooms. [2]

---

2 *See Patel*, 738 F.3d at 1060. Under Section 41.49, guest registries must contain the following:

Underscoring the infringement of the hotel guests' privacy rights is the fact that, when the guests initially reserved a room at the Beverly Hills hotel, they were *required* to disclose their name, address, and license plate number. In the context of metadata collection, one could at least make the argument, however implausible, that citizens can choose not to use their cell phones or to surf the internet. The same cannot be said for citizens who are traveling by car on an unseasonably chilly evening in Los Angeles and need a place to sleep, except for those who would be willing to sleep—and shiver—in the back seat.

Of course, some might argue that hotel guests can protect their privacy simply by using an alias. Citizens should not have to go incognito—or sleep in their vehicles—to enjoy basic Fourth Amendment protections. *See generally Katz v. United States,* 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (to trigger Fourth Amendment protections, an individual must have "exhibited an actual (subjective) expectation of privacy and, second, that the

---

> 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. *Id.* (citing § 41.49(2)(a)).

expectation be one that society is prepared to recognize as 'reasonable'").

Simply put, a hotel owner's expectation of privacy in a guest registry is only the tip of the Fourth Amendment iceberg. The continuing viability of the third-party doctrine in an era characterized by sweeping and indiscriminate searches that reveal, among other things, the identity and physical location of citizens throughout the United States, is where the rubber meets the constitutional road.

Indeed, focusing solely on whether a hotel owner has a reasonable expectation of privacy in a guest registry is tantamount to asking whether Verizon Wireless has a reasonable expectation of privacy in its customer lists. Regardless of the answer to this question, the sixty-four-thousand-dollar question—and the elephant in the room—is whether hotel *guests*, cell phone *users*, and internet *subscribers* automatically forfeit their privacy rights simply by checking into the Beverly Hills Hotel, calling their significant others from a Smartphone while driving on the Santa Monica Freeway, or sending an email to their best friend from Yahoo.

Although this case does not involve digital era technology, the Court's answer to this question—if it decides to reexamine the third-party doctrine—will have implications for the constitutionality of the National Security Agency's ("NSA") metadata collection program and the privacy rights of millions of citizens. *See, e.g.,* Electronic Frontier Foundation,

How the NSA's Domestic Spying Program Works, available at: https://www.eff.org/nsa-spying/how-it-works (broadly describing the National Security Agency's surveillance techniques).

After all, if citizens have no reasonable expectation of privacy in the information contained in a hotel guest registry, what principle would prohibit the Government from collecting cell phone metadata, which typically reveals a user's outgoing phone calls but does not disclose the user's identity?[3]

Nothing.

Surely not the Fourth Amendment. And that, in a nutshell, is the problem.

The Ninth Circuit relied on this Court's precedent, however, to hold that hotel guests have no expectation of privacy in a guest registry. *See Patel,* 758 F.3d at 1062 ("[t]o be sure, the guests lack any privacy interest of their own in the hotel's records") (*citing Smith v. Maryland*, 442 U.S. 735 (1979) (upholding law enforcement's use of a pen register to

---

[3] *See In re Application of F.B.I.*, No. BR 14-01, 2014 WL 5463097, at *8 (F.I.S.A. Ct. Mar. 20, 2014). (cell phone metadata collection does not reveal "subscriber names or addresses or other identifying information," which 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").

monitor outgoing calls from a private residence); *United States v. Miller*, 425 U.S. 435 (1976) (holding that citizens have no expectation of privacy in deposit slips and checks given to a bank teller). *Amici* respectfully submit that, while the Ninth Circuit correctly invalidated Los Angeles Municipal Code Section 41.49, it erred in this respect. If Section 41.49 is upheld *or* if the Ninth Circuit's approval of the third-party doctrine is left undisturbed, the Government will almost certainly be able to continue tracking outgoing calls from the cell phones of millions of unsuspecting citizens, including those who call their significant others from a cell phone on First Street Northeast and who perform a Google search from a laptop computer on the Metro in Washington, D.C.[4]

The Court's recent jurisprudence suggests that these practices violate the Fourth Amendment, and that the third-party doctrine's days are numbered. In fact, in *Riley v. California,* 134 S. Ct. 2473 (2014), and *United States v. Jones,* 132 S. Ct. 945 (2012), the Court began to chip away at the third-party doctrine. In holding that law enforcement officers could not search an arrestee's cell phone without a warrant or demonstrable exigency, the *Riley* Court implicitly

---

[4] *See* Washington Post, *The NSA May Be Reading Your Searches But Your Local Police Probably Aren't,* (Aug. 3, 2013), available at: http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/03/the-nsa-might-be-reading-your-searches-but-your-local-police-probably-arent/ (discussing the warrantless monitoring of citizens' internet search history)

recognized that some information is so private that its voluntary disclosure to a third party does not automatically waive all Fourth Amendment protections. *See Riley,* 134 S. Ct. at 2491 ("A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is").

Likewise, in *Jones,* the Court held that the tracking of a suspect's movements in a public place for twenty-eight days with a GPS device constituted a search under the Fourth Amendment. *See Jones,* 132 S. Ct. at 949. Although the Court was divided over whether the Government's conduct constituted a trespass or infringed on the suspect's reasonable expectation of privacy, a majority found that the length of the search was a significant factor. *See Jones,* 132 S. Ct. at 964 (Alito, J., concurring) ("the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy"); 132 S. Ct. at 955 (Sotomayor, J., concurring) (agreeing that long-term monitoring infringes on expectations of privacy).

In addition, several Justices focused on whether the Government's conduct violated a societal, not a subjective or individual, expectation of privacy. *See*, *Jones*, 132 S. Ct. at 964 (Alito, J., concurring) ("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 of an individual's

car for a very long period"); 132 S.Ct. at 955 (Sotomayor, J., concurring) ("the same technological advances that have made possible nontrespassory surveillance techniques will also affect the *Katz* test by shaping the evolution of societal privacy expectations").[5]

Thus, *Riley* and *Jones* rejected the proposition that individuals have no reasonable expectation of privacy concerning "how the Government will use or handle the information after it has been divulged by the recipient." *In re Application of F.B.I.,* 2014 WL 5463097, at *6. In both cases, the Court's reasoning reflected an understanding that, as technology continues to advance at a pace approximating the speed of light, the creation of new doctrines—or the abandonment of old ones—to protect privacy rights must not move at a snail's pace. A significant

---

[5] In other words, it may be time for this Court to consider amending the two-prong (subjective and objective) *Katz* reasonable expectation of privacy standard. The first prong (subjective) has caused much of the confusion. Specifically, because it is widely known that the Government collects cell phone metadata and has the ability to monitor internet browsing history, it would be difficult to assert that citizens have an actual, subjective expectation of privacy in such information. This does not mean, however, that these surveillance techniques do not infringe upon an objective, societal expectation of privacy. Thus, it may be time to discard prong one of the *Katz* test, to focus exclusively on whether society has a reasonable expectation of privacy in information such as a hotel guest registry.

component of this doctrinal evolution is abandoning the principle that "secrecy is a prerequisite to privacy," *Jones,* 132 S. Ct. at 957 (Sotomayor, J., concurring), and acknowledging that "privacy is not a discrete commodity, possessed absolutely or not at all." *Smith,* 442 U.S. at 749 (Marshall, J., dissenting).

To be sure, searches of hotel guest registries are of a scope and breadth that *Smith* (pen registers) and *Miller* (paper deposit slips) neither foresaw nor would have countenanced. *See id.* ("[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"); *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 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, with the latter raising Fourth Amendment concerns") (citing *Ferguson v. Charleston*, 532 U.S. 67 (2001)).

There are good reasons to reexamine the third-party doctrine here. As Fourth Amendment challenges to the NSA's metadata collection program continue to divide the federal courts, there will likely come a day in the not-so-distant future where the Court may be forced to decide whether the third-

party doctrine should be applied to sweeping searches like the one at issue here. *See Klayman,* 957 F. Supp. 2d at 35-37 (refusing to apply the third-party doctrine and holding that the NSA's metadata collection program constitutes a search under the Fourth Amendment); *but see ACLU v. Clapper*, 959 F. Supp. 2d 724, 749 (E.D.N.Y. 2014) (reaffirming the third-party doctrine and holding that "an individual has no legitimate expectation of privacy in information provided to third parties"); *United States v. Moalin*, No. 10cr4246 JM, 2013 WL 6079518, at *7–8 (S.D. Cal. Nov. 18, 2013) (applying *Smith* to uphold the NSA's metadata collection program). In addition, reexamining the third-party doctrine now will give the Court an opportunity to provide guidance to lower courts, possibly spur legislation at the federal and state level, and put a stop to practices that infringe privacy on an almost daily basis.

The deleterious effects of the third-party doctrine on privacy rights cannot be understated. Whether it is the warrantless search of a hotel guest registry or the indiscriminate collection of cell phone metadata, the third-party doctrine has become a runaway train that has ushered privacy rights out to pasture the moment an individual discloses information—no matter how private—to a third party. *See, e.g.*, *United States v. Skinner*, 690 F.3d 772 (6th Cir. 2012) (individuals have no expectation of privacy in information transmitted from a pay-as-you-go cell phone); *In re Smartphone Geolocation Data Application*, 977 F. Supp. 2d 129, 146 (E.D.N.Y.

2013) ("[g]iven 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").

The flaw in the third-party doctrine is "the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties." *Jones,* 132 S. Ct. at 957 (Sotomayor, J., concurring). In fact, case law interpreting the third-party doctrine has routinely held that "*all* information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection." *Id.* (citing *Smith,* 442 U.S. at 749) (Marshall, J., dissenting); *see also Katz v. United States*, 389 U.S. 347, 351 (1967) ("[w]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected") (brackets added). In an era of mass surveillance, this principle leaves all citizens vulnerable to systematic and pervasive infringement of privacy rights by state and federal law enforcement officials. Section 41.49 is just one example of what the third-party doctrine has left in its wake.

Ultimately, comparing the use of a pen register to warrantless searches of a hotel guest registry is "like saying a ride on horseback is materially indistinguishable from a flight to the moon." *Riley,*

134 S. Ct. at 2488; *see also 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"). Both are "ways of getting from point A to point B, but little else justifies lumping them together." *Riley,* 132 S. Ct. at 2488.

Make no mistake: searches of hotel guest registries have the potential to affect every citizen in the United States. Section 41.49 permits law enforcement to march into the lobby of the Beverly Hills Hotel without a warrant—or any suspicion whatsoever—and discover if a Supreme Court Justice is staying in the Sunset Suite or the Presidential Bungalow.

That's not all.

The guest registries would also reveal:

(1) The make, model, and license plate number of the Justice's vehicle;

(2) The length of time the Justice has been staying there, including the Justice's scheduled departure date;

(3) The Justice's room number; and

(4) The number of people staying in the Justice's room.[6]

In fact, armed with the threat of six months' imprisonment and a $1000 fine, law enforcement officers can require hotel owners to disclose the above information about *every* guest staying in every hotel. This should be troubling to every citizen who understands that liberty depends on knowing that the Government cannot constitutionally watch your every move simply because an ordinance purports to permit it or a new intrusive technology enables it.

It gets worse.

Given the lack of judicial oversight, there is no way to determine whether law enforcement is investigating a particular hotel while serving a valid public interest or just picking hotel names out of a hat. It is not difficult to see how the third-party doctrine can lead to significant abuses of privacy protections and violate the Fourth Amendment.

Amici respectfully submit that, although the third-party doctrine need not be abandoned entirely, it should be modified. Instead of focusing on whether an individual has demonstrated an actual and subjective expectation of privacy in a guest registry, the Court should consider the broader societal expectation in keeping citizens' names and locations

---

6 *See Patel,* 738 F.3d at 1060.

private. *See Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (discussing "the existence of a reasonable societal expectation of privacy in the sum of one's public movements"). This approach should take into account factors such as the length and intrusiveness of a search, the quantity and quality of data collected, the amount of time that data are kept, and the level of suspicion required to obtain such data. *See id.*

Applying these factors, searches of hotel guest registries unquestionably implicate the privacy rights of hotel guests, not merely the owners. As stated above, these searches allow law enforcement to know where you are sleeping, who you are sleeping with, when you arrived, and when you intend to leave. Surely, the information contained in a hotel guest registry is one that society would reasonably expect to be protected from disclosure absent some degree of suspicion and some quantum of judicial oversight. *See generally 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").

Accordingly, the Court should hold that hotel guest registries can be searched only if law enforcement has reasonable suspicion of criminal conduct or is faced with exigent circumstances. *See, e.g.*, *Terry v. Ohio*, 392 U.S. 1 (1968); 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 contents of a wire or electronic communication . . . are relevant and material to an ongoing criminal investigation").

Finally, should the Court decline to directly address the third-party doctrine, it should hold that Section 41.49 is not justified under the administrative records exception. Like the third-party doctrine, the administrative records exception should not be applied to wide-ranging and warrantless searches. Indeed, it is one thing for regulatory officials to inspect a restaurant to make sure that a filet mignon is not being cooked in a room full of fruit flies, but quite another for law enforcement officers to conduct warrantless and suspicionless searches of records that reveal every guest's name and precise location in the hotel.

Lest there be any doubt about the urgency of this issue, one need only look to Justice Alito's prediction in *Jones,* 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." 132 S. Ct. at 962 (Alito, J., concurring).

That is a tradeoff that no citizen—and certainly not this Court—should find worthwhile.

ARGUMENT

I. THE THIRD-PARTY DOCTRINE RENDERS INFORMATION DISCLOSED FOR A LIMITED PURPOSE AVAILABLE TO THE GOVERNMENT FOR ANY PURPOSE.

In *Riley*, the Court stated that "privacy comes at a cost." 134 S. Ct. at 2493. The costs that citizens pay for checking into a Los Angeles hotel are far too great, and the protections afforded by the Fourth Amendment far too insubstantial, to adequately protect privacy rights.

As a threshold matter, it is irrelevant that hotel guest registries do not reveal information of "great personal value." *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 … '[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)).

What matters is that the Fourth Amendment protects information in hotel guest registries from unreasonable searches and seizures. *See Patel,* 738 F.3d at 1061 ("[t]he 'papers' protected by the Fourth Amendment include business records like those at issue here") (citing *Hale v. Henkel*, 201 U.S. 43, 76–

77 (1906)). Indiscriminate and warrantless searches of this information, however, are anything but reasonable. *See Riley*, 134 S. Ct. at 2482 (reasonableness is the "ultimate touchstone" of the Fourth Amendment) (quoting *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006)).

In *Riley* and *Jones,* this Court began to turn the tide in favor of greater privacy protections, and against the third-party doctrine.

A. Citizens Should Not Forfeit *All* Privacy Rights Whenever They Surrender Information to Third Parties.

The time has arrived to ask "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on." *Jones,* 132 S. Ct. at 956 (Sotomayor, J., concurring).

The problem with the third-party doctrine is the notion that "*all* information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection." *Id.* at 957 (emphasis added). Such a rule requires citizens to assume the risk that information given to a third party may be accessed by the Government for whatever reason it pleases or even for no reason at all. *See United States v.*

Jacobson, 466 U.S. 109, 117 (1984) ("[i]t is well settled that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information").

To begin with, it is difficult to believe that the Court in *Smith* and *Miller* expected or anticipated that the third-party doctrine would one day authorize a sweeping government dragnet that is a far more intrusive—and much less supportable—version of the sobriety checkpoint. *See Michigan Dept. of State Police v. Sitz*, 496 U.S. 444 (1990) (upholding a sobriety checkpoint against a Fourth Amendment challenge where it was targeted to address an enumerated public safety issue, not a general law enforcement interest); *see also Skinner v. Railway Labor Execs. Ass'n*, 489 U.S. 602, 620 (1989) (permitting random drug testing of employees in "safety-sensitive" positions).

Indeed, it would be reasonable for law enforcement to stop motorists at a sobriety checkpoint on New Year's Eve because a substantial portion of citizens indulge in excessive quantities of alcohol and decide to get behind the wheel while intoxicated. The authority to use a sobriety checkpoint on New Year's Eve, however, does not mean that motorists can be forced to stop at general crime interdiction checkpoints 365 days a year in Anywhere, U.S.A., when returning home from work.

In other words, a practice that is constitutional in isolation can become unconstitutional in the aggregate. *See United States v. Knotts*, 460 U.S. 276 (1983) (a person traveling in public has no expectation of privacy in the vehicle's movements); *but see Jones*, 132 S. Ct. at 964 (Alito, J., concurring) ("relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable . . . but the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy").

Similarly, it might be constitutional to inspect a hotel guest registry when the hotel is known to harbor child sex traffickers or drug dealers, or to monitor vehicles that pass through toll booths on public highways. But Section 41.49 is far broader. It gives law enforcement the power to conduct warrantless searches of guest registries at *any* hotel in Los Angeles without any suspicion or judicial oversight whatsoever. Such practices inch us closer to the type of police state that the Founders rejected, and eviscerate "the protections for which they fought." *Riley*, 134 S. Ct. at 2495. That is precisely the point: the third-party doctrine is inching us in the wrong direction.

1. The Court Should Focus on a Societal, Not an Individual or Subjective, Expectation of Privacy.

In *Jones*, the Court was divided over whether the Government's conduct constituted a trespass or infringed on the motorist's reasonable expectation of privacy. A majority of the Court agreed, however, that monitoring a suspect's movements with a GPS tracking device for twenty-eight days violated the Fourth Amendment. *See Jones*, 132 S. Ct. at 958 (Sotomayor, J., concurring); 132 S. Ct. at 964 (Alito, J., concurring, joined by Justices Breyer, Ginsburg, and Kagan). In addition, the plurality suggested that "achieving the same result through electronic means . . . [may be] an unconstitutional invasion of privacy." *Id.* at 954 (brackets added).

Perhaps most importantly, a majority of the Court intimated that a standard focusing on the societal, not individual or subjective, expectation of privacy should govern the Fourth Amendment analysis. Justice Alito wrote in his concurring opinion that the two-pronged *Katz* standard "involves a degree of circularity," and that "judges are apt to confuse their own expectations of privacy with those of the hypothetical reasonable person to which the *Katz* test looks." *Id.* at 962 (Alito, J., concurring).

Rather than emphasizing an individual's actual and subjective expectation of privacy, Justice Alito held that the Government's conduct violated a

societal expectation of privacy. *See id.* at 964 ("society's expectation has been that law enforcement agents and others would not . . . secretly monitor and catalogue every movement that respondent made in the vehicle while driving").

Under *Jones,* there should be little doubt that society as a whole has a legitimate expectation of privacy in the type of information that a hotel guest registry reveals. As stated above, these records reveal the names, room, license plate numbers, check-in times, and scheduled departure dates of every guest in a hotel. Thus, Section 41.49 has the practical effect of giving law enforcement officers the power to know the whereabouts of thousands of citizens who are not suspected of any wrongdoing, and who have done nothing other than make the decision to check into a Los Angeles hotel.

Justice Sotomayor's concurrence in *Jones* speaks to the harms that result from interpreting the third-party doctrine to permit the unregulated and prolonged monitoring of citizens:

> Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about

> any person whom the Government, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and government in a way that is inimical to democratic society." *Jones,* 132 S. Ct. at 956 (Sotomayor, J., concurring) (quoting *United States v. Cuevas–Perez*, 640 F.3d 272, 285 (7th Cir. 2011)) (Flaum, J., concurring).

Make no mistake: Section 41.49, like the GPS tracking device at issue in *Jones*, has the potential to affect every citizen in the United States, including the Justices of this Court. In *Jones,* Chief Justice Roberts engaged in the following colloquy with the Government's attorney, Michael Dreeben:

> CHIEF JUSTICE ROBERTS: You think there would also not be a search if you put a GPS device on all of our cars, monitored our movements for a month? You think you're entitled to do that under your theory?
>
> MR. DREEBEN: The Justices of this Court?
>
> CHIEF JUSTICE ROBERTS: Yes.
> (Laughter.)
>
> MR. DREEBEN: Under our theory and under this Court's cases, the Justices of this Court when driving on public roadways have no greater expectation of —

> CHIEF JUSTICE ROBERTS: So, your answer is yes, you could tomorrow decide that you put a GPS device on every one of our cars, follow us for a month; no problem under the Constitution?
>
> MR. DREEBEN: Well, equally, Mr. Chief Justice, if the FBI wanted to, *it could put a team of surveillance agents around the clock on any individual and follow that individual's movements as they went around on the public streets.*

Transcript of Oral Argument at 9-10, *Jones,* 132 S. Ct. 945 (emphasis added).[7]

The Court in *Smith* and *Miller* could not possibly have expected that the third-party doctrine would one day lead to such pervasive and widespread monitoring of unsuspecting citizens.

---

[7] *See* Brian Owsley, *Triggerfish, Stingrays, and Fourth Amendment Fishing Expeditions,* 66 HASTINGS L. J. 183, 224 (2014) (stating that "Chief Justice Roberts appeared to address the reasonable expectations of privacy as it personally relates to him and the other members of the Court").

2. The Original Justifications for the Third-Party Doctrine Do Not Apply to Indiscriminate Searches of Private Information.

In *Riley,* the Court significantly weakened the foundation upon which the third-party doctrine rests. The Court recognized that the original justifications for the search incident to arrest doctrine—officer safety and evidence preservation—had been interpreted so broadly that the doctrine had nearly swallowed the rule against unreasonable searches and seizures. *See Riley*, 134 S. Ct. at 2483-92 (*citing 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); *New York v. Belton,* 453 U.S. 454 (1982) (holding that officers may search a passenger compartment incident to arrest); *Thornton v. United States*, 541 U.S. 615, 632 (2004) (a search of the passenger compartment is permissible if "the arrestee is unsecured and within reaching distance of the passenger compartment at the time of the search") (Scalia, J., concurring).[8]

In *Arizona v. Gant,* 556 U.S. 332 (2009), the Court began to limit the reach of the search incident to arrest doctrine, acknowledging that the

---

[8] In *Chimel v. California*, 395 U.S. 752, 762-63 (1969), the Court held that officers may perform a limited search of an arrestee's person incident to arrest for the purpose of protecting the officers' safety and preserving evidence).

relationship between the searches upheld in *Belton* and *Thornton,* and the original justifications for the search incident to arrest doctrine, was tenuous. *Id.* at 350-51 (limiting *Belton* and holding that searches of a vehicle must be for evidence related to the crime of arrest). Subsequently, in *Riley* the Court drew a categorical line that forced law enforcement to do what it should do most of the time—get a warrant. *See Riley*, 134 S. Ct. at 2495 ("[o]ur answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant").

Writing for the majority, Chief Justice Roberts stated that cell phones "hold for many Americans 'the privacies of life'" 134 S.Ct. at 2495 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)), and thus differ in a "qualitative and quantitative sense from other objects that might be kept on an arrestee's person." 134 S.Ct. at 2489. For example, unlike searches of plastic containers, crumpled cigarette packs, or other finite physical spaces, warrantless searches of a cell phone's contents allowed law enforcement to rummage through a virtual treasure trove of private data "in an unrestrained search for evidence of criminal activity." *Id.* at 2494. As such, searches of an arrestee's cell phone resembled the "reviled 'general warrants' and 'writs of assistance' of the colonial era." *Id.*; *see also Olmstead v. United States*, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting) ("[t]he progress of science in furnishing the Government with means of espionage is not likely to stop with wiretapping").

Furthermore, the *Riley* Court recognized that privacy rights extend to items of uniquely personal value, *and* to information such as the numbers a person has dialed and the people with whom a citizen associates. This conclusion echoes Justice Stewart's dissent in *Smith*, where he wrote that citizens have an expectation of privacy in, among other things, their names, outgoing calls, and location:

> The numbers dialed from a private telephone—although certainly more prosaic than the conversation itself—are not without "content." Most private telephone subscribers may have their own numbers listed in a publicly distributed directory, but I doubt there are any who would be happy to have broadcast to the world a list of the local or long distance numbers they have called. This is not because such a list might in some sense be incriminating, but because it easily *could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life*.

442 U.S. at 748 (Stewart, J., dissenting) (emphasis added). In fact, the *Riley* Court specifically rejected the Government's contention that "officers should always be able to search a phone's call log." 134 S. Ct. at 2492.

After *Riley,* there should be no justification for

upholding a law that gives investigators unfettered authority to discover the identity and whereabouts of thousands of hotel guests—none of whom are suspected of criminal conduct—through searches that reveal far more than an outgoing call log.

The same principles that motivated the Court to invalidate warrantless cell phone searches incident to arrest counsel in favor of limiting the third-party doctrine. Like the search incident to arrest doctrine, which was created before man landed on the Moon, the third-party doctrine is the product of "Supreme Court decisions that . . . are decades old." Jeremy H. Rothstein, *Track Me Maybe: The Fourth Amendment and the Use of Cell Phone Tracking to Facilitate Arrest*, 81 FORDHAM L. REV. 489, 507-08 (2012).

Admittedly, the third-party doctrine might be appropriate when referring to a federal investigation that includes a targeted search of an individual's bank records or the use of a pen register to monitor a single suspect's outgoing calls from a rotary telephone. Indeed, it is one thing for customers to know that a bank teller may disclose financial information to the government in connection with criminal and regulatory investigations. *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)) (emphasis added) (brackets added). It is quite another to hold that once citizens check into a

hotel, they give up all rights to information that reveals where they are staying, who they are staying with, when they arrived, and when they are leaving.

Put differently, citizens should reasonably expect "phone companies to occasionally provide information to law enforcement," but not expect "all phone companies to operate . . . a joint intelligence gathering operation with the government." *Klayman,* 957 F. Supp. 2d at 33 (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") (brackets added).

Some commentators argue that the third-party doctrine poses no threat to the privacy rights of those who have nothing to hide. *See, e.g.,* Nick Gillespie, *Richard Posner: Privacy is Mostly About Concealing Guilty Behavior* (December 8, 2014), available at: http://reason.com/blog/2014/12/08/richard-posner-privacy-is-mainly-about-c) ("[p]rivacy interests should really have very little weight when you're talking about national security"). Well, imagine if the third-party doctrine applied to a churchgoer entering a confessional, a client sitting in an attorney's office, or a patient seeking psychiatric care. These individuals might hesitate before speaking, or watch every word they say, if they knew that law enforcement might be eavesdropping.

The point, of course, is that privacy rights are not about hiding wrongdoing. They are about creating a

"realm of personal liberty which the government may not enter" without at least some degree of suspicion. *Planned Parenthood v. Casey,* 505 U.S. 833, 847 (1992). After all, privacy and liberty are two sides of the same constitutional coin. Without privacy, liberty is less secure.[9]

This is not to say that the Court must abandon the third-party doctrine entirely. For example, when citizens walk into a Safeway Pharmacy with a prescription for Seconal, drug enforcement agency officials should have the right to inspect Safeway's records to ensure that it is not overprescribing controlled substances, or that individuals are not doctor-shopping. *See* National Alliance for Model State Drug Laws, available at: http://www.namsdl.org/library/80E22BDA-19B9-E1C5-319D10D2D8989B6C/ (discussing the Health Insurance Portability and Accountability Act Privacy Rule and explaining the circumstances when disclosure is mandated by law).

Likewise, when someone checks in at the

---

[9] It is not sufficient to say that hotel guest registries only contain superficial information such as an individual's name and location. After all, would it be reasonable for law enforcement—without the slightest degree of suspicion—to know the location of a citizen's psychiatrist, but be prohibited from knowing the substance of that citizen's communications to his or her psychiatrist? No. A physical or digital location reveals more than where a person is; a location may—and often does—reveal what a person is doing.

Hollywood Hills Hotel and uses the hotel's free internet access, the hotel's owners should be able to access the guest's search history to ensure that he or she is not downloading child pornography or arranging a secret meeting with members of Al-Qaeda. But when the state is involved, it must show, at the very least, that it possesses something more than a generalized suspicion of criminal conduct, and certainly much more than a hunch. Section 41.49 requires neither.

Furthermore, the third-party doctrine is not without limits. For example, the Drug Enforcement Agency may not use its authority to inspect Safeway's records as a pretext to conduct a broader search for evidence of criminal conduct. Section 41.49 permits law enforcement officials to do precisely that, thus making it likely that law enforcement can do precisely what the Fourth Amendment forbids: obtain evidence of criminal activity without having the authority to be in the area where the evidence was discovered. *See, e.g.*, *Minnesota v. Dickerson*, 508 U.S. 366, 375 (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"). Simply put, monitoring everyone just to catch a few bad apples is exactly what the Fourth Amendment's drafters sought to avoid.[10]

---

[10] By way of analogy, warrantless searches of medical records are typically limited to circumstances where the government's

No one questions law enforcement's and the Government's interest in preventing crime and protecting national security. But this does not entitle law enforcement to sift through a hotel registry to find a needle in a haystack. If the Fourth Amendment is to have any meaning, it must be construed to prohibit law enforcement from going on a fishing expedition.

B. Searches of Hotel Guest Registries Should Require Reasonable Suspicion.

Amici respectfully submit that, before law enforcement can discover whether someone is staying at the Beverly Hills Hotel, it must provide reasonable, articulable facts upon which to conclude that a hotel guest may be engaged in criminal conduct.

The reasonable suspicion standard will help to ensure that the stamp of judicial approval is made of something other than rubber. *See Skinner*, 690 F.3d at 779 (noting that the Government's argument was

---

purpose is to "identify or locate a suspect, fugitive, witness, or missing person," when a crime is committed on the premises, or when there is a "medical emergency in connection with a crime." *See* American Civil Liberties Union, *FAQ on Government Access to Medical Records*, available at: https://www.aclu.org/technology-and-liberty/faq-government-access-medical-records#_edn3 (discussing 45 C.F.R. § 164.512(f)(2002)).

"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") (brackets added); *In re Application of the United States of America for Historical Cell Site Data*, 724 F.3d 600, 606 (5th Cir. 2013); *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") (quoting 18 U.S.C. § 2703(d) (brackets added).

The urgency in this case is driven in part by the fact that the Fourth Amendment is already on dangerously thin ice. Carving out exception after exception to the warrant and probable cause requirements—from "good faith" to "special needs"—has diluted the privacy protections that citizens, in an era of indiscriminate searches and rapid technological advances, need now more than ever. *See, e.g., United States v. Leon*, 468 U.S. 897 (1984) (holding that improperly seized evidence is admissible if the officer's mistake was made in good faith); *City of Ontario, Cal. v. Quon,* 560 U.S. 746, 756 (2010) (stating that "'special needs, beyond the normal need for law enforcement' may make the warrant and probable-cause requirement impracticable for government employers.") (quoting *O'Connor v. Ortega*, 480 U.S. 709, 725 (1987)).

Surely, citizens should not be forced to travel through such treacherous terrain to enforce privacy

rights, and law enforcement should not have such an easy path to act on a mere hunch—or no hunch at all. And it does not matter whether hotels are considered closely regulated industries. What matters is that law enforcement's authority to uncover personal information concerning every hotel guest is entirely unregulated.[11]

By affirming the Ninth Circuit's decision with respect to the constitutionality of Section 41.49 and modifying the third-party doctrine to focus on a societal expectation of privacy, the Court will send a loud and clear message that "the diminution of privacy" that broad and indiscriminate searches entail, and that Section 41.49 enables, is not and need not be inevitable. *Jones,* 132 S. Ct. at 962 (Alito, J., concurring).

---

11 The injury to privacy rights is particularly acute in the digital era. The NSA's metadata collection program and the monitoring of internet search history might make someone hesitate before calling a loved one, pause before emailing a friend, or think twice before downloading a controversial video on YouTube. Given that cell phones are owned by approximately ninety-one percent of the population and a repository for the papers and effects traditionally protected by the Fourth Amendment, the threat to privacy rights is grave indeed. *See Riley,* 134 S. Ct. at 2490.

II. THE ADMINISTRATIVE RECORDS EXCEPTION SHOULD NOT APPLY TO WARRANTLESS AND SUSPICIONLESS SEARCHES OF HOTEL GUEST REGISTRIES.

Sifting through a hotel guest registry is not equivalent to searching a restaurant's business records to ensure that it is complying with health and safety regulations. *See Camara v. Municipal Court*, 387 U.S. 523, 539 (1967) (administrative searches are valid as long as a "public interest justifies the intrusion"). When regulatory inspectors walk into a restaurant, they do not have the authority to know the names, license plates, credit card numbers, arrival and departure times, and entrée choices of every patron in the restaurant.

Likewise, guest registry searches cannot be compared to inspecting a liquor store's receipts to ensure that business owners are not selling whiskey to underage teenagers, or to examining a pawn shop's receipts to make sure that AK-47s are not being sold to convicted felons. *See Colonnade Catering Corp. v. United States*, 397 U.S. 72 (1970) (upholding the warrantless search of a catering business that sold liquor because the liquor industry was pervasively regulated); *United States v. Biswell*, 406 U.S. 311 (1972) (upholding the warrantless search of a pawn shop because of the public interest in regulating firearms to prevent violent crimes).

The purposes justifying searches of a

restaurant's or liquor store's records render them fundamentally different from searches of hotel guest registries or the collection of cell phone metadata. The former are conducted for a limited purpose and therefore guard against infringements on privacy, while the latter are pervasive and indiscriminate. Simply stated, searching a pawn shop's sales receipts does not affect thousands, or in the context of metadata collection, millions of citizens. *See e.g., Klayman*, 957 F. Supp. 2d at 42 (emphasizing the indiscriminate nature of the NSA's metadata collection program).

Of course, few would question the proposition that protecting public safety and strengthening national security are vital government interests. The more salient question, however, is whether these interests can justify a warrantless law enforcement dragnet that monitors the whereabouts of countless citizens without any judicial oversight whatsoever. The answer should be no. After all, the interest in preventing child sex trafficking at hotels should not give law enforcement officers unchecked power to do whatever they want, whenever they want, and for whatever reason they want.[12]

---

12 If the Los Angeles City Council enacted the records disclosure features of Section 41.49 to combat, say, child prostitution and human trafficking, and the Court deemed that justification sufficient, application of Section 41.49 should be limited to those stated purposes. Thus, any warrantless application beyond those purposes is unconstitutional. On the other hand, if the Los Angeles City Council enacted Section 41.49's records disclosure features to give law enforcement

At the end of the day, one need only look to history, which "teaches that grave threats to liberty often come in times of urgency, when constitutional rights seem too extravagant to endure." *Skinner*, 489 U.S. at 635 (Marshall, J., dissenting). Constitutional rights such as privacy are essential, not extravagant, and the only thing difficult to endure is the sacrifice of liberty in the name of security, and the belief that privacy is only something that should be valued if we decide to commit a crime. The societal interest in privacy is not about hiding nefarious conduct from the state. Rather, it reflects a core value upon which liberty rests: that the right to reserve a hotel room without being monitored by the government "transcends the convenience of the moment." *See Clinton v. New York*, 524 U.S. 417, 449 (1998) (Kennedy, J., concurring).

---

warrantless access to those hotel records at any time and for any purpose or even no purpose, then Section 41.49 violates the Fourth Amendment. Without any judicial oversight, there is no way to know what law enforcement is doing.

CONCLUSION

For these reasons, the judgment of the United States Court of Appeals for the Ninth Circuit should be affirmed in part and reversed in part.

Respectfully submitted,

James J. Berles
Counsel of Record
Charles E. MacLean &
Adam Lamparello
Assistant Professors of Law
Indiana Tech Law School
1600 E. Washington Blvd.
Fort Wayne, IN 46803
1-855-TECHLAW
JJBerles@IndianaTech.edu
CEMacLean@IndianaTech.edu
AXLamparello@IndianaTech.edu