Notre Dame Law Review

Volume 97 | Issue 2 Article 7

4-2022

A Solution for the Third-Party Doctrine in a Time of Data Sharing, Contact Tracing, and Mass Surveillance

Tonja Jacobi
Stanford Clinton and Zylpha Kilbride Clinton Research Professor, Northwestern University Pritzker School of Law

Dustin Stonecipher
Law clerk to Judge Roy W. McLeese III, D.C. Court of Appeals

A SOLUTION FOR THE THIRD-PARTY DOCTRINE IN A TIME OF DATA SHARING, CONTACT TRACING, AND MASS SURVEILLANCE

Tonja Jacobi & Dustin Stonecipher***

Today, information is shared almost constantly. People share their DNA to track their ancestry or for individualized health information; they instruct Alexa to purchase products or provide directions; and, now more than ever, they use videoconferencing technology in their homes. According to the third-party doctrine, the government can access all such information without a warrant or without infringing on Fourth Amendment privacy protections. This exposure of vast amounts of highly personal data to government intrusion is permissible because the Supreme Court has interpreted the third-party doctrine as a per se rule. However, that interpretation rests on an improper understanding of the reasonable expectation of privacy standard developed in Katz v. United States.

There is a solution. A close reading of Katz*'s logic can reorient third-party analysis from a per se rule to a tailored test of the knowledge of the sharer and the nature of the recipient, asking whether the sharer (1) knowingly exposed information (2) to the public. This interpretation allows the Fourth Amendment to better evolve with changing technology, such that the exception no longer risks swallowing the rule.*

* Stanford Clinton and Zylpha Kilbride Clinton Research Professor, Northwestern University Pritzker School of Law. t-jacobi@law.northwestern.edu.

** Law clerk to Judge Roy W. McLeese III, D.C. Court of Appeals. stonecipher.dustin@gmail.com.

Thanks to Laurent Sacharoff, Deborah Tuerkheimer, Ronald Allen, and Jillian Stonecipher for their invaluable feedback on this manuscript.

INTRODUCTION

The Supreme Court Justices seem to take a bashful pride in their struggles with technology: Justice Breyer jokes that he does not know how to open his iPhone;[1] Justice Kagan reports that most of the Justices do not understand Facebook or Twitter and do not use email;[2] and while the rest of the world was moving to videoconferencing in the face of the COVID-19 pandemic, the Supreme Court opted for the "antiquated technology of the telephone"[3]—and still multiple Justices

1 Transcript of Oral Argument at 7, United States v. Wurie, 134 S. Ct. 2473 (2014) (No. 13-212):

> MR. DREEBEN: So if you have an iPhone, Justice Breyer, and I don't know what kind of phone that you have—
>
> JUSTICE BREYER: I don't either because I can never get into it because of the password. [*Laughter.*]

2 Jason Leopold, *The US Supreme Court Uses Email After All—Or at Least Two Justices Do*, VICE (July 11, 2016) https://www.vice.com/en_us/article/qv5ad3/the-us-supreme-court-uses-email-after-all-or-at-least-two-justices-do [https://perma.cc/TQ3P-B63R] ("They didn't really understand Facebook and Twitter, she said, and . . . '[t]he court hasn't really "gotten to" email,' . . . because the justices are old, they had a difficult time grasping new technology.").

3 Tonja Jacobi, Timothy R. Johnson, Eve M. Ringsmuth & Matthew Sag, *Oral Argument in the Time of COVID: The Chief Plays Calvinball*, 30 S. CAL. INTERDISCIPLINARY L.J. 399, 400 (2021).

struggled.[4] And yet, the Supreme Court must decide issues that hinge on rapidly changing technology, including cases with great import for privacy rights.[5] The most significant of these issues is the third-party doctrine, for that doctrine has the potential to annihilate the privacy rights of individuals engaged in a variety of everyday behaviors, from checking email to browsing a website, merely because doing so involves an Internet Service Provider (ISP) or some other third party.

The third-party doctrine holds that when an individual voluntarily hands information over to a third party, that person cannot then claim to have a reasonable expectation of privacy in the information.[6] Back in 1976, the third-party doctrine enabled the government to access a "pen register"—the list of numbers dialed from a phone.[7] But the advent of new technology has enabled the government, via the third-party doctrine, to engage in mass surveillance of individuals without any recourse to the Fourth Amendment.[8] Today, individuals share information constantly: every email is transmitted through a third-party email platform such as Google as well as an Internet provider; banking is done through a third-party bank; text messages are sent through a third-party cell phone provider; smart technology like Alexa

4 For instance, Justice Sotomayor struggled to get back on mic in the first two oral arguments heard by telephone—Transcript of Oral Argument at 22, U.S. Pat. & Trademark Off. v. Booking.com B.V., 140 S. Ct. 2298 (2020) (No. 19-46); Transcript of Oral Argument at 21, Agency for Int'l Dev. v. All. for Open Soc'y Int'l, Inc., 140 S. Ct. 2082 (2020) (No. 19-177)—as did Justice Alito in another case—Transcript of Oral Argument at 36, McGirt v. Oklahoma, 140 S. Ct. 2452 (2020) (No. 18-9526). There was also the notorious failure of someone to turn off their mic in one oral argument, during which a toilet could be heard flushing. Jeremy Art (@cspanJeremy), TWITTER (May 6, 2020, 12:48 PM), https://twitter.com/cspanJeremy/status/1258076164234579969 [https://perma.cc/5GGT-2RA7]. The sound is not recorded in the transcript, but it can be heard at timestamp 59:48 on the recording. Oral Argument at 59:48, Barr v. Am. Ass'n of Pol. Consultants, Inc., 140 S. Ct. 2335 (2020) (No. 19-631), https://www.oyez.org/cases/2019/19-631 [https://perma.cc/X8WL-R44H].

5 The Court must also decide new technology cases with great commercial significance—for example, *Google LLC v. Oracle America, Inc.*, 141 S. Ct. 1183 (2021), is estimated to be worth $9 billion. *See* Roger Parloff, *Google and Oracle's $9 Billion 'Copyright Case of the Decade' Could Be Headed for the Supreme Court*, NEWSWEEK (May 23, 2019), https://www.newsweek.com/2019/06/07/google-oracle-copyright-case-supreme-court-1433037.html [https://perma.cc/28SQ-4JUN].

6 United States v. Miller, 425 U.S. 435, 443 (1976) ("The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government." (citing United States v. White, 401 U.S. 745, 751–52 (1971)); Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

7 *See Smith*, 442 U.S. at 737, 745–46.

8 *See generally* Mary Anne Franks, *Democratic Surveillance*, 30 HARV. J.L. & TECH. 425 (2017) (describing the history of mass surveillance, particularly of marginalized minorities).

exists throughout modern homes. Under the third-party doctrine as it is currently interpreted, all of these activities can be monitored by government agents, without themselves being monitored by a neutral judge as to whether they comply with the Fourth Amendment, because every individual has "voluntarily" conveyed this information to a third party.[9] The potential risks this per se standard poses to individual privacy are multifarious and potentially constitutionally groundbreaking—in today's information age, we bring third parties into our homes,[10] into our cars,[11] and even into our bodies.[12]

The Supreme Court, other courts, and scholars have all recognized that there is a serious problem with the third-party doctrine.[13] Yet, the Court has refused to provide an adequate solution. In 2018, the Court recognized that applying a doctrine built for pen registers to smart phones is inappropriately intrusive.[14] But rather than tackling the underlying problem, the Court merely carved out a narrow exemption for cell site location information (CSLI)—and only some forms of such information at that—saying:

> Cell phone location information is not truly "shared" as one normally understands the term. In the first place, cell phones and the services they provide are "such a pervasive and insistent part of daily life" that carrying one is indispensable to participation in modern society. Second, a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up. Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates. Apart from

9 *See* discussion *infra* Part I.

10 *See* Minyvonne Burke, *Amazon's Alexa May Have Witnessed Alleged Florida Murder, Authorities Say*, NBC NEWS (Nov. 2, 2019), https://www.nbcnews.com/news/us-news/amazon-s-alexa-may-have-witnessed-alleged-florida-murder-authorities-n1075621 [https://perma.cc/5EDE-N5B8].

11 *See* Thomas Brewster, *Cartapping: How Feds Have Spied on Connected Cars for 15 Years*, FORBES (Jan. 15, 2017), https://www.forbes.com/sites/thomasbrewster/2017/01/15/police-spying-on-car-conversations-location-siriusxm-gm-chevrolet-toyota-privacy/ [https://perma.cc/EN28-XK3G].

12 *See* Lindsey Van Ness, *DNA Databases Are Boon to Police but Menace to Privacy, Critics Say*, PEW: STATELINE (Feb. 20, 2020), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2020/02/20/dna-databases-are-boon-to-police-but-menace-to-privacy-critics-say [https://perma.cc/KYQ9-6GYB].

13 *See infra* note 33.

14 Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018) (acknowledging the "seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years").

> disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data.[15]

All these points are true, but each also applies to multiple other daily activities that the third-party doctrine continues to exempt from Fourth Amendment protection. As Justice Sotomayor noted, the third-party doctrine leaves a similar amount of information unprotected when individuals carry out "mundane tasks," including when "disclos[ing] the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers."[16] Blithely ignoring the fact that these very same concerns arise with so many other technologies leaves individuals unprotected from mass surveillance, unhinges the third-party doctrine from its doctrinal moorings, and leaves unaddressed future applications, including vital information gathering measures.

In this Article, we provide a solution for the problem that the third-party doctrine categorically exempts from any expectation of privacy so many modern forms of communication and other ordinary life activities. Our solution avoids creating a patchwork of exceptions, which would undermine certainty and doctrinal coherence, but nor does it require marching boldly into the unknown future.[17] Rather, the solution lies simply in returning to the core principles upon which modern search and seizure law rests: the landmark case of *Katz v. United States*.[18]

Katz established that government conduct constitutes a search when it intrudes upon a reasonable expectation of privacy; in such a case, Fourth Amendment protection applies.[19] But a person cannot shout their secrets from the rooftops and still claim an expectation of privacy, and so *Katz* also specified that when a person knowingly exposes information to the public, there will be no such expectation of privacy.[20] It is from this language that the third-party doctrine is drawn. But in two cases decided within a few years of *Katz*—*United*

15 *Id.* at 2220 (citation omitted) (quoting Riley v. California, 573 U.S. 373, 385 (2014)).

16 United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

17 These two competing concerns are discussed further in Section III.E.

18 389 U.S. 347 (1967).

19 *Id.* at 360–61 (Harlan, J., concurring) (laying out the dominant "reasonable expectation of privacy" test).

20 *Id.* at 351 (first citing Lewis v. United States, 385 U.S. 206, 210 (1966); and then citing United States v. Lee, 274 U.S. 559, 563 (1927)) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.").

States v. Miller[21] and *Smith v. Maryland*[22]—the Court effectively left behind both the language and the conceptual framework underlying this qualification, by crafting the third-party doctrine as a categorical exception to the *Katz*ian reasonable expectation of privacy.

Instead of inquiring, as *Katz* mandated, whether a person "knowingly expose[d]" information "to the public," *Miller* and *Smith* subtly changed both of these requirements. First, the two decisions changed the "knowingly" requirement to "voluntarily," and deemed actions to be voluntary even if a person had no option to avoid sharing information if they wished to use a given technology.[23] So, even though it was impossible not to share information dialed with the telephone company in order to have a home telephone,[24] or to share bank details with the bank teller in order to have a bank account,[25] these activities were still deemed voluntary. Second, the decisions interpreted information as having been exposed "to the public" any time they were shared with a third party, regardless of the circumstances.[26] So even if Mr. Miller's bank had promised to keep his information secret, by sharing it with the bank itself, the Court deemed this equivalent to sharing with the public, and thus Miller had no expectation of privacy in his banking information.[27] *Miller* and *Smith* created a categorical test by which any information shared under any circumstances with any party for any reason constituted conveying information to the public, thus losing all expectation of privacy.

This broad application of the third-party doctrine is problematic not just in terms of being faithless to foundational precedent and enabling mass surveillance, but it also has the potential to hamstring the capacity of the United States government to respond to the COVID-19 pandemic, as well as other likely future pandemics.[28] The most effective means of combating the spread of infectious diseases is through tracking and tracing, which itself is best operationalized through digital means.[29] Yet, the public rightly fears making its highly personal health data, location data, and contact information available to the government or to third parties,[30] for the third-party doctrine

21 425 U.S. 435 (1976).

22 442 U.S. 735 (1979).

23 *Miller*, 425 U.S. at 442–43; *Smith*, 442 U.S. at 744–45.

24 *See Smith*, 442 U.S. at 737.

25 *See Miller*, 425 U.S. at 436.

26 *Smith*, 442 U.S. at 743–44.

27 *Miller*, 425 U.S. at 443.

28 *See infra* Conclusion.

29 *See infra* Conclusion.

30 *See* Alice Miranda Ollstein & Mohana Ravindranath, *Getting It Right: States Struggle with Contact Tracing Push*, POLITICO (May 17, 2020), https://www.politico.com/news/2020/05/17/privacy-coronavirus-tracing-261369 [https://perma.cc/7XC7-JDDV] ("[T]he new

renders that information, once exposed, forever subject to government scrutiny, for any purpose, including criminal investigation. As such, finding a solution to the third-party doctrine is not merely a question of jurisprudential coherence, but a matter of survival, since such a solution would enable rapid responses to major crises.

This Article proceeds in four parts. Part I details the creation and development of the third-party doctrine, the function it serves, and how it has become unmoored from its foundation in *Katz*. Part II describes how dire the need is for a solution to the problem, illustrating how invasive the third-party doctrine has become to Fourth Amendment rights. Part III considers how to solve the problem: first, it critically examines the various solutions considered by the Supreme Court; then, it highlights the advantages and flaws with solutions proposed by prior scholars; and finally, it provides our solution. This Article concludes by explaining how the need for reform to the third-party doctrine has become increasingly pressing in the time of the COVID-19 pandemic and how, without reform, the response of the United States to this and future crises will be undermined by the current categorical version of the third-party doctrine.

I. MISREADING *KATZ*: THE DEVELOPMENT OF THE THIRD-PARTY DOCTRINE

The third-party doctrine governs how and what the government can collect from third parties in criminal investigations.[31] For over four decades, the doctrine has stood for the seemingly straightforward concept that when a person shares something, they can no longer claim a reasonable expectation of privacy in that shared information.[32] This "you share it, you lose it" idea, while controversial,[33] was affirmed

state apps may still be viewed skeptically by a public reluctant to submit to digital tracking. And the early experience of these states is raising questions about whether locally developed apps will gain enough critical mass to help health officials keep tabs on the virus before new hot spots explode.").

31 Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009).

32 Michael Gentithes, *The End of* Miller*'s Time: How Sensitivity Can Categorize Third-Party Data After* Carpenter, 53 GA. L. REV. 1039, 1042 (2019).

33 The Court's bright line rule has inspired passionate dissents and concurrences articulating problems, both legal and functional. *See* Smith v. Maryland, 442 U.S. 735, 751 (1979) (Marshall, J., dissenting) ("The use of pen registers, I believe, constitutes such an extensive intrusion. To hold otherwise ignores the vital role telephonic communication plays in our personal and professional relationships . . . ." (citing Katz v. United States, 389 U.S. 347, 352 (1979)); United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) ("[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.").

as recently as 2018, albeit with at least one exception.[34] This expansive approach to the third-party doctrine, whereby Fourth Amendment protection is lost with any sharing to any third-party, ostensibly arises from *Katz v. United States*,[35] the seminal case on whether a search or seizure has taken place and thus whether the Fourth Amendment applies to any government action. However, the current categorical approach to the third-party doctrine rests on a fundamental misreading of that case's key language. Rather than categorically excluding all shared information from Fourth Amendment protection, the Court in *Katz* articulated a fact-intensive test: "What a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[36] Embedded within this short phrase is a two-part test that requires a nuanced, as-applied analysis of, first, whether information was in fact knowingly exposed, and second, whether that exposure was made to the public. This Part shows that subsequent cases have read down in various ways both prongs of that test.

In addition, subsequent cases have also equated this test with the similar, yet distinct, false-friend doctrine. In the false-friend line of cases, the Court held that individuals have no reasonable expectation of privacy in information shared with a confidant who then reveals it to the government.[37] Under the third-party doctrine as articulated in *Katz*, the Fourth Amendment does not cover information knowingly exposed "to the public." These are conceptually distinct—under the false-friend doctrine, the information sharer takes a *risk* their information will be exposed by their friend and so left unprotected, but under the third-party doctrine, the information is unprotected regardless of how the third party responds.[38] By both misreading the *Katz* test and creating a false equivalence between the false-friend doctrine and the third-party doctrine, the Court leaves unprotected all information "voluntarily turn[ed] over to third parties."[39] While this overinclusive sharing doctrine has been somewhat cabined by modern

34 Carpenter v. United States, 138 S. Ct. 2206, 2216–17, 2220 (2018) ("[W]hile the third-party doctrine applies to telephone numbers and bank records, it is not clear whether its logic extends to the qualitatively different category of cell-site records.").

35 Katz v. United States, 389 U.S. 347 (1967).

36 *Id.* at 351 (first citing Lewis v. United States, 385 U.S. 206, 210 (1966); and then citing United States v. Lee, 274 U.S. 559, 563 (1927)).

37 United States v. White, 401 U.S. 745 (1971); Hoffa v. United States, 385 U.S. 293 (1966); *Lewis*, 385 U.S. 206; On Lee v. United States, 343 U.S. 747 (1952).

38 *See* discussion *infra* Section I.D.

39 *Carpenter*, 138 S. Ct. at 2216 (quoting Smith v. Maryland, 442 U.S. 735, 743–44 (1979)).

courts,[40] the limitations are developed in an ad hoc "I know it when I see it" standard that provides little guidance to government agents or reviewing courts.

A. Katz *and the Origin of the Third-Party Doctrine*

The third-party doctrine originated with the declaration in *Katz* that "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection."[41] To understand why this public exposure limitation was necessary, we must delve into the *Katz* case itself, for the third-party doctrine was a counterbalance to expanding what could constitute "unreasonable searches and seizures" beyond the traditional confines of a person's home or property and into any area where a person has a "reasonable expectation of privacy."[42]

"Give me Duquesne minus 7 for a nickel," Charles Katz said in a phone call with his bookie.[43] Unbeknownst to Mr. Katz, FBI agents were recording this conversation, and he would soon face up to two years in prison for illegal interstate gambling.[44] The FBI had placed recording devices on two phone booths that Katz used almost daily.[45] These recording devices could be turned on and off by nearby agents, recorded only Katz's side of conversations, and were taped to the outside of the phone booths—all factors that, under traditional analysis, indicate the recordings did not constitute searches.[46] The FBI used these recordings to obtain a warrant to search Katz's apartment, where more evidence of illegal gambling was found.[47]

In finding for Mr. Katz, the Supreme Court held that the traditional property-based determination of what constitutes an illegal search or seizure was too "narrow" and did not adequately take into

40 *Id.* at 2222 (holding that cell site location information, despite being held by a third party, conveys too much information about a user's whereabouts and cannot be shared with the government without a warrant).

41 *Katz*, 389 U.S. at 351 (first citing *Lewis*, 385 U.S. at 210; and then citing *Lee*, 274 U.S. at 563).

42 *See id.* at 360 (Harlan, J., concurring).

43 Katz v. United States, 369 F.2d 130, 132 (9th Cir. 1966), *rev'd*, 389 U.S. 347 (1967).

44 Matthew Lasar, *The Crooks Who Created Modern Wiretapping Law*, ARS TECHNICA (June 2, 2011), https://arstechnica.com/tech-policy/2011/06/the-crooks-who-created-modern-wiretapping-law/2/ [https://perma.cc/K7JY-TEXY].

45 *Katz*, 369 F.2d at 131.

46 *See* Olmstead v. United States, 277 U.S. 438, 466 (1928) (noting that without "actual physical invasion of his house 'or curtilage' for the purpose of making a seizure," the Fourth Amendment is not implicated).

47 *Katz*, 369 F.2d at 132.

account changing technology.[48] According to the Court, as long as there is some indicia of the existence of a subjective and objective expectation of privacy, then "[w]herever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures."[49]

The Court in *Katz* was rejecting its 1928 decision, *Olmstead v. United States*, which held that placing wiretaps on public phone lines without a warrant did not constitute an illegal search because government agents did not infringe upon Olmstead's property rights.[50] In the 1920s, during the height of Prohibition, Roy Olmstead managed a bootlegging operation in the Pacific Northwest that employed over fifty people and earned in excess of $2,000,000 per year.[51] The FBI, without warrants, placed wiretaps on public phone lines and in an office building's publicly accessible basement to intercept phone calls between Olmstead and his team.[52] Over seventy-two people were indicted, and the recordings were used to convict Olmstead at trial.[53] Olmstead challenged the use of the wiretaps, claiming that recording and using private telephone conversations violated both the Fourth and Fifth Amendments.[54] The majority held that neither Amendment was implicated, basing the analysis in large part on the fact that the government agents never invaded Olmstead's property; as Chief Justice Taft wrote for the majority, there was neither a search nor a seizure because "[t]here was no entry of the houses or offices of the defendants."[55]

It is important to note the dissent from Justice Brandeis, who presciently argued that limiting the Fourth Amendment's reach to a property-based standard inadequately prepares the Amendment for future challenges posed by changing surveillance technology. Essentially, Justice Brandeis argued that although trespass may address the use of wiretaps, "[w]ays may some day be developed by which the Government, without removing papers from secret drawers, can

48 Katz v. United States, 389 U.S. 347, 353 (1967) ("[O]nce it is recognized that the Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures, it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion . . . .").

49 *Id.* at 359.

50 *Olmstead*, 438 U.S. at 466 (finding that the Fourth Amendment has not been violated "unless there has been an official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion" which "the wire tapping here . . . did not amount to").

51 *Id.* at 456.

52 *Id.* at 456–57.

53 *Id.* at 455.

54 *Id.*

55 *Id.* at 464.

reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home."[56] It was this perceived limitation of the property-based model to respond to technological advancement that led the Court in *Katz*, forty years later, to make the question one of a person's privacy expectations, rather than formal demarcations of their property boundaries—that is, to define Fourth Amendment protection in terms of "people, not places."[57]

Evaluating the legality of a search based on what was gathered rather than how it was taken represented a dramatic redistribution of Fourth Amendment protections. The Fourth Amendment has long been understood as balancing two key interests: individual privacy and governmental needs.[58] By moving the Fourth Amendment into the public sphere, new limitations were needed to balance the newly expanded coverage. Changing technology meant that there were novel ways to communicate and surveil, so information moving outside the home needed protection.[59] But if the distinction between what was in the home and what was out of the home was no longer a limiting principle, a different means of determining *which* places outside of the home were protected was required. The solution *Katz* provided was to shift the focus to one of knowledgeable public exposure: "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[60] The public exposure limit was essential for the *Katz*ian test not to be all-encompassing. However, the public exposure qualification also had limits, ones that shortly came to be misunderstood by the Court itself, allowing instead for the public exposure caveat to swallow up much of the Fourth Amendment protection of *Katz*.

---

56 *Id.* at 474 (Brandeis, J., dissenting).

57 Katz v. United States, 389 U.S. 347, 351 (1967).

58 *See* Delaware v. Prouse, 440 U.S. 648, 654 (1979) (noting that the reasonableness of a search "is judged by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests").

59 Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 515 (2011) ("[T]he power to monitor communications in a phone booth when a person placed a call was the modern equivalent to the power to break into a home and listen to conversations there.").

60 *Katz*, 389 U.S. at 351–52 (internal citations omitted) (first citing Lewis v. United States, 385 U.S. 206, 210 (1966); then citing United States v. Lee, 274 U.S. 559, 563 (1927); then citing Rios v. United States, 364 U.S. 253 (1960); and then citing *Ex parte* Jackson, 96 U.S. 727, 733 (1878)).

B. Losing Katz*'s First Prong: Unknowingly Shared Is Not "Knowingly Expose[d]"*

The first two post-*Katz* cases that addressed shared information accessed without a warrant misread both prongs of the *Katz* test, effectively replacing a reasonableness analysis with a per se rule based solely on whether information was shared with any third party.[61] These two cases, *United States v. Miller*[62] and *Smith v. Maryland*,[63] laid the groundwork for a per se third-party doctrine that is ill-suited for our modern information-sharing age.[64]

In 1973, following the discovery of illegal whiskey distilling equipment on property owned by Mitch Miller, investigators from the Treasury Department's Alcohol, Tobacco and Firearms Bureau subpoenaed local banks holding Mr. Miller's accounts to provide all records of his bank transactions to date to a grand jury.[65] The banks complied, and the records were used as supporting evidence in Miller's trial.[66] Miller challenged the warrantless seizure of his bank documents, arguing that he had a reasonable expectation that they would be kept private.[67] The Supreme Court disagreed, finding that Miller had no reasonable expectation of privacy in the documents.[68] In making this determination, the Court quoted the relevant language from *Katz*.[69] Yet the Court went through none of the *Katz*ian voluntary exposure to the public analysis, writing only that "[a]ll of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[70] The Court continued: "The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[71]

The Court's analysis assumes that it was unreasonable to expect documents given to a bank teller to remain private without explaining

---

61 Under the correct *Katz*ian analysis, both cases likely would have come out differently. *See* discussion *infra* Section III.D.

62 425 U.S. 435 (1976).

63 442 U.S. 735 (1979).

64 United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) ("This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.").

65 *Miller*, 425 U.S. at 437–38.

66 *Id.*

67 *Id.* at 442.

68 *Id.* at 443.

69 *Id.* at 442.

70 *Id.*

71 *Id.* at 443 (citing United States v. White, 401 U.S. 745, 751–52 (1971) (plurality opinion)).

why Miller should have known that he lacked any privacy right in the financial documents, either subjectively—for example, asking if the bank teller mentioned anything about document privacy to Miller—or objectively—for example, asking if the bank had a posted policy about document privacy. The Court instead points to the fact that banks must keep transaction records under the Bank Secrecy Act and syllogistically reasons that (1) since banks have to keep records, and (2) banks are a third party, (3) information shared with banks is unprotected by the Fourth Amendment.[72] In doing so, it is quietly substituting an overly simplistic and underinclusive categorical sharing rule in place of a case-by-case *Katz*ian analysis of privacy expectations.

The analysis in *Miller* took a large leap away from *Katz*'s two-prong test. Like a game of judicial telephone, in the next major case, *Smith v. Maryland*, the Court relied on *Miller*'*s* misreading of *Katz* to further misinterpret the "voluntary sharing with the public" notion.[73] In 1976, Baltimore police suspected Michael Lee Smith in a robbery; police believed that the robber had then begun making threatening phone calls to the victim, but police had little evidence and no probable cause.[74] Investigators contacted the telephone company and requested, without a warrant, that a pen register—a device that records the numbers dialed by a particular phone line—be placed on Smith's home telephone.[75] The pen register recorded a phone call from Smith to the victim, and police then used this information to get a warrant to search Smith's home, where they discovered evidence linking him to the robbery.[76] Smith challenged the legality of the warrantless use of the pen register, claiming that it was an illegal search under the Fourth Amendment.[77]

The Court held that the use of the pen register was not a search. According to the majority, "[t]his Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[78] The Court continued:

> When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and "exposed" that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed. The switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally

72 *Id.* at 443–44.
73 *See* Smith v. Maryland, 442 U.S. 735 (1979).
74 *Id.* at 737.
75 *Id.*
76 *Id.*
77 *Id.* at 742.
78 *Id.* at 743–44.

> completed calls for the subscriber. Petitioner concedes that if he had placed his calls through an operator, he could claim no legitimate expectation of privacy. We are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate.[79]

By equating an automated system with a human third party, *Smith* completes the transition from *Katz*ian privacy analysis to *Miller*'s categorical privacy assumptions. After *Smith*, information that no human being is ever likely to see is considered shared with a third party. This jump was problematic back in 1976 but it is downright dangerous in our current digital world; now, third parties host emails, store photos, and record health data and travel information.[80] By assuming the privacy analysis *and* extending that to automated systems, the *Smith* Court left little room for any privacy expectation in an enormous number of activities of modern life.

The combination of first equating "exposure" with sharing in a public way and then further equating sharing with an automated third party as sharing with an individual is particularly dangerous, as the dissent notes:

> [E]ven assuming, as I do not, that individuals "typically know" that a phone company monitors calls for internal reasons, . . . it does not follow that they expect this information to be made available to the public in general or the government in particular. Privacy is not a discrete commodity, possessed absolutely or not at all.[81]

As the dissent points out, the majority opinion rests on two faulty conclusions. First, that it is reasonable to know exactly what happens when you make a phone call, and second, that knowing a third party has access to your information means a reasonable person should expect that information has been exposed to the public.[82] This misreading further entrenched the move from a two-pronged public exposure test to a per se sharing rule. In making this radical yet unacknowledged transformation, the Court further exposed everyday activities to the risk of greater state intrusion.

---

79 *Id.* at 744–45 (internal citation omitted) (citing Transcript of Oral Argument at 3–5, 11–12, 32, *Smith*, 442 U.S. 735 (No. 78-5374)).

80 See Section III.C below for further discussion on the significance of having no human agent.

81 *Smith*, 442 U.S. at 749 (Marshall, J., dissenting) (internal citation omitted) (citing *Smith*, 442 U.S. at 743 (majority opinion)).

82 *See id.* at 749–50.

1. Jettisoning the "Knowingly" Requirement: Introducing "Voluntariness"

The first prong of the third-party test articulated by *Katz*, whether the information has been "knowingly expose[d]," itself has two parts: "knowingly" and "expose[d]."[83] In addition to substituting a per se sharing rule in place of a case-by-case *Katz*ian analysis to assess if information has been "knowingly" shared, the Court in *Miller* and *Smith* also redefined both specific elements of the first prong. We deal with each in turn.

Katz explicitly included a knowledge requirement, but neither *Miller* nor *Smith* incorporate this as part of their analysis. In *Miller*, the bank kept records of transactions and deposits as required by the Bank Secrecy Act.[84] As the dissent notes, "[i]t cannot be gainsaid that the customer of a bank expects that the documents, such as checks, which he transmits to the bank in the course of his business operations, will remain private, and that such an expectation is reasonable."[85] Yet, the opinion of the Court did not address whether or not Miller knew these records were being kept, and for what purpose. Nevertheless, it found that the Fourth Amendment did not apply to these records.[86]

In *Smith*, the Court did address the knowledge element but disposed of it with little analytical rigor, relying on a bald assertion of what the public is likely to know:

> [W]e doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must "convey" phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills. In fact, pen registers and similar devices are routinely used by telephone companies "for the purposes of checking billing operations, detecting fraud, and preventing violations of law."[87]

What is especially troubling about this disregard for the knowledge component is that, unlike in *Miller*, Smith "shared" his phone call information with an automated system that facilitates phone calls. How can something be knowingly exposed to an

---

83 Katz v. United States, 389 U.S. 347, 351 (1967) (first citing Lewis v. United States, 385 U.S. 206, 210 (1966); and then citing United States v. Lee, 274 U.S. 559, 563 (1927)).

84 United States v. Miller, 425 U.S. 435, 436 (1976).

85 *Id.* at 448 (Brennan, J., dissenting) (quoting Burrows v. Superior Ct., 529 P.2d 590, 593–96 (Cal. 1974)).

86 *Id.* at 440.

87 *Smith*, 442 U.S. at 742 (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 174–75 (1977)).

automated conduit, to a third party whose entire purpose is to process that information? In *Miller* and *Smith*, the Court effectively read the knowledge requirement out of the third-party doctrine, and in doing so, it left unprotected a host of records and information kept, knowingly or unknowingly, by any third party, regardless of their purpose within the information transaction—both the type of information available in the 1970s when the Court was deciding these cases, but also vast amounts of information that would come to be voluntarily "shared" in the future.[88]

Without a strong knowledge prong, complacency increases the risk of privacy loss. As technology becomes more ubiquitous and more automated, the government gains greater access into users' activities and personal lives.[89] For example, in the 1980s and early 1990s, courts routinely found that communication over cordless telephones was unprotected by the Fourth Amendment because their signals could be intercepted by AM/FM radios or common radio equipment purchasable at any electronics store.[90] Despite *Katz*'s explicit acknowledgement of the importance of telephonic communication and the general Fourth Amendment special protection of the home,[91] the ubiquity of the radio equipment alone gave the government access to all communication over cordless phones.

An element that makes the Court approving government access to otherwise private information via the third-party doctrine especially dangerous is the issue of where the government is going to access this data. This information is not being gathered from people with their consent in any meaningful way and then marshalled by the government to combat this disease. Instead, third parties like Facebook and Google, with whom millions of Americans constantly share their location information simply by having their applications on their phones,[92] are collecting and giving this information to the government upon request.[93] As such, anyone who wants to have a cell phone—

88 *See* discussion *infra* subsection I.B.2.

89 David A. Sklansky, *Back to the Future:* Kyllo*,* Katz*, and Common Law*, 72 MISS. L.J. 143, 202 (2002); *see also* Kyllo v. United States, 533 U.S. 27, 47 (2001) (Stevens, J., dissenting) ("[I]t seems likely that the threat to privacy will grow, rather than recede, as the use of intrusive equipment becomes more readily available.").

90 Sklansky, *supra* note 89, at 203.

91 *See* discussion *infra* Section II.A.

92 Justin Pot, *Facebook Is Tracking Your Phone's Location, Here's How to Review Your History*, HOW-TO GEEK (May 30, 2018), https://www.howtogeek.com/fyi/facebook-is-tracking-your-phones-location-heres-how-to-review-your-history/ [https://perma.cc/C8DE-DCGU].

93 *See* Jack Nicas & Daisuke Wakabayashi, *Apple and Google Team Up to 'Contact Trace' the Coronavirus*, N.Y. TIMES (June 3, 2020), https://www.nytimes.com/2020/04/10

something that the Court in *Carpenter* recognized as so fundamental to modern life that government access to certain types of information constituted an exception to the third-party doctrine's per se application[94]—will, without a similar exception being crafted by the Court, have "voluntarily" shared that private health information.

This chipping away at the knowledge requirement is particularly pertinent in response to government efforts to control the spread of COVID-19. Many countries, including the United States, have turned to electronic surveillance as a means of both tracking those infected[95] and monitoring adherence to social distancing guidelines.[96] While the Court's decision in *Carpenter* could apply to this gathering of data, there is a strong logical argument that, because the information is shared with a third party, the Fourth Amendment would be inapplicable. Given the fact that this type of location data can be used for everything from commercial advertisements to identifying who attends political campaign events,[97] relying on the "goodwill" of the government and multi-billion-dollar companies in handling sensitive and private information seems insufficient.[98] Even if such access begins in the context of a global pandemic, once so accessed, the current Court interpretation of the third-party doctrine would render it forever able to be accessed, as it will have been deemed to be publicly exposed.[99] Clearly, a knowledge component, as articulated in *Katz*, would better protect information like this from falling victim to

/technology/apple-google-coronavirus-contact-tracing.html [https://perma.cc/2RNP-UTRL].

94 Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) ("We decline to extend *Smith* and *Miller* to cover these novel circumstances. Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection.").

95 Nicas & Wakabayashi, *supra* note 93.

96 Craig Timberg, Elizabeth Dwoskin, Drew Harwell & Tony Romm, *Governments Around the World Are Trying a New Weapon Against Coronavirus: Your Smartphone*, WASH. POST (Apr. 17, 2020), https://www.washingtonpost.com/technology/2020/04/17/governments-around-world-are-trying-new-weapon-against-coronavirus-your-smartphone/ [https://perma.cc/9SKD-PM9S].

97 Sam Schechner, Emily Glazer & Patience Haggin, *Political Campaigns Know Where You've Been. They're Tracking Your Phone*, WALL ST. J. (Oct. 10, 2019), https://www.wsj.com/articles/political-campaigns-track-cellphones-to-identify-and-target-individual-voters-11570718889 [https://perma.cc/6YV6-CLSG].

98 Sara Morrison, *The Government Might Want Your Phone Location Data to Fight Coronavirus. Here's Why That Could Be Okay*, VOX (Mar. 18, 2020), https://www.vox.com/recode/2020/3/18/21184160/government-location-data-coronavirus [https://perma.cc/ZZ83-F6WG] ("Right now, we're relying on the goodwill of both the government and the tech companies to have our interests in mind.").

99 See Conclusion below for further discussion of the impact of the third-party doctrine on the response to the COVID-19 pandemic.

societal complacency and provide better protection as more technology is unknowingly shared with more facilitating third parties.

2. Redefining Any Sharing as "Exposure"

Not only did the Courts in *Miller* and *Smith* read the "knowingly" requirement out of the *Katz* test, they equated exposure with sharing. This is still the current standard set by the Court,[100] and a common standard by which the Fourth Amendment is approached academically.[101] Yet we show here that these words differ at the plain meaning level, and that ignoring this difference has led to an expansive rule that over time encompasses more and more information shared, sent, and stored through third parties.

To "expose" is defined as "to make known" and "to cause to be visible or open to view."[102] It can be accomplished with a third party or without. This has two significant implications: first, the onus rests on the exposer, not on any particular recipient. Second, this emphasizes that the "knowingly expose" and the "to the public" requirements both have a public element to them—the former in terms of the action of the sharer and the latter in terms of the nature of the recipient. This second aspect illustrates both that the "public" element should not be downplayed, since it is twice incorporated in the test, and it again emphasizes that the *Katz* test draws distinctions between the sharer and the recipient—our solution explores the significance of these demarcated roles.[103] It is also important to retain the public distinction: as Judge Posner writes, "[o]ne must not confuse solitude with secrecy."[104] The *Katz* test specifically uses the word "expose," and the Court has since reinforced that language.[105]

100 *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

101 *See* RICHARD A. POSNER, NOT A SUICIDE PACT: THE CONSTITUTION IN A TIME OF NATIONAL EMERGENCY 140 (2006) ("Informational privacy does not mean refusing to share information with everyone."); Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 122 (2002) ("[T]reating exposure to a limited audience as identical to exposure to the world, means failing to recognize degrees of privacy in the Fourth Amendment context."); Kerr, *supra* note 31, at 571 ("The Justices envision privacy as an on-off switch, equating disclosure to one with disclosure to all, and as a result they miss the many shades of gray.").

102 *Expose*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/expose [https://perma.cc/B4UN-G7QF].

103 *See infra* Section III.C.

104 POSNER, *supra* note 101, at 140.

105 Katz v. United States, 389 U.S. 347, 351 (1967); Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) ("We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras.").

To "share," on the other hand, is defined as "to partake of, use . . . to grant or give a share in."[106] In contrast to exposing, sharing is defined by the relationship between the sharer and the recipient. This difference is not simply rhetorical. If you write a confession to a crime on a piece of paper and tape it to your forehead, you are exposing that information. If you write your confession on a piece of paper, fold it up, and give it to a friend to keep in their pocket, you have shared it with them, but it has not yet been exposed. This is a vital distinction. The friend has autonomy to do with your confession what they want. Your friend might be false, and they might share your confession with the police. But significance of the truth or falsity of their friendship is governed by a separate doctrine, the false-friend doctrine.[107] The third-party doctrine is instead focused on whether actions taken by the primary individual reveal the information. And as *Katz* made clear, sharing information—be it a confession written on a piece of paper or betting information shared over the telephone—is not the same as exposing it: Katz shared that information with his friend but he did not expose it, and so it was still protected.[108]

Legally, reading these two different concepts as one created a rule that was too expansive and so left too much information open for warrantless collection. As Katz shared his betting information with his friend, Miller may have shared his deposit slips and bank statements with bank employees who handled those documents, and Smith may have shared the numbers he dialed with the phone company, in that he gave them to an automated system owned by the company. However, the Court never grapples with the complexity of the *Katz* standard, instead opting to revoke Fourth Amendment protection because the information was voluntarily *conveyed* to a third party, which, to the Court, necessarily means that the information has been "exposed."[109]

This misreading also runs counter to one of *Katz*'s more groundbreaking principles: that unavoidable provision of information does not equal exposure. While it may be unavoidable that pen numbers are shared with the telephone company, or that copies of deposited checks pass through the hands of bank employees, it was also unavoidable that sound leaks out of a public telephone booth or a person's lips can be read. However, as the Court said in *Katz*, once the

106 *Share*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/share [https://perma.cc/VS6B-5Q5Z].

107 The false-friend doctrine holds that a person "assumes the risk" in sharing information with a third party that the person may betray them, but if that betrayal does not occur, the information remains protected—discussed in detail below in Section I.D.

108 *See Katz*, 389 U.S. at 348.

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

toll is paid and the door is shut, that information is nevertheless inaccessible without a warrant.[110] Information can be unavoidably shared, just as if a passerby had overheard Katz talking in the phone booth. But when the standard is knowing exposure, information does not lose its Fourth Amendment protection simply because a third party has access to it.

C. Abandoning Katz*'s Second Prong: The Disappearing "Public"*

The second prong of the third-party test articulated by *Katz* is whether the information has been knowingly exposed *to the public*.[111] Again, the Court in *Miller* and *Smith* misread *Katz*, equating the public as equivalent to any single third party.[112] Not only does this run contrary to the plain meaning of "public," which is defined as "exposed to general view,"[113] but it also runs contrary to the way "the public" is viewed by the Court in other doctrines. In the seminal defamation case, *Florida Star v. B.J.F.*, the Court wrote, "We also recognized that privacy interests fade once information already appears on the public record."[114] Privacy interests did not fade once a third party had access to the information; rather, those interests were limited when it appeared on the broader public record. Similarly, in patent law, the Court has written that the public domain encompasses works "already available to the public or that which may be readily discerned from publicly available material."[115] Something does not enter the public domain when it is shared with another person, but rather when it is "available to the public" more broadly.

The distinction between a third party and the public is important when the facts of *Katz* are examined in more detail. Katz disclosed his conversation to the recipient, and possibly the phone company that connected the call, in the same way that Smith disclosed the telephone numbers he dialed to the telephone company and Miller conveyed the checks he deposited to the bank employees. *Miller* and *Smith* assumed that when a third party has access to information, that information is

110 *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

111 *Id.* at 351 (majority opinion) (first citing Lewis v. United States, 385 U.S. 206, 210 (1966); and then citing United States v. Lee, 274 U.S. 559, 563 (1927)).

112 *Miller*, 425 U.S. at 442 (Miller shared his bank records with a single entity: the bank); Smith v. Maryland, 442 U.S. 735, 744 (1979) (Smith shared his phone numbers with a single entity: the phone company).

113 *Public*, MERRIAM-WEBSTER, https://www.merriamwebster.com/dictionary/public [https://perma.cc/J2JU-LRAX].

114 Fla. Star v. B.J.F., 491 U.S. 524, 532 n.7 (1989) (citing Cox Broad. Corp. v. Cohn, 420 U.S. 469, 494–95 (1975)).

115 Bonito Boats, Inc. v. Thunder Craft Boats, Inc., 489 U.S. 141, 150 (1989).

no longer shielded by the Fourth Amendment.[116] *Katz* never made that jump. In fact, *Katz* would have come out differently if it was decided after *Miller* and *Smith* overlaid their interpretation of *Katz* itself on the third-party doctrine. In the words of *Smith*, by sharing the phone call with the call recipient, Mr. Katz

> can claim no legitimate expectation of privacy here. When he used his phone, petitioner voluntarily conveyed [his conversation] to the [recipient] and "exposed" that information . . . in the ordinary course of business. In so doing, petitioner assumed the risk that the [recipient] would reveal to police the [contents of the conversation].[117]

Yet, this quote perfectly describes what Katz did. By equating the risk that a single third party might reveal information with exposure *to the public*, *Miller* and *Smith* contradicted their progenitor, *Katz*.

In an effort to solve this problem with the *Miller–Smith* interpretation of *Katz*, some scholars argue that "the public" indicates a requirement that a larger audience have the information before the Fourth Amendment is implicated.[118] However, this solution is itself problematic. The use of the word "public" typically denotes an exposure level, not a size of audience. Furthermore, the way the Court has interpreted the concept of the "public" in the aforementioned defamation and patent contexts makes it clear that something can be in the public domain and yet seen by nobody. The requirement is that is must be *available* to the public. It is unwieldy, both for government agents and reviewing courts, to turn Fourth Amendment protections on and off based on the size of the audience. Likewise, in *Katz*, it was central that by shutting the door and paying the toll, the conversation was deemed not available to the public. But in the same way, neither dialing a phone number automatically recorded by a telephone company nor depositing a check with a bank teller make that information *available to the public*.

If Person A posts a confession to a crime to their 10,000 followers on Twitter, that confession has obviously been knowingly exposed to the public. If Person B posts a confession to a crime to Twitter, but they have zero followers, then nobody can see their posts, but they have likewise exposed their information to the public, assuming their profile is not private. Both Person A and Person B have paid no toll, shut no door, nor exhibited any actions indicating an intent to retain

116 *Miller*, 425 U.S. at 443; *Smith*, 442 U.S. at 745.

117 *Smith*, 442 U.S. at 744.

118 Colb, *supra* note 101, at 153 (critiquing allowing "government officials to treat as knowingly exposed to the world (and thus to the police as well) not only those things that have been exposed to the public at large, but also those things that have been knowingly exposed to *any* third party").

their right to privacy. Both have knowingly shared with the public—the mere availability of each post triggers the second prong, regardless of the size of the audience.

* * *

Both elements—knowing exposure and to the public—create a commonsense limitation on Fourth Amendment protection in the public sphere, one that balances expanded privacy protection for "people, not places,"[119] with government investigatory needs. The per se sharing doctrine articulated by *Miller* and *Smith* was a misreading of *Katz* that risks leaving a significant amount of personal information unprotected by the Fourth Amendment. The per se rule is simple to apply but is increasingly hard to justify in the information age. Returning to the two-part third-party test articulated in *Katz* provides more analytical nuance and allows the Fourth Amendment to appropriately recalibrate with changing technology.

D. Trust Nobody: False Friends and Third Parties

In establishing a per se third-party doctrine, where any sharing is automatically treated as abolishing any reasonable expectation of privacy, *Miller* and *Smith* relied in large part on the Court's false-friend jurisprudence. The false-friend doctrine holds that when a person shares information with another person, they "assume the risk" that the recipient is a false friend working with the government.[120] According to the Court, because any friend could potentially be false, the sharer cannot rely on a reasonable expectation of privacy if the friend shares the information, and so the Fourth Amendment does not protect them.[121] There is clearly a similarity here between false friends and third parties, but the two doctrines are different, and by conflating them, the Court misunderstood them both, further distancing the third-party doctrine from its legal and logical foundation in *Katz*.

To understand how the third-party doctrine was corrupted by subsuming the false-friend doctrine, we need to briefly review the development of the false-friend cases and the logic behind the

119 *See* Katz v. United States, 389 U.S. 347, 351 (1967).

120 *See* United States v. White, 401 U.S. 745, 749 (1971); Hoffa v. United States, 385 U.S. 293, 302 (1966); Lewis v. United States, 385 U.S. 206, 211 (1966); On Lee v. United States, 343 U.S. 747, 751 (1952).

121 Donald L. Doernberg, *"Can You Hear Me Now?": Expectations of Privacy, False Friends, and the Perils of Speaking Under the Supreme Court's Fourth Amendment Jurisprudence*, 39 IND. L. REV. 253, 255 (2006) ("[E]vidence revealed to the government by a confidant of the defendant is admissible precisely because there is no reasonable expectation of privacy in such situations.").

doctrine. Prior to *Miller*, these cases were largely relegated to conversations between individuals and undercover government agents.[122] The logic was that because any friend can go to the police and tell them the information or show them the incriminating evidence, then having an undercover agent listen in on a conversation is no different—the sharer has assumed the risk that the friend is false, in one way or another.[123]

Confidential informants, secret agents, and undercover operatives have long been vital tools in government investigations.[124] In the first of the Court's major false-friend cases, *On Lee v. United States*,[125] the government had arrested and charged On Lee for dealing narcotics.[126] While out on bail, On Lee had conversations in his laundromat with Chin Poy, a former employee turned government agent, during which he made "damaging admissions" about his case.[127] Unbeknownst to On Lee, Chin Poy was wearing a wire, which transmitted his conversations to government agents stationed outside. On Lee argued that Chin Poy had trespassed when he entered the laundromat under false pretenses.[128] The Court disagreed, holding that On Lee consented to Chin Poy's presence, regardless of the underlying motives for the conversation.[129] Essentially, the Court embraced the idea that a false friend can effectively undermine a person's reasonable expectation of privacy.

A decade later, the Court subsequently expanded this notion into the home, in two major false-friend cases handed down on the same day. In *Lewis v. United States*,[130] the defendant invited an undercover government agent into his home in order to purchase narcotics.[131] Lewis argued that any warrantless government intrusion into his home constituted a violation of the Fourth Amendment.[132] Chief Justice Warren, writing for the majority, disagreed, holding that, since the government agent was invited into the home to purchase drugs and had not affirmatively misrepresented his purpose in order to gain

122 *See White*, 401 U.S. at 746–47; *Hoffa*, 385 U.S. at 296; *Lewis*, 385 U.S. at 207; *On Lee*, 343 U.S. at 747, 749.

123 *White*, 401 U.S. at 759 (Douglas, J., dissenting) ("The risk of being overheard by an eavesdropper or betrayed by an informer or deceived as to the identity of one with whom one deals is probably inherent in the conditions of human society.").

124 *See* Kerr, *supra* note 31, at 576.

125 *On Lee*, 343 U.S. at 747.

126 *Id.* at 748.

127 *Id.* at 749.

128 *Id.* at 751–52.

129 *Id.* at 752.

130 385 U.S. 206 (1966).

131 *Id.* at 207.

132 *Id.* at 208.

entry, the surreptitious purchase was not a search under the Fourth Amendment and no warrant was required.[133] This expansion of the false-friend doctrine made it clear that the special protection of the home does not guard against a false friend—we are taking a risk when we invite someone into our most intimate space, and can lose our ordinary expected protections even within the home.

The second case, *Hoffa v. United States*,[134] reinforced the application of the false-friend doctrine to the home (including the temporary home of a hotel room), and also expanded the doctrine further, including those paid to be false friends by the government. In 1962, James Hoffa, president of the Teamsters Union, was arrested and charged with violating the Taft-Hartley Act.[135] While on trial, Hoffa met with a co-defendant to discuss bribing jurors.[136] Edward Partin, a Teamsters Union official and paid informant for the government, was also in the room and overheard the comments.[137] He relayed the conversation to a government agent, and the comments were later used to convict Hoffa and his co-defendants for jury tampering.[138] Hoffa argued that, because Partin did not disclose his role as a paid informant, any consent Hoffa gave to Partin to be in the hotel room was negated.[139] The Court disagreed. Writing for the plurality, Justice Stewart wrote:

> Partin did not enter the suite by force or by stealth. He was not a surreptitious eavesdropper. Partin was in the suite by invitation, and every conversation which he heard was either directed to him or knowingly carried on in his presence. The petitioner, in a word, was not relying on the security of the hotel room; he was relying upon his misplaced confidence that Partin would not reveal his wrongdoing.[140]

Hoffa's notion of "misplaced confidence" would go on to become the crux of the false-friend doctrine. As long as the third party was a friend (knowingly in the protected space), it did not matter what made them false. But as we see below, this element came to be expanded far more when applied beyond the context of friends, via incorporation into the third-party doctrine, to include faceless organizations that an individual does not know in any meaningful sense and has little choice

133 *Id.* at 211.
134 385 U.S. 293 (1966).
135 *See id.* at 294.
136 *Id.* at 296.
137 *Id.* at 296, 298.
138 *Id.* at 294–95.
139 *Id.* at 300.
140 *Id.* at 302.

over whether to "invite in" to their home and their other private spaces.

On Lee, *Lewis*, and *Hoffa* allowed the government to do what they otherwise could not—by using a third-party agent, government investigators were able to gain access to the home and private property of suspects in ways they could not do themselves without a warrant.[141] Yet these cases all predated *Katz*, and it was unclear if they would survive the move to a reasonable expectation of privacy test.

The Court's first opportunity to evaluate false-friend cases under the new *Katz*ian regime was *United States v. White*.[142] The facts of *White* are quite similar to those in *On Lee*. James White was convicted on charges of narcotics trafficking, largely based on conversations between him and Harvey Jackson, a government informant.[143] Jackson wore a radio transmitter that broadcast their conversations to nearby police officers.[144] Justice White, writing for a plurality, affirmed the legality of *On Lee*, *Lewis*, and *Hoffa*, explaining that

> the law permits the frustration of actual expectations of privacy by permitting authorities to use the testimony of those associates who for one reason or another have determined to turn to the police, as well as by authorizing the use of informants in the manner exemplified by *Hoffa* and *Lewis*.[145]

As well as confirming that the false-friend analysis applies under *Katz*, *White* also extended the application of the doctrine to wireless transmission, saying: "If the law gives no protection to the wrongdoer whose trusted accomplice is or becomes a police agent, neither should it protect him when that same agent has recorded or transmitted the conversations which are later offered in evidence to prove the State's case."[146] *White* has been criticized on both of these fronts. On the former, critics have argued that whereas *Katz* sought to expand Fourth Amendment protection for conversations that took place over changing technology (the telephone), *White* eliminated protection based on changing technology (radio transmitters).[147] On the latter, *White* is criticized as undermining a person's feeling of freedom and

141 *See* On Lee v. United States, 343 U.S. 747, 766 (1952) (Burton, J., dissenting) ("[I]f Lee, under like conditions, without warrant and without authority, entered the room with Chin Poy and, while concealed, overheard petitioner's conversation with Chin Poy, Lee's testimony should be excluded.").

142 401 U.S. 745 (1971).

143 *Id.* at 746–47 (plurality opinion).

144 *Id.*

145 *Id.* at 752.

146 *Id.*

147 Tracey Maclin, Katz, Kyllo, *and Technology: Virtual Fourth Amendment Protection in the Twenty-First Century*, 72 MISS. L.J. 51, 75–78 (2002) ("[T]he protective shield of *Katz* was just as ineffective in *Smith* as it was in *White*.").

privacy by rendering a person subject to recording at any time, because now a person has to assume not only that they could be talking to a government agent, but that the person they are talking to could also be wearing a wire.[148] But there is a much more fundamental problem with *White* that has not been emphasized previously: by combining the false-friend doctrine with the third-party doctrine, the Court in *White* misunderstands both doctrines. This doctrinal confusion diminishes privacy interests far more than the decision of whether a particular technological development can be differentiated from the overall direction of prior case law.

First, the false-friend doctrine was meant to be a narrow exemption from the normal presumption of an expectation of privacy, applying to a "wrongdoer[] . . . confid[ing] his wrongdoing."[149] Under the *Miller* and *White* interpretation, now a "depositor . . . revealing his affairs to another"[150] loses his Fourth Amendment protection simply because of the possibility "that the information will be conveyed by that person to the Government."[151] The Court took the relatively narrow notion that all conversations with secret agents are unprotected by the Fourth Amendment and expanded it, effectively turning a person's bank teller into an undercover agent for the government. By equating these two doctrines, the Court answers the age-old question: If a tree falls in the forest and nobody is around to hear it, does it make a sound because the government *could* have heard it? If so, that sound can be acquired without a warrant.

Second, the false-friend doctrine is premised on the notion that a person *takes a risk* when confiding in a friend: the risk that that friend may be false. But this notion of risk necessarily contains two potential outcomes: if the friend is false, the confider loses out; but if the friend is true, the confider has taken a risk but has won that gamble. Their information has been shared with the friend, yet their privacy remains intact. When the Court implicitly incorporated the false-friend doctrine into the third-party doctrine, it warped this fundamental logic. Rather than acknowledging these dual potential outcomes, the Court assumed that when a person confides to a friend, or any third party, that friend *must* be false.[152] But that is not the risk that the person takes in taking a confidant: they risk the *possibility* of betrayal, not the certainty. By treating any sharing as an automatic and entire

148 *White*, 401 U.S. at 790 (Harlan, J., dissenting).

149 *Id.* at 749 (plurality opinion).

150 United States v. Miller, 425 U.S. 435, 443 (1976).

151 *Id.*

152 *See id.* ("The depositor takes the risk, in revealing his affairs to another, that the information *will* be conveyed by that person to the Government." (emphasis added) (citing *White*, 401 U.S. at 751–52)).

loss of any reasonable expectation of privacy, the Court is essentially treating every friend as false. Thus, the third-party version of the false-friend doctrine is a distorted one.

Third, the Court's approach in combining the third-party and false-friend doctrines undermines the very notion of the *Katz*ian reasonable expectation of privacy. Under a reasonable expectation of privacy analysis, the Court must ascertain whether the information sharer reasonably expected their information to be exposed, and part of that analysis is an inquiry into the knowledge of the individual.[153] Instead of undertaking this inquiry, *Miller* assumed all third parties were false, and *Smith* similarly assumed everybody knew their friends were false.[154] In *Smith*, the Court's analysis of the reasonable expectation of privacy in dialed telephone numbers utilized a very thin application of facts—claiming that "all subscribers" know that the phone company records which numbers are dialed,[155] a factual claim that was somewhat dubious at the time, as the dissent notes[156]—and concluded therefore that there is no expectation of privacy in a person's call log.[157] Having undertaken this *Katz*ian analysis once, in the context of a landline phone system, the Court then assumed that conclusion to apply *in all other cases*, by making the third-party doctrine categorical rather than a case-by-case assessment. However, regardless of the rigor—or lack thereof—in the Court's factual claim and its legal conclusion, telephones were just one very limited factual application. Since then, the Court has simply *assumed* that same conclusion applies to numerous other factual questions, regardless of whether the application is to entirely different technology (such as an encrypted email account), whether the technology application is completely automated and always has been (unlike the previously sentient telephone operator), and whether the equivalent of the phone book information is available to the new technology user (or if in fact the provider has made promises not to access such information).

For example, it would be difficult for a court to conclude—without blushing—that a person has no expectation of privacy in their heart rate information just because they use a third-party application

153 Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 NW. U. L. REV. 139, 152 (2016).

154 *See Miller*, 425 U.S. at 443; Smith v. Maryland, 442 U.S. 735, 743 (1979) ("[I]t is too much to believe that telephone subscribers . . . harbor any general expectation that the numbers they dial will remain secret.").

155 *Smith*, 442 U.S. at 742.

156 *Id.* at 748–49 (Marshall, J., dissenting) (analyzing the claim that "individuals somehow infer from the long-distance listings on their phone bills . . . that pen registers are regularly used for recording local calls").

157 *Id.* at 743 (majority opinion).

in their watch.[158] But instead of undertaking the difficult task of explaining why a person should not have any privacy expectation in their heart rate information, the Court need only cite *Miller* and *assume* that answer, based on the automatic application of the third-party doctrine. Then a court need only ask if there was some exception that might apply, based on the scope of the governmental inquiry[159] or the nature of the intrusion.[160] But what *Katz* requires is that the court ask that more difficult question. The Court in *Smith* provided a roadmap for avoiding *Katz*'s difficult knowledge question; by assuming the implicit claim when making this third-party argument, the Court had no need to examine the individual or societal expectations of privacy in telephones, or heart rate monitors, or any other application where a third party has a person's information, however private it may appear to the ordinary person.

* * *

If knowledge is a required part of the analysis, why does the Court so often avoid this inquiry that *Katz* demands? It is likely an issue of judicial economy: evaluating the societal and individual knowledge of a particular subject on a case-by-case basis, especially in today's information age, would be fact- and resource-intensive, and would likely lead to legal uncertainty as different courts apply different standards to determine what is "reasonable."[161] So, if it is problematic to assume knowledge of a third party's actions, but it also impractical to gauge that knowledge on a case-by-case basis, what is the solution? Our solution provides a straightforward mechanism for ascertaining whether a person in fact has a reasonable expectation of privacy in a given situation, including using a third-party application, without those additional resource costs. Applying the "knowing exposure to the public" analysis provides the best of both worlds—by looking at who the individual is contracting with and the circumstances of that contract, it is easy to efficiently and effectively assess whether a

158 *Cf.* Kris Holt, *Fitbit Data Helps Police Arrest Another Murder Suspect*, ENGADGET (Oct. 4, 2018), https://www.engadget.com/2018-10-04-fitbit-data-heart-rate-murder-arrest.html [https://perma.cc/UHV4-3S8X] (describing an investigation in which police used a murder victim's heart rate data recorded on her Fitbit to identify her alleged killer).

159 *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 n.3 (2018) ("It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.").

160 *See* Kyllo v. United States, 533 U.S. 27, 40 (2001) (holding that warrantless government use of technology not in public use—in this case a thermal detection device used to detect heat spikes—to search a home is unconstitutional).

161 See Section III.B below for more on the difficulty of applying a reasonableness standard to the third-party doctrine.

reasonable person would have an expectation of privacy or not. This gets at the *Katz*ian mandate without being so fact-intensive as to be uncertain, as explored further in Part III. But first, Part II illustrates why this is not simply a concern about doctrinal purity: it shows that the actual effect of the Court's distorted third-party doctrine has the potential to massively contract and contort privacy interests that society recognizes as reasonable and that individuals hold dear.

II. WHEN THE CURE IS WORSE THAN THE DISEASE

Over one hundred million Alexa-enabled devices sit inside customers' homes, constantly listening as they wait for a "wake word" to activate.[162] Once that word is spoken, Alexa devices continue to record for a period of time after communication has ended.[163] That information is stored forever in order to learn from and remember a user's commands.[164] And while companies like Amazon have so far been resistant to revealing information to the government without a warrant, the value of an in-home recording device has not gone unnoticed by the police.[165] Similarly, Nest, the camera and thermostat company, has received over three hundred information requests from the government since 2015.[166] Nest thermostats use biometric sensors to record when their users are physically at home and which rooms they use most often to create a tailored and efficient heating and cooling schedule.[167] Information given to Alexa or Nest from within the home has been shared, often in the ordinary course of business, with a third party. As such, under the Court's current articulation of the third-party doctrine, that information is likely accessible without a warrant by government investigators.

This Part examines how the Court's current categorical third-party doctrine applies to these and other modern applications. It

162 Judith Shulevitz, *Alexa, Should We Trust You?*, ATLANTIC (Nov. 2018), https://www.theatlantic.com/magazine/archive/2018/11/alexa-how-will-you-change-us/570844/ [https://perma.cc/2ZHT-XBJ7].

163 *Id.*

164 Geoffrey A. Fowler, *Alexa Has Been Eavesdropping on You This Whole Time*, WASH. POST (May 6, 2019), https://www.washingtonpost.com/technology/2019/05/06/alexa-has-been-eavesdropping-you-this-whole-time/ [https://perma.cc/Y4T9-P9D3].

165 Burke, *supra* note 10; Zack Whittaker, *Judge Orders Amazon to Turn Over Echo Recordings in Double Murder Case*, TECHCRUNCH (Nov. 14, 2018), https://techcrunch.com/2018/11/14/amazon-echo-recordings-judge-murder-case/ [https://perma.cc/L3CP-TQ4P].

166 Thomas Brewster, *Smart Home Surveillance: Governments Tell Google's Nest to Hand Over Data 300 Times*, FORBES (Oct. 13, 2018), https://www.forbes.com/sites/thomasbrewster/2018/10/13/smart-home-surveillance-governments-tell-googles-nest-to-hand-over-data-300-times/ [https://perma.cc/5SBV-MDFK].

167 *See* Fowler, *supra* note 164.

shows that, as technology rapidly progresses, the implications of the Court's approach continue to massively expand the potential for state intrusion on individual privacy. It also shows that the doctrine does so in a way that is inconsistent with much else of Fourth Amendment law.

A. How Special Is the Home?

It is well-established that the "Fourth Amendment draws 'a firm line at the entrance to the house.'"[168] The idea that a person's home is their sanctuary, unreachable by government intrusion "without some specific charge upon oath,"[169] was a widely accepted feature of pre-Revolution English common law.[170] It was the Founders' "desire to protect the privacy and security of their homes from promiscuous intrusion" that led to the constitutional protection against unreasonable searches and seizures.[171]

For over a century, the boundaries of the home were where the Fourth Amendment began and ended. Courts literally parsed whether government intrusion pierced[172] or merely touched[173] the outer walls of a house to determine if an action constituted a search. This presumptive protection of the home implicitly acknowledges that illegal actions can be rendered unreachable by virtue of their taking place inside the home, and the Court has struck this balance time[174] and again,[175] protecting illegal behavior that occurred within the home from warrantless government intrusion. The focus was where the

168 Kyllo v. United States, 533 U.S. 27, 40 (2001) (quoting Payton v. New York, 445 U.S. 573, 590 (1980)).

169 Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1237 (2016) (quoting J. ALMON, A LETTER CONCERNING LIBELS, WARRANTS, THE SEIZURE OF PAPERS, AND SURETIES FOR THE PEACE OR BEHAVIOUR; WITH A VIEW TO SOME LATE PROCEEDINGS, AND THE DEFENCE OF THEM BY THE MAJORITY 58 (3d ed., London 1765) (signed by "The Father of Candor")).

170 *See* Entick v. Carrington [1765] EWHC (KB) J98, 95 Eng. Rep. 807 (finding that the King's agents had trespassed); Tracey Maclin, *The Complexity of the Fourth Amendment: A Historical Review*, 77 B.U. L. REV. 925, 933 (1997) (describing the reversal of the common law presumption that "an Englishman's home was the King's castle" to a person's own); Donohue, *supra* note 169, at 1203 ("In vain has our house been declared, by the law, our asylum and defence, if it is capable of being entered, upon any frivolous or no pretence at all, by a secretary of state." (quoting Wilkes v. Wood (1763) 98 Eng. Rep. 489, 490)).

171 Maclin, *supra* note 170, at 955.

172 *See* Silverman v. United States, 365 U.S. 505, 509 (1961) (holding that warrantless use of a "spike mike" to penetrate walls and eavesdrop was unconstitutional).

173 *See* Goldman v. United States, 316 U.S. 129, 134–35 (1942) (holding that warrantless use of a detectaphone pressed up against the wall of an adjoining room and used to eavesdrop was constitutional).

174 *Kyllo*, 533 U.S. at 40.

175 Florida v. Jardines, 569 U.S. 1 (2013) (holding that bringing a drug-sniffing dog onto a private porch without a warrant was unconstitutional).

government accessed the information, an inquiry firmly rooted in the doctrine of trespass, which meant that while behavior that remained within the home could be protected, behavior that began in the home but was observed in public was not.[176]

The inquiry shifted after *Katz*, expanding protection to temporarily private applications outside the home. Developing the new "reasonable expectation of privacy" test in place of trespass analysis, the Court reformulated the Fourth Amendment as protecting "people, not places."[177] The Fourth Amendment was now free to enter the public sphere. But, despite the (temporary) move away from a trespass-defined doctrine, importantly, *Katz* was meant to expand beyond the confines of the home, not to undermine the special protection for the home.[178] However, subsequent interpretation of *Katz* via the third-party doctrine used reasonable expectation analysis to radically undermine the protection of the home.

The uniqueness of the home permeates the jurisprudence of the Fourth Amendment. In *Kyllo v. United States*,[179] government agents used a thermal imaging device to show that an unusual amount of heat was radiating from the petitioner's garage. This information was used to obtain a search warrant for petitioner's home on the assumption that the halide lights used to grow marijuana indoors create an unusual amount of heat. Agents subsequently found over one hundred marijuana plants growing in petitioner's garage. The Court held that the warrantless use of the thermal imaging device was an impermissible search because the Fourth Amendment "draws 'a firm line at the entrance to the house.'"[180] The Court refused to limit this special protection by assessing "which home activities are 'intimate' and which are not."[181] In *Florida v. Jardines*,[182] the sanctity of the home was so strong that Court held the warrantless use of a drug-sniffing dog—ordinarily not a search at all[183]—was an unconstitutional search when conducted on the front porch of a private residence.[184]

176 Olmstead v. United States, 277 U.S. 438, 466 (1928).

177 Katz v. United States, 389 U.S. 347, 351 (1967).

178 United States v. Jones, 565 U.S. 400, 406–07 (2012).

179 533 U.S. 27 (2001).

180 *Id.* at 40 (quoting Payton v. New York, 445 U.S. 573, 590 (2012)).

181 *Id.* at 38–39.

182 569 U.S. 1 (2013).

183 United States v. Place, 462 U.S. 696, 707 (1983) ("[E]xposure of respondent's luggage, which was located in a public place, to a trained canine—did not constitute a 'search' within the meaning of the Fourth Amendment.").

184 *Jardines*, 569 U.S. at 6 (noting that "the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion" is at the "very core" of the Fourth Amendment).

The sanctity of the home in the search and seizure context has persisted for centuries and remains a pivotal part of nearly every application of the Fourth Amendment.[185] Yet the one area where the home's heightened protection is not respected is in the third-party doctrine. As the Court held in *Smith*, the government could access the phone numbers dialed in the privacy of Smith's home because they had been exposed to the phone company.[186] Similarly, in *White*, the Court held that the government could use a wireless transmission that incriminated the defendant, even when one of those conversations took place in the defendant's home.[187] The current third-party doctrine's ability to pierce the home puts one of the bastions of the Fourth Amendment at risk.

The significance of the potential intrusion that this doctrine permits has only increased with rapidly developing technology, such as communication services. In 2008, Skype, a telecommunications application that specializes in providing video chat and voice calls between computers and tablets, categorically denied the possibility that their peer-to-peer online voice and video calls could be tapped.[188] Microsoft walked that language back after purchasing Skype in 2011, and for good reason: a 2012 National Security Agency (NSA) document conveniently titled "User's Guide for PRISM Skype Collection" was part of a trove of leaked documents detailing how Microsoft allowed the NSA access to its servers in order to search and monitor communication over the Skype system. While this warrantless monitoring ostensibly targeted only non-U.S. citizens, what was eventually recorded was a network of information including anything said or chatted between the targeted individual and any recipient, citizen or not.[189] Why did Microsoft feel free to give the NSA this kind of extensive access to its users' data? The reason is that the Court's expansive interpretation of the third-party doctrine has given governments and companies expansive powers over individuals' otherwise private information. Quite simply, Skype users were not protected by the Fourth Amendment because their information was carried by a third party.

185 Collins v. Virginia, 138 S. Ct. 1663 (2018) (holding that a vehicle parked on the curtilage of the home cannot be searched without a warrant).

186 Smith v. Maryland, 442 U.S. 735, 744 (1979).

187 United States v. White, 401 U.S. 745, 754 (1971).

188 Declan McCullagh, *NSA Docs Boast: Now We Can Wiretap Skype Video Calls*, CNET (July 11, 2013), https://www.cnet.com/news/nsa-docs-boast-now-we-can-wiretap-skype-video-calls/ [https://perma.cc/QA2F-2U92].

189 Sean Gallagher, *Newly Published NSA Documents Show Agency Could Grab All Skype Traffic*, ARS TECHNICA (Dec. 30, 2014), https://arstechnica.com/tech-policy/2014/12/newly-published-nsa-documents-show-agency-could-grab-all-skype-traffic/ [https://perma.cc/85PP-ADPL].

Those same leaked documents showed that, from 2003 to 2013,[190] AT&T gave the NSA access to billions of emails that passed through its domestic networks.[191] AT&T was "highly collaborative," installing surveillance equipment for the government in seventeen of its American internet hubs.[192] In 2011, AT&T began handing over 1.1 billion domestic calling records per day.[193] And while the NSA's program was shuttered in 2017, a recent report confirmed that AT&T continues to give Drug Enforcement Administration officers access to billions of domestic and international call records which show when and where calls were made and by whom.[194] Again, AT&T was free to do so because calls and emails made from inside the home were likely left unprotected simply because they were managed by a third party, AT&T.

In 2019, a cache of leaked documents revealed that Skype relied on human contractors to augment their translation service.[195] As these documents showed, Skype's translation service, ostensibly run by artificial intelligence and machine learning software, often used human contractors to analyze voice data and improve the AI's algorithms.[196] Skype's website did mention that calls may be analyzed to improve translation functionality, yet nowhere did it say that countless third-party Skype employees were part of that process.[197] While Microsoft responded that all identifying information was removed before the contractors were given access, they did not deny that Microsoft employees not only had the ability, but also the employment responsibility, to listen in as users conducted job interviews, repeated names and full addresses, discussed travel plans, or even engaged in phone sex.[198] Had the government requested

190 Julia Angwin, Charlie Savage, Jeff Larson, Henrik Moltke, Laura Poitras & James Risen, *AT&T Helped U.S. Spy on Internet on a Vast Scale*, N.Y. TIMES (Aug. 15, 2015), https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html [https://perma.cc/75CD-4L5K].

191 *Id.*; Dante D'Orazio, *Leaked NSA Documents Show AT&T Had a 'Highly Collaborative' Relationship with Spy Agency*, VERGE (Aug. 15, 2015), https://www.theverge.com/2015/8/15/9159777/att-had-a-highly-collaborative-relationship-with-the-nsa [https://perma.cc/MY4X-DAXN].

192 Angwin et al., *supra* note 190.

193 *Id.*

194 Zack Whittaker, *DEA Says AT&T Still Provides Access to Billions of Phone Records*, TECHCRUNCH (March 28, 2019), https://techcrunch.com/2019/03/28/hemisphere-phone-records/ [https://perma.cc/9KY8-R6HH].

195 Joseph Cox, *Revealed: Microsoft Contractors Are Listening to Some Skype Calls*, VICE: MOTHERBOARD (Aug. 7, 2019), https://www.vice.com/en_us/article/xweqbq/microsoft-contractors-listen-to-skype-calls [https://perma.cc/EFB5-E5DU].

196 *Id.*

197 *Id.*

198 *Id.*

information from Skype about a user's voice or video chat history, under the Court's current third-party jurisprudence, that information was likely accessible by government investigators without a warrant, even if the conversation occurred entirely in the caller's home.

While a dog sniffing around on a person's front porch is a Fourth Amendment search, a doorbell recording that dog may not be, due to the current third-party doctrine. Amazon has partnered its Ring doorbell camera with over four hundred local police departments.[199] These police departments offer reduced cost, or even free, Ring doorbell systems, often at taxpayer expense, in exchange for access to a fast-growing network of private security cameras.[200] In some cases, these Ring giveaways are conditioned on full release of videos upon request.[201] Cooperating police departments also get access to the Ring Neighbors app, a free download allowing Ring owners to post videos, view crime information, and comment on other users' posts.[202] Amazon, Ring's parent company, has already developed facial recognition software used by police nationwide.[203] As applied so far, information is being shared with the police voluntarily, but if that were not the case, it may make no difference, because of the Court's stringent interpretation of the third-party doctrine.

When the information is on—or even in—a person's body, a doctrine designed to address pen registers seems especially outdated. Fitbit data has been used in several murder investigations to determine time of death.[204] But there is no reason that police use of such information need be limited to the information of the victim. By virtue of wearing a Fitbit, users share their heart rate, location, distance traveled, and even sleep patterns with a third party. Under the current third-party doctrine, there is no privacy interest in that most fundamentally personal information. As such, police could use Fitbit incriminating evidence of the suspect's increased heart rate, location information, etc., at the time of a crime, all without a warrant.

In each of these real-world applications, information is shared with a third party, and thus is fair game for government investigators.[205]

---

199 Drew Harwell, *Doorbell-Camera Firm Ring Has Partnered with 400 Police Forces, Extending Surveillance Concerns*, WASH. POST (Aug. 28, 2019), https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach [https://perma.cc/FAP8-E8YZ].

200 *Id.*

201 Alfred Ng, *Amazon's Helping Police Build a Surveillance Network with Ring Doorbells*, CNET (June 5, 2019), https://www.cnet.com/features/amazons-helping-police-build-a-surveillance-network-with-ring-doorbells/ [https://perma.cc/XC2R-XN7Y].

202 *Id.*

203 *Id.*

204 *See, e.g.*, Holt, *supra* note 158.

205 *See* Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018).

And, in contrast to all other applications of Fourth Amendment doctrine, this problem is not solved by the presumption of the home protection, because the third-party doctrine has consistently been interpreted to overcome that presumption and allow the government to enter the home without a warrant. Thus, the Supreme Court's current interpretation of the third-party doctrine is not simply incompatible with the foundational pillars of *Katz*, the landmark case from which the doctrine was birthed; it is irreconcilable with all Fourth Amendment doctrine in which the sanctity of the home is paramount.

B. Some *People and* Some *Places*

After *Katz*, the Fourth Amendment ostensibly protected people, not places, expanding the Fourth Amendment beyond the confines of the home and bringing it into the public sphere. Yet the Court has been highly selective in how it has done so, using the current categorical approach to the third-party doctrine to pick and choose when and to whom the Fourth Amendment applies, and when it does not.

DNA, the substance that literally makes a person one of "we the people," is potentially accessible to government agents under the modern Court's third-party approach. Tens of millions of people have shared their DNA with companies like 23AndMe and Ancestry looking for everything from genealogical history to medical data and disease predisposition.[206] These companies are third parties; by sending in DNA samples, customers are indirectly sharing this highly personal information with government investigators,[207] and (often unwittingly) adding their genetic information to national databases.[208] The third-party doctrine gives the lie to the constitutional protection of "people, not places."

Technological change is exacerbating this failure to protect people and their most private information. As discussed, the *Miller* Court established a categorical bar on Fourth Amendment protection for information shared with third parties; because of this, even in the face of quite different circumstances, the Court continues to fail to

206 Jessica Bursztynsky, *More than 26 Million People Shared Their DNA with Ancestry Firms, Allowing Researchers to Trace Relationships Between Virtually All Americans: MIT*, CNBC (Feb. 12, 2019), https://www.cnbc.com/2019/02/12/privacy-concerns-rise-as-26-million-share-dna-with-ancestry-firms.html [https://perma.cc/KL82-L858].

207 Kristen V. Brown, *Major DNA Testing Company Sharing Genetic Data with the FBI*, BLOOMBERG (Feb. 1, 2019), https://www.bloomberg.com/news/articles/2019-02-01/major-dna-testing-company-is-sharing-genetic-data-with-the-fbi [https://perma.cc/296G-FC8A].

208 Sara Boboltz, *Judge Says Police Can Search Company's Entire DNA Database*, HUFFPOST (Nov. 5, 2019, 6:07 PM), https://www.huffingtonpost.ca/entry/police-search-dna-database_n_5dc1dc4ee4b08b735d616096 [https://perma.cc/4E62-ZFFB].

apply *Katz* to quite different banking scenarios. Police officers frequently use debit and credit card transactions to track suspected criminals, accessed following a subpoena, or upon request to a third party by government investigators.[209] Yet banking records have come a long way from the paper statements in *Miller*.[210] Now, purchase records can show the date and time of purchase, the location of the purchase, and sometimes even the purchased product, all without a warrant.

The Court worsened the problem in *Jones*, by promoting a trespass analysis that, by the Court's own analysis, has questionable application in an increasingly technological world.[211] In reinvigorating the role of trespass in search and seizure analysis,[212] the Court turned "people, not places," into (some) people and (some) places, re-emphasizing the physical importance of the home and other property but leaving the large hole in that doctrine represented by the third-party doctrine unaddressed. The only Justice who addressed the issue at all cast doubt on its long-term survival. As Justice Sotomayor noted in her concurrence, the third-party doctrine, as articulated in *Smith* and *Miller*, 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," including "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."[213] But the Court has failed to heed Justice Sotomayor's clarion call on the dangers of the third-party doctrine.[214]

The sole area in which the Court has addressed the problem is the application of cell phone data. This is an important area for the third-party doctrine—not only is location information shared with a cellular company (a third party), but smartphones contain thousands of third-party applications that monitor and record location and other

209 John Egan, *How Credit Cards Can Lead Law Officers to Criminals*, CREDITCARDS.COM (Sept. 18, 2018), https://www.creditcards.com/credit-card-news/credit-cards-track-criminals.php [https://perma.cc/Y9EK-6YH6].

210 United States v. Miller, 425 U.S. 435, 438 (1976).

211 United States v. Jones, 565 U.S. 400, 426 (2012) (Alito, J., concurring) (arguing that revitalizing trespass does not respond sufficiently to electronic searches).

212 *Id.* at 406 (majority opinion) ("[W]e must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001))).

213 *Id.* at 415, 417 (Sotomayor, J., concurring) (quoting People v. Weaver, 909 N.E.2d 1195, 1199 (2009)).

214 Discussed further below in Section III.A.

personal information.[215] Yet the Court's cell phone data doctrine, as articulated in *Carpenter*, is both subjective and exceedingly narrow.[216] The Court refused to solve the broader difficulties created by its third-party doctrine, or even to recognize the breadth of those underlying problems.[217] The Court reaffirmed *Smith* and *Miller*'s categorical exemption for information shared with third parties generally, while at the same time relying on an analysis of the quantity of the information shared with the third party to determine whether the Fourth Amendment applied in this narrow application.[218] As the majority maintained, "[t]he Government will be able to use subpoenas to acquire records in the overwhelming majority of investigations. We hold only that a warrant is required in the rare case where the suspect has a legitimate privacy interest in records held by a third party."[219] And that rare case involved the relatively high bar of "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years."[220] After *Jones* and *Carpenter*, we are left with a third-party doctrine that is categorical, unless it is isn't; that protects people, sometimes, but not places, including the home.

Our proposed reinterpretation of the third-party doctrine, drawing it back to the fundamental principles of *Katz*, provides a solution to both this doctrinal problem and the dilemmas raised by these practical applications. Extending Fourth Amendment protection to data that is not *knowingly* exposed to the *public*, as *Katz* set out, would better reconcile third-party doctrine with the "long view" of the Fourth Amendment that the Court takes in other areas.[221] While many of these situations involve warrant requests, others rely simply on subpoenas. Constitutional privacy protections should not depend on the judgement of private companies, substituting for the detached and neutral judgment of a magistrate. Many companies may publicly

215 Stuart A. Thompson & Charlie Warzel, Opinion, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html [https://perma.cc/3VSH-CG9M].

216 *See* discussion *infra* Conclusion.

217 Although the dissent did: Carpenter v. United States, 138 S. Ct. 2206, 2262 (2018) (Gorsuch, J., dissenting) ("Today we use the Internet to do most everything. Smartphones make it easy to keep a calendar, correspond with friends, make calls, conduct banking, and even watch the game. Countless Internet companies maintain records about us and, increasingly, *for* us.").

218 *Id.* at 2222 (majority opinion).

219 *Id.* In fact, the actual ruling was even narrower, applying only to historical records exceeding more than seven days. *Id.* at 2217 n.3.

220 *Id.* at 2220.

221 Kyllo v. United States, 533 U.S. 27, 40 (2001).

"resist" government requests in their official privacy policies,[222] but without strong legal protections, the only thing standing between the government and access to increasingly detailed personal information is a for-profit company.

Now, consumers generally rely on the market to encourage companies to prioritize consumer privacy. However, as technology becomes more integrated in our lives and homes, the opportunity for abuse becomes greater. Without adequate constitutional protections and a clear third-party standard informing both government investigators and private companies of the proper boundaries of the Fourth Amendment, if the market for privacy lags behind the market for government cooperation, corporate priorities can shift.[223] The current third-party doctrine offers no clear impediment to expanding the use of these tools for increased surveillance, and we should not wait for the problem to move from science fiction to scientific fact before we find solutions.

III. SOLVING THE THIRD-PARTY DILEMMA: RETURNING TO *KATZ*

Fourth Amendment jurisprudence and scholarship aims to find a balance between privacy and security.[224] The third-party doctrine is an important limit on the reach of the Fourth Amendment: without it, the state would be forced to ignore information in the public domain.[225] It is in the best interest of society for government investigators to be able to investigate crime. For instance, *Miller* is instrumental in financial fraud investigations, as information shared with banks is viewed as unprotected by the Fourth Amendment's warrant requirement.[226] More generally, providing criminals with a technological

222 Peter Aldhous, *This Genealogy Database Helped Solve Dozens of Crimes. But Its New Privacy Rules Will Restrict Access by Cops*, BUZZFEED NEWS (May 19, 2019), https://www.buzzfeednews.com/article/peteraldhous/this-genealogy-database-helped-solve-dozens-of-crimes-but [https://perma.cc/D5SL-TUYH].

223 For example, GEDmatch previously had a strong opt-in policy for use of genetic information by police; it was recently purchased by a company that provides DNA sequencing information to crime labs. Jennifer Lynch, *Genetic Genealogy Company GEDmatch Acquired by Company with Ties to FBI & Law Enforcement—Why You Should Be Worried*, ELEC. FRONTIER FOUND. (Dec. 10, 2019), https://www.eff.org/deeplinks/2019/12/genetic-genealogy-company-gedmatch-acquired-company-ties-fbi-law-enforcement-why [https://perma.cc/HQ8V-BUQV].

224 Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 354 (1974); Kerr, *supra* note 31, at 574.

225 *See supra* Part I.

226 Jeremy Ciarabellini, *Cryptocurrencies' Revolt Against the BSA: Why the Supreme Court Should Hold that the Bank Secrecy Act Violates the Fourth Amendment*, 10 SEATTLE J. TECH. ENV'T & INNOVATION L. 135, 138, 147 (2020) (arguing that *Miller* and the Supreme Court's third-

cloak of invisibility in an age where most communication is done online would severely hamper the ability of police and government agents to do their jobs.[227] However, we are a long way from spike bugs and radio transmitters: third parties sit in our living rooms and record our families' conversations.[228] There is almost nothing in our lives that third parties do not touch.[229] Courts struggled to find that security-privacy balance when government investigators merely retrieved dialed phone numbers;[230] as more and more third parties enter our homes, lives, and bodies, maintaining that balance becomes even more treacherous. The Court's current construction tilts too heavily in favor of security over privacy; in the digital age, the third-party doctrine has become one of the biggest threats to the privacy-security balance.

But the doctrine can be fixed. In this Section, we examine the competing judicial and academic solutions to the third-party doctrine conundrum, and then explain why giving substantive meaning to the "knowing[] expos[ure] to the public" test articulated in *Katz* would restore balance between privacy and security. By combining a knowledge requirement with an evaluation of the nature of the third-party, this test limits the scope of the doctrine while at the same time providing government investigators—and reviewing courts—a clear, ex ante standard to apply.

A. Too Many Cooks: The Supreme Court's Solutions

After years of skirting around the inherent problems with the modern application of the third-party doctrine,[231] the Supreme Court faced the issue directly in 2018, in *Carpenter v. United States.*[232] Suspecting Mr. Carpenter in a series of robberies, police requested access to his CSLI from his cellular service provider. CSLI records are created when a cell phone moves into the vicinity of a nearby cell tower. Under a strict application of the third-party doctrine, CSLI is a third-party business record, unprotected by the Fourth Amendment.

---

party doctrine application is wrong, but that the current articulation insulates the Bank Secrecy Act from constitutional challenge).

227 *See generally* Tonja Jacobi & Jonah Kind, *Criminal Innovation and the Warrant Requirement: Reconsidering the Rights-Police Efficiency Trade-off,* 56 WM & MARY L. REV. 759 (2015) (describing the need for law enforcement agencies to innovate in response to criminal innovation).

228 Fowler, *supra* note 164.

229 *See* examples *supra* Part II.

230 Smith v. Maryland, 442 U.S. 735, 737–38 (1979).

231 United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring); Riley v. California, 573 U.S. 373, 385 (2014) (opining on the importance of cell phones to our daily lives).

232 138 S. Ct. 2206 (2018).

However, the government acquired and analyzed 127 days' worth of CSLI, effectively tracking Carpenter for over four months.[233] *Carpenter* brought to a head the risk that a strict following of the categorical third-party sharing rule espoused in *Smith* and *Miller* could lead to essentially ubiquitous and comprehensive warrantless surveillance.

Many hoped that the Court would use *Carpenter* to provide clarity on the state of the doctrine; many were disappointed.[234] The Court instead dodged the difficult question and fudged a simple solution, simultaneously affirming the categorical *Smith-Miller* third-party doctrine but exempting weeks' worth of highly specific location tracking.[235] What resulted was an admittedly narrow holding that endorsed a categorical rule with ad hoc exemptions determined by their "uniqueness."[236] This approach amounts to a judicial whack-a-mole that provides little surety to citizens currently living with third-parties recording conversations in their living rooms, and even less guidance to government investigators hoping to listen to those recordings.

The majority opinion in *Carpenter* acknowledges the new digital reality: technology has changed since *Smith* was decided in 1979, and the amount of information shared through phones and third parties dwarfs the dialed phone numbers at issue in that case.[237] Yet, rather than rethink its problematic categorical articulation of the doctrine, the majority upheld both *Smith* and *Miller*, choosing simply to not apply those cases to the "unique" facts at issue.[238] However, these facts are not unique—there are countless devices and applications that provide

233 *Id.* at 2212–13.

234 Christopher C. Fonzone, Kate Heinzelman & Michael R. Roberts, *Carpenter and Everything After: The Supreme Court Nudges the Fourth Amendment into the Information Age*, 58 INFRASTRUCTURE 3, 3 (2019) ("Would it hold that the Amendment offers no protection to the digital tracks that are a necessary byproduct of the Information Age? Or would it reverse a doctrine that law enforcement officials have relied on for two generations? In fact, the Court appeared to do neither."); Elizabeth De Armond, *Tactful Inattention: Erving Goffman, Privacy in the Digital Age, and the Virtue of Averting One's Eyes*, 92 ST. JOHN'S L. REV. 283, 296 (2018) ("Nonetheless, the reach of *Carpenter* is narrow for the moment . . . ."); Orin Kerr, *Understanding the Supreme Court's* Carpenter *Decision*, LAWFARE BLOG (June 22, 2018, 1:18 PM), https://www.lawfareblog.com/understanding-supreme-courts-carpenter-decision [https://perma.cc/8CPF-LKH2] (writing that the third-party doctrine lives, but with an equilibrium adjustment cap).

235 *Carpenter*, 138 S. Ct. at 2220. Although some have argued that *Carpenter* might do more work than its language indicates—*see* Kerr, *supra* note 234—without a formal test, individuals must rely on the whims of lower courts interpreting vague language.

236 *Carpenter*, 138 S. Ct. at 2217.

237 *Id.* ("After all, when *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements.").

238 *Id.*

far more information than CSLI: for instance, there are watches that keep track not only of a person's location, but of the wearer's heart rate, calorie count, step count, and sleep cycles.[239] Investigators and lower courts must now analogize a Ring doorbell to *Carpenter*'s CSLI dumps, or differentiate a simple Fitbit step counter from those comprehensive health monitor watches, and numerous other variations of such devices, in order to determine if they are subject to the warrant requirement. *Carpenter* did limit the third-party doctrine, but it left open the questions of when, where, and how much.

The four individual dissenting opinions in *Carpenter* are worth analyzing, as they are representative of the debate surrounding the third-party doctrine and indicative of the doctrine's divisiveness. Justice Kennedy's logic is simple: CSLI is a routine business record owned by the phone company that the government "has a lawful right to obtain by compulsory process" under *Miller* and *Smith*.[240] He criticizes the majority opinion's shift from a categorical distinction to a balancing test that weighs privacy interests against the fact of third-party disclosure.[241] And, in a particularly important point directly addressing the privacy-security balance, Justice Kennedy writes that CSLI is "uniquely suited" to linking individual perpetrators with criminal acts.[242] In doing so, he includes usefulness to government investigators as a factor in his analysis. Justice Kennedy downplays the risk to privacy, arguing that CSLI is not particularly accurate and does not pose a substantial risk.[243]

Although this opinion is consistent with precedent, it overvalues security at the expense of privacy. Justice Kennedy provides little analysis of how this categorical view would address a more detailed tracking system, or third-party activity in the home. Could police warrantlessly track where you are in your home because you send that information to your smart thermostat? Could they subpoena video from inside your home because you share that with your security system company? Is your sleep cycle fair game simply because it is stored on a third-party cloud hosting service? And Justice Kennedy barely acknowledges customer knowledge, simply assuming it is reasonable for cell phone owners to expect information collected by the phone company will be used for "a variety of business and

239 *See, e.g.*, *Forerunner® 735XT*, GARMIN, https://buy.garmin.com/en-US/US/p/541225 [https://perma.cc/7LHC-GD5X].

240 *Carpenter*, 138 S. Ct. at 2223–24 (Kennedy, J., dissenting).

241 *Id.* at 2232 ("*Miller* and *Smith* do not establish the kind of category-by-category balancing the Court today prescribes.").

242 *Id.* at 2226.

243 *Id.* at 2233.

commercial purposes."[244] Justice Kennedy treats the main points of analysis in a third-party doctrine question as (1) whether the information is sold to third parties and (2) whether it is helpful to police; under this analysis, the restrictions of the Fourth Amendment become nothing more than a paper tiger. While Justice Kennedy's opinion is consistent with prior opinions, it would shift the Fourth Amendment balance dangerously towards security and away from privacy, putting everything from Alexa recordings to email at risk of warrantless search.

Justices Alito and Thomas signed on to Justice Kennedy's dissent, but Justice Alito also wrote separately to address a central quandary with the majority's opinion: either the holding applies broadly, and is better able to respond to changing technology while greatly restricting the third-party doctrine, or it applies in an ad hoc way, leaving the doctrine "subject to all sorts of qualifications and limitations that have not yet been discovered."[245] But ironically, Justice Alito then creates his own exception, arguing that the Fourth Amendment should not apply to subpoenas and compelled production. According to Justice Alito, a subpoena should not be held to the same standard as a search, as the risks of government overreach are simply not present when government agents are not doing the searching,[246] and doing so "would cripple the work of courts in civil and criminal cases alike."[247] So Justice Alito's solution actually has two significant disadvantages: he strays from precedent to carve out an entirely new exception for Fourth Amendment searches for subpoenaed information, while criticizing the majority for the same thing, and at the same time shifting the balance even more sharply towards security and away from privacy.

Justice Thomas largely agreed with Justice Alito, writing individually to argue *Katz*'s reasonable expectation of privacy is neither based in history nor easily applied, and, as such, should be overturned.[248] Justice Thomas would prefer the Court return exclusively to *Olmstead*'s trespass model, requiring a physical trespass before the Fourth Amendment is triggered.[249] This position likely also favors security over privacy, for the reasons detailed below regarding Justice Gorsuch's similar solution. It also has the disadvantage of being inconsistent with prior precedent: although *Olmstead* was given new life in *Jones*, the Court made it clear that the Fourth Amendment was

244 *Id.* at 2230.
245 *Id.* at 2261 (Alito, J., dissenting).
246 *Id.* at 2250–51.
247 *Id.* at 2252.
248 *Id.* at 2243–46 (2018) (Thomas, J., dissenting).
249 *See id.* at 2236–37, 2240.

governed by trespass *and* the reasonable expectation of privacy, not one or the other.[250]

In contrast to the other dissenting opinions, Justice Gorsuch's dissent is far more concerned with the dangers to privacy posed by the third-party doctrine in the modern age. As he writes, "Can the government demand a copy of all your e-mails from Google or Microsoft without implicating your Fourth Amendment rights? Can it secure your DNA from 23andMe without a warrant or probable cause? *Smith* and *Miller* say yes it can . . . ."[251] Acknowledging the risks that a categorical third-party doctrine pose in the modern age, Justice Gorsuch writes that if the third-party doctrine is "supposed to represent a normative assessment of when a person should expect privacy, the notion that the answer might be 'never' seems a pretty unattractive societal prescription."[252] Yet Justice Gorsuch rejects a balancing test like the one proposed by the majority, arguing that it offers little guidance to lower courts beyond "judicial intuition[]."[253] Despite being far more explicitly concerned about the important privacy problems raised in this Article than Justice Thomas,[254] Justice Gorsuch comes to largely the same conclusion: his solution is to scrap the third-party doctrine and *Katz*'s reasonable expectation of privacy test entirely, returning to a property-based approach that would rest Fourth Amendment protection on a party's ownership rights over a particular item or information.[255]

By emphasizing property rights, Justice Gorsuch's solution ostensibly promotes privacy over security. Yet, by eliminating the third-party doctrine and *Katz*'s reasonable expectation of privacy test, his solution would rely heavily on Congress and the states to create particular and actionable property interests in digital information.[256] Given the slow, deliberative nature of state and federal legislative bodies, it is questionable whether they can adequately respond to rapidly changing technological trends and shared data. Further, it is unclear how courts should respond when Congress articulates a limited property right, for example, when Congress requires only a

250 United States v. Jones, 565 U.S. 400, 409 (2012).

251 *Carpenter*, 138 S. Ct. at 2262 (Gorsuch, J., dissenting).

252 *Id.* at 2263 (citing William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1872 (2016)).

253 *Id.* at 2264.

254 Yet, unlike Justice Thomas's more limited view of property, Justice Gorsuch would allow property to be defined by anything—tangible or intangible—in which the state or federal legislature has conferred a property right. *Id.* at 2268–72.

255 *Id.* at 2268 (arguing that one solution to determining Fourth Amendment violations is to look to positive legal rights to determine whether a property interest exists—and was violated—in the searched or seized item).

256 *Id.*

subpoena or written request to access data. Does this trigger an overriding warrant requirement under the Fourth Amendment, or can Congress both dictate what is property and the constitutional response? As such, despite his sensitivity to the dangers to privacy raised in the digital age, without state intervention, Justice Gorsuch's solution, too, ultimately errs in favor of security over privacy.

The *Carpenter* majority opinion had its categorical cake and ate its balancing test, too. By affirming *Miller* and *Smith* while simultaneously limiting them based on the uniqueness of CSLI, the Court transformed the clunky categorical approach to the third-party doctrine into a new pseudocategorical approach that becomes a balancing test at some unspecified level of informational detail.[257] This raises more questions than it answers. The Court says seven days of CSLI are too much, but what about three?[258] What if the issue is not CSLI but rather information gathered from a maps app that records your movements to suggest better routes? The third-party doctrine applies until the situation becomes unique, so people wondering if this means their Alexa is an undercover agent must wait until the Court addresses Alexas. The dissenting opinions in *Carpenter* all end up worsening the problem, expanding state power and restricting privacy rights to varying degrees. Seemingly, then, waiting for a solution to the third-party problem to come from the Supreme Court may be in vain. As such, we now consider potential solutions proposed by others.

B. The Goldilocks Zone of Privacy: Academic Solutions

Many academics criticize the third-party doctrine, but their solutions are as varied, and arguably just as muddled, as the Court's. The various viewpoints can be catalogued into three dominant proposals of how to restore the balance between privacy and security: first, that the third-party doctrine, while flawed, should be left as-is; second, that the third-party doctrine should be eliminated; and third, that the *Katz*ian third-party standard should be replaced by a variety of tests, from multipart, bright line rules[259] to a reasonable suspicion standard similar to that articulated in *Terry v. Ohio*.[260] Each approach has drawbacks: the first, like the dissents in *Carpenter*, fails to properly recognize the downside of prioritizing privacy over security; the second

257 *Id.* at 2219 (majority opinion).

258 *Id.* at 2234 (Kennedy, J., dissenting).

259 H. Brian Holland, *A Third-Party Doctrine for Digital Metadata*, 41 CARDOZO L. REV. 1549, 1588–99 (2020); Note, *If These Walls Could Talk: The Smart Home and the Fourth Amendment Limits of the Third Party Doctrine*, 130 HARV. L. REV. 1924, 1942–45 (2017).

260 Terry v. Ohio, 392 U.S. 1, 39 (1968) (establishing reasonable suspicion, a lower threshold than probable cause, for a short, temporary detainment by police).

goes too far in the other direction, failing to ensure the state can engage in investigations of activities, even those occurring in public; and the third has pragmatic problems in operation.

A paradigmatic example of the first proposed solution—that the third-party doctrine should remain largely unchanged—is provided by Professor Orin Kerr.[261] Kerr argues that the third-party doctrine both provides ex ante clarity for government investigators and reviewing courts and ensures that criminals cannot take advantage of changing technologies to hide their activities—what Kerr calls "substitution effect[s]."[262] He suggests that the Court's third-party doctrine jurisprudence can be better understood as a subset of the consent doctrine, as it is built around the notion that "[t]hird-party disclosure eliminates privacy because the target voluntarily consents to the disclosure."[263] This argument is problematic for four important reasons.

First, Kerr's defense shifts the balance of the Fourth Amendment dramatically towards security and away from privacy by essentially preferring that one guilty person be caught than a hundred innocent people have privacy in their digital information.[264] Kerr argues that the third-party doctrine's categorical rule is beneficial because it keeps criminals from substituting public, easily investigable acts with private acts hidden with technology.[265] While it is true that criminals might use technology to hide their illegal activities, those same technologies are often used by many more people not engaged in criminal activity.[266] If a criminal uses Google to send an email to a co-conspirator rather than talk in an alley, does that mean the police should have warrantless access to all Gmail accounts? The risk of negative externalities—mainly deterring innocent conduct for fear of government investigation—makes this defense of the third-party doctrine as constructed particularly troublesome.

Second, it is unclear how significant this substitution risk really is. Some crimes, such as white-collar fraud or child-rape pornography,

261 Kerr, *supra* note 31, at 564.

262 *Id.* at 564–65.

263 *Id.* at 588 ("So long as a person knows that they are disclosing information to a third party, their choice to do so is voluntary and the consent valid.").

264 This is a reversal of the famous maxim that "it is better that a few criminals escape than that the privacies of life of all the people be exposed to the agents of the government." *See* Olmstead v. United States, 277 U.S. 438, 479 n.12 (1928) (Brandeis, J., dissenting).

265 Kerr, *supra* note 31, at 575–77.

266 Erin Murphy, *The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239, 1241 (2009) ("[B]ecause the technologies left exposed by third-party doctrine are not exclusively deployed for illicit purposes, failing to protect them generates negative externalities (by dissuading innocent, desirable conduct) . . . ."); Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39, 45 (2011).

often use technology as an indispensable element of the crime, but others, like murder, drunk driving, disorderly conduct, and larceny, might be able to be planned online, but there is no way to substitute the public criminal act for a private act cloaked in technology.[267] In reality, the third-party doctrine does not provide a bulwark against savvy criminals, but rather puts an enormous amount of private information at risk in order to better investigate a particular *subset* of private criminal activity.[268] The Fourth Amendment does not vary its protection based on the public or private nature of the criminal investigation—this is clear in the text of the Amendment, and in *Katz*'s famous holding that protection follows people, not places.[269] As such, rationalizing the third-party doctrine on substitution grounds puts significant amounts of private information at risk in the hopes that marginal security gains may be met.

Third, providing ex ante clarity to investigators is not a sufficient reason to allow for an overbroad third-party doctrine. Just as applying the death penalty to prevent parking violations would be effective, abolishing all privacy rights would provide such ex ante clarity, but both cases would constitute over-deterrence, making the cost to society too high.[270] The value of ex ante clarity must be weighed against the need for privacy, and the need for certainty for police officers cannot be used as a cudgel to beat back privacy rights or mask the cost of such investigative techniques. Furthermore, such clarity does not depend on the current formulation of the categorical third-party rule: as we show below, it can also be found by giving structure to the *Katz* test of whether the information was knowingly shared with the public, relieving investigators of the need to grapple with the difficulties of determining the "information history" of something shared with a third party.

Fourth, placing the third-party doctrine within the doctrine of consent is problematic. Kerr—and frequently the Court—assume consent from the mere act of sharing information with another.[271] Yet knowledge of a risk is not the same as assuming the risk. If it was, the government could simply give notice of any Orwellian investigatory technique, and by remaining in the country, we would be deemed to

267 Murphy, *supra* note 266, at 1243.

268 *Id.* at 1243–44.

269 Katz v. United States, 389 U.S. 347, 353 (1967).

270 On the social costs of over-deterrence, see A. Mitchell Polinsky & Steven Shavell, *The Theory of Public Enforcement of Law*, *in* 1 HANDBOOK OF LAW AND ECONOMICS 403, 410 (A. Mitchell Polinsky & Steven Shavell eds., 2007) ("[T]he strict sanctioning rule does not achieve the first-best outcome because it leads to the imposition of costly sanctions.").

271 United States v. Miller, 425 U.S. 435, 442–43 (1976); Smith v. Maryland, 442 U.S. 735, 742 (1979).

have consented to that risk. This is obviously at odds with the Fourth Amendment itself and would put the authority of determining the bounds of the Fourth Amendment in the hands of the very party the Amendment seeks to confine.[272]

The second proposed solution—that the third-party doctrine needs to be radically transformed—has been made by many scholars, explicitly or implicitly,[273] who typically argue that the third-party doctrine is too dangerous and should be eliminated.[274] To these scholars, the doctrine is incompatible with the digital age: a third-party doctrine that might have worked when calls were made in phone booths simply cannot work when calls are made from a device that coordinates hundreds of third parties to act as GPS trackers, bank tellers, call operators, cameras, personal computers, home security monitors, and so much more.[275] This fear is legitimate and widely acknowledged—while the Court has not offered workable solutions, it has acknowledged the risks to allowing warrantless government access to everything that third-party technology has to offer.[276]

Arguing for the elimination of the third-party rule is understandable given the risks imposed by a categorical sharing rule.

---

272 As the Court recognized in *Smith*'s famous footnote: "[W]here an individual's subjective expectations had been 'conditioned' by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was." *Smith*, 442 U.S. at 741 n.5.

273 For instance, Professor Sherry Colb has argued that consent should be viewed as requiring voluntary, explicit consent, in which case the third-party doctrine is effectively eliminated. Colb, *supra* note 101, at 123 ("First, it would represent an open acknowledgement that 'knowing exposure' only occurs when there has been some explicit or tacit consent to public observation, and not simply the *taking of a risk* or the *limited exposure* of what is then further disseminated.").

274 *See, e.g.*, Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975, 1024–26 (2007); Daniel Solove, *10 Reasons Why the Third Party Doctrine Should be Overruled in Carpenter v. US*, TEACHPRIVACY (Nov. 28, 2017), https://teachprivacy.com/carpenter-v-us-10-reasons-fourth-amendment-third-party-doctrine-overruled/ [https://perma.cc/UC4K-UHPS]; Andrew J. DeFilippis, Note, *Securing Informationships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence*, 115 YALE L.J. 1086, 1089 (2006).

275 Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 753 (2005) ("The third party doctrine presents one of the most serious threats to privacy in the digital age.").

276 *See Smith*, 442 U.S. at 746 (Stewart, J., dissenting) (arguing that "the broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards"); *see also* Carpenter v. United States, 138 S. Ct. 2206, 2262 (2018) (Gorsuch, J., dissenting) ("Even our most private documents—those that, in other eras, we would have locked safely in a desk drawer or destroyed—now reside on third party servers. *Smith* and *Miller* teach that the police can review all of this material, on the theory that no one reasonably expects any of it will be kept private. But no one believes that, if they ever did.").

However, such drastic reform would significantly hamper certain valuable investigations, especially those, like that of white-collar crimes, in which it is particularly hard to generate individualized suspicion without personal information held by third parties.[277] White-collar crime has a massive effect on the financial well-being of millions of Americans—it is estimated to account for between $300 and $600 billion annually.[278] Yet white-collar crime largely involves tools and mechanisms legally used by millions of people.[279] What makes white-collar crime unlawful is that illegal acts often intermingle with legal acts, differentiated only by their "purpose and intent."[280] This makes investigating white-collar crime particularly difficult, as white-collar crimes are difficult to report for a number of reasons.[281] These crimes are often very technical and, because of their complexity and use of legal tools and techniques, victims often do not even know that they were victimized.[282] Investigators must gather significant amounts of information—often personal financial information—to search for patterns that suggest illegality.[283] Both the Court and Congress have recognized these challenges in ruling bank records accessible without a warrant.[284]

Although Kerr's fear of a substitution effect is overdrawn, it is true that there exist countless ways for criminals to use third parties to facilitate or obfuscate their actions. In the 2014 Playpen cases, hundreds of people were convicted of downloading child-rape pornography using Tor browsers to disguise their IP addresses.[285] In a

277 John S. Applegate, *The Business Papers Rule: Personal Privacy and White Collar Crime*, 16 AKRON L. REV. 189, 194 (1982).

278 Bruce Kennedy, *Why White Collar Criminals Often Get Away*, CBS NEWS (May 11, 2015), https://www.cbsnews.com/news/getting-away-with-white-collar-crime/ [https://perma.cc/8T4T-4RNQ].

279 Applegate, *supra* note 277, at 192.

280 *Id.*

281 *Id.* at 194.

282 *Id.*

283 *Id.* at 195.

284 United States v. Miller, 425 U.S. 435, 442–43 (1976) ("The lack of any legitimate expectation of privacy concerning the information kept in bank records was assumed by Congress in enacting the Bank Secrecy Act . . . because they 'have a high degree of usefulness in criminal, tax, and regulatory investigations and proceedings.'" (quoting 12 U.S.C. § 1829b(a)(1) (1976)); Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3697 (1978) (codified at 12 U.S.C. §§ 3401–22 (1982)). Bank records kept pursuant to the Bank Secrecy Act may only be obtained by customer consent, subpoena, search warrant, or "formal written request," barring a narrowly defined emergency or exigent circumstance. 92 Stat. at 3698.

285 *The Playpen Cases: Frequently Asked Questions*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/playpen-cases-frequently-asked-questions#whathappened [https://perma.cc/H78B-R3G5].

massive national and international raid, the government installed malware that searched the suspects' computers for their actual IP addresses, which were later used to gather evidence of an extensive child-rape pornography ring.[286] Services like Tor browsing have made committing criminal acts online, like sharing child-rape pornography, much more difficult to investigate. Simply eliminating the third-party doctrine would swing too far away from security, hamstringing investigations of crimes that can be hidden by legal third-party tools yet are extremely damaging to society. Privacy is not the only value that must be weighed in Fourth Amendment analysis.

The final major approach that scholars have put forward proposes various compromise positions, incorporating everything from multipart bright line tests[287] to a *Terry*-style reasonable suspicion standard as a middle ground between eliminating the third-party doctrine and embracing a categorical third-party rule.[288] These solutions seek to bridge the gap between a categorical rule and an ad hoc application in a way that police and courts are familiar with: determining whether there was reasonable suspicion for the search, and whether the search was carried out in reasonable scope.[289]

We focus on the reasonable suspicion solution, as it attempts to provide a fully ad hoc judicial solution to the third-party quandary outside of the traditional *Katz*ian framework. There are three problems with this solution. First, reasonable suspicion is a notoriously lenient standard for police to meet, as many critics have noted: "[C]ourts have interpreted the 'totality of the circumstances' broadly, thus expanding the scope of what constitutes an acceptable *Terry* stop."[290] Even some courts agree with this characterization: "[The doctrine has] expanded beyond [its] original contours, in order to permit reasonable police action when probable cause is arguably lacking."[291] Replacing a categorical rule with any sort of limiting doctrine would seemingly restrict the power of government agents, but this restriction is likely to turn out to be illusory. As technology becomes more and more integrated into people's daily lives, and thus more central to an increasing number of criminal investigations, a

286 *Id.* The warrant was ultimately invalidated as exceeding jurisdictional scope, but the evidence was not suppressed as a reasonable officer would have thought the warrant was valid. United States v. Taylor, 935 F.3d 1279, 1282 (11th Cir. 2019), *cert. denied.*

287 *See, e.g.*, Holland, *supra* note 259, at 1588–99.

288 Lucas Issacharoff & Kyle Wirshba, *Restoring Reason to the Third Party Doctrine*, 100 MINN. L. REV. 985, 987 (2016).

289 *Id.* at 1036.

290 Rachel Karen Laser, *Unreasonable Suspicion: Relying on Refusals to Support* Terry *Stops*, 62 U. CHI. L. REV. 1161, 1169 (1995).

291 United States v. Chaidez, 919 F.2d 1193, 1198 (7th Cir. 1990).

reasonable suspicion standard will not provide the bulwark against abuse that is necessary in the modern age.

Second, that lenient standard was justified because *Terry* stops and frisks are highly constrained.[292] *Terry* stops require only reasonable articulable suspicion because they are less intrusive than searches, and because typically a swift response is required to a suspicion raised by on-the-spot observation, which is thus unforeseeable.[293] Accordingly, reasonableness is only met if the stop or frisk is carefully proscribed in both time and content.[294] In contrast, the third-party doctrine has been applied to detailed, comprehensive analysis of bank records, emails, etc.—clearly not meeting the limited intrusion requirement of *Terry*. Furthermore, the third-party doctrine is not normally tied to the need for swift action: *Carpenter* is the only case to have suggested that there is any time constraint applicable, and that was only in relation to a very specific exception—historical CSLI data spanning more than seven days' duration—not in any way linked to the need for immediacy of action.

Third, how *Terry*-style analysis would apply beyond the constrained nature of stops and frisks is highly uncertain. Supporters of this view argue that this would provide ex ante clarity for police officers and government agents, all of whom know how to apply reasonable suspicion analyses. However, applying this approach beyond stop-and-frisk to full searches would likely turn the third-party doctrine into a reasonableness Rorschach blot.[295] What simple, easily applied standard would apply to bank records, phone GPS data, Alexa recordings, Fitbit health information, and so on? Any reasonable suspicion standard that worked to bridge that contextual divide would end up being so vague as to be nearly useless. Furthermore, it would need to answer not only what can be searched, but how extensively, which opens up a fresh batch of distinctions that *Terry* has never had to answer. For example, evaluating what is a reasonable scope for a search of a person's phone[296] and a person's CSLI data[297] is dramatically different. What ex ante clarity is there when officers must compare a Facebook private message to a Nest thermostat? A simple

292 Terry v. Ohio, 392 U.S. 1, 30 (1968).

293 *Id.* at 20.

294 *Id.* at 29 ("The sole justification of the search in the present situation is the protection of the police officer and others nearby, and it must therefore be confined in scope to an intrusion reasonably designed to discover guns, knives, clubs, or other hidden instruments for the assault of the police officer.").

295 Amsterdam, *supra* note 224, at 393.

296 Riley v. California, 573 U.S. 373, 378 (2014).

297 Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).

reasonableness inquiry leaves far too much room for judicial interpretation and far too little clarity for acting agents.

While many scholars have come to agree that the third-party doctrine is highly problematic, there is no consensus on how to resolve the difficulty of balancing security and privacy in the third-party doctrine. Each of the broad categories of solutions discussed here raise as many problems as they solve. In the next Section, we provide an alternative that sidesteps the problems of both extremes, discussed here, and avoids creating a chasm of ambiguity and discretion, which the more moderate solutions typically create.

C. The Solution: Reinvigorating Katz*'s Two-Part Test*

The third-party doctrine was established during the age of land-line telephones and pocket radio transmitters. A categorical rule based around sharing information was more palatable when the most a person would likely share were numbers dialed[298] or deposit slips.[299] But in our information-sharing age, we cannot permit such a dramatically over-inclusive rule that risks exposing highly sensitive information to government surveillance. And doing so is not even required by the logic of the underlying doctrine: the cases that established the categorical third-party doctrine did so by ignoring the language and facts of *Katz*.

Our solution retains much of the ex ante clarity of a categorical rule while providing enough analytical flexibility to avoid overbreadth, all while being rooted in both the language and spirit of *Katz*. According to *Katz*, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[300] Thus, information (1) knowingly exposed (2) to the public ought to be excluded from Fourth Amendment protection. The existing third-party doctrine glosses over both these elements. Rather than simply excluding from Fourth Amendment protection everything that has been shared, or asking courts and police to make complicated, ad hoc reasonableness inquiries, we can rigorously operationalize this two-part test by focusing on the nature of the recipient and the knowledge of the sharer.

298 Smith v. Maryland, 442 U.S. 735, 742 (1979).

299 United States v. Miller, 425 U.S. 435, 442 (1976).

300 Katz v. United States, 389 U.S. 347, 351 (1967) (first citing Lewis v. United States, 385 U.S. 206, 210 (1966); and then citing United States v. Lee, 274 U.S. 559, 563 (1927)).

1. Knowingly Exposes

Miller and *Smith* base their rule on the simplistic formalism that if a person shares information, that information is compellable by the government precisely and only because it was shared. But that is inconsistent with the facts of *Katz*. In *Katz*, the very case that birthed the third-party doctrine, Mr. Katz was on the phone with another person, actively sharing information, yet that communication retained its Fourth Amendment protection.[301] A standard higher than simple sharing is implied by the facts alone.

The difference between "knowingly exposes" as used in *Katz* versus *Miller* and *Smith* is that in *Katz*, this "knowingly" element had bite, not just window dressing. It is clear from the text of *Katz* that "knowingly" was meant to have substantive meaning:

> The Government stresses the fact that the telephone booth from which the petitioner made his calls was constructed partly of glass, so that he was as visible after he entered it as he would have been if he had remained outside. But what he sought to exclude when he entered the booth was not the intruding eye—it was the uninvited ear. He did not shed his right to do so simply because he made his calls from a place where he might be seen. No less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment. One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.[302]

The *Katz* Court is essentially saying that even though Katz *knew* that it was possible to be seen in a glass phone booth, a reasonable person would not expect that to translate into him having made his externally inaudible speech public. In the same way, when a person sends an email, they may know that they are using a platform such as Gmail, but the reasonable person would not expect that to translate into having no privacy in the correspondence, because they have not knowingly made the content public, even though they have knowingly transmitted through a third party. The exposure must be knowing, not presumed simply from having used a potentially unavoidable conduit, be it a landline telephone or an email provider.

The Court in *Katz* is thus using "knowingly expose[]" to capture the concept of making an *informed choice* to convey information to a third party. If Mr. Katz knowing that a person could be standing close

301 *Id.* at 359.

302 *Id.* at 352 (footnotes omitted) (first citing Silverthorne Lumber Co. v. United States, 251 U.S. 385 (1920); then citing Jones v. United States, 362 U.S. 257 (1960); and then citing Rios v. United States, 364 U.S. 253 (1960)).

to the phone booth and overhear his conversation is not enough to annihilate his expectation of privacy, then the Court clearly required something more than simple knowledge of the *possibility* of exposure occurring to undermine the expectation of privacy. In the same way, simple awareness that an ISP is involved in the email transmission process similarly cannot obliterate an expectation of privacy in one's email. The *Katz* Court stressed the significance of Mr. Katz shutting the door and paying the toll because in doing so Mr. Katz was evincing his choice *not* to convey the information to any person other than his conversation partner.

Interestingly, it is not only *Katz* that makes this implication clear. In *Smith*, the Court explicitly stated that pure knowledge cannot be enough:

> Situations can be imagined, of course, in which *Katz*' two-pronged inquiry would provide an inadequate index of Fourth Amendment protection. For example, if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation of privacy regarding their homes, papers, and effects. . . . where individual's subjective expectations had been "conditioned" by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was.[303]

Thus, even the *Smith* Court is acknowledging that simple knowledge can be inadequate.

But importantly, the *Katz* Court did not merely refer to "knowingly" on its own, it referred to "knowingly expos[ing]."[304] Exposure is an act—an active verb. The Court since *Katz* has used the term in a very passive way, in terms of knowledge of the possibility of exposure occurring. The *Katz* Court, in contrast, required a positive action by the person potentially losing their expectation of privacy—that is, a voluntary act on their part.

For this reason, the Court's choice to eventually turn to voluntariness language made sense: choice necessitates positive action, not simply a state of knowledge. However, where *Smith* and *Miller* went wrong is, first, in refusing to see that choice implies there must be an alternative option, and second, in jettisoning the knowledge requirement in favor of voluntariness—as we have seen, voluntariness of exposure is inadequate also. By contrast, the way that *Katz* conceives

303 *Smith*, 442 U.S. at 740 n.5.

304 *Katz*, 389 U.S. at 351 (first citing Lewis v. United States, 385 U.S. 206, 210 (1966); and then citing United States v. Lee, 274 U.S. 559, 563 (1927)).

of knowingly exposing incorporates both knowledge and voluntariness. The *Katz* Court used "knowing[] expos[ure]" to mean that a person must know that their actions are making their information no longer private and have an actual choice to avoid such exposure, yet make the decision to so act anyway. In *Smith* and *Miller*, even if the defendants knew the phone company and the bank kept their records, they had no choice but to use the phone or bank. *Katz* requires both knowledge and voluntariness in the face of that knowledge. It is this way in which "knowingly expose[]" can be given back its bite. And that can occur using terms that are familiar to courts—both knowledge and voluntariness are well-known concepts.

Reinvigorated in this way, a *Katz*ian "knowingly expose[d]" component appropriately protects citizens against illicit government surveillance and intrusion, given the ubiquitous sharing that occurs daily. Importantly, it would address situations where the sharing occurs unbeknownst to a reasonable consumer. Snapchat sells itself as an app that allows users to send pictures and messages to other users and have those messages delete themselves shortly after being shared.[305] Yet users' snaps are not literally deleted—instead, they are stored on the recipient's device in an unmapped but accessible form.[306] To the surprise of millions of Snapchat users, it was subsequently revealed that snaps are also kept in a central database accessible by two high-level Snapchat employees.[307] Under *Smith*, a court would not be out of line to assume that users knew Snapchat had to store snaps for business purposes. Under a reinvigorated *Katz*ian knowingly exposed prong, however, given the publicly portrayed nature of Snapchat, an applying court would easily conclude that Snapchat's likely users would not have read such fine print and would have relied instead on Snapchat's advertised purpose of providing a private forum, and thus any public exposure was not knowing.

This analysis also provides a better means of deciding *Carpenter*, as there was likely nothing that would have indicated to Carpenter or a reasonable cell phone owner that their CSLI was going to be recorded and stored indefinitely by their cell phone provider. As such, there is

305 Snapchat Support, *When Does Snapchat Delete Snaps and Chats?*, SNAPCHAT, https://support.snapchat.com/en-US/article/when-are-snaps-chats-deleted [https://perma.cc/A9RF-CLNX] ("Delete is our default.").

306 Alyson Shontell, *Actually, Snapchat Doesn't Delete Your Private Pictures and Someone Found a Way to Resurface Them*, BUS. INSIDER (May 9, 2013), https://www.businessinsider.com/snapchat-doesnt-delete-your-private-pictures-2013-5 [https://perma.cc/WLG7-FA88].

307 William Stanton, *Can Snapchat Employees See Your Snaps?*, ALPHR (Apr. 28, 2019), https://www.alphr.com/snapchat-employees-see-your-snaps/ [https://perma.cc/JY58-XN8V].

no need for the Court to craft an exception for cell phone location information, with all of the caveats and qualifications that involved, and all of the unknown implications for future applications that decision created. Instead, under our approach—which is really the *Katz* Court's approach—courts can look at contracts and terms of service for guidance on what reasonable users expect.

Giving meaning to the "knowingly expose[d]" component in this way, by equating it with an informed choice, solves the problem of inferring knowledge from an act that is in essence forced upon a person. In *Miller*, even as the Court stressed voluntariness over knowledge, voluntary action was assumed despite the fact that most people need bank accounts to have jobs, homes, utilities, and other life necessities.[308] The majority in *Miller* determined that "[a]ll of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[309] Yet the Court did not address the dissent's argument that owning and operating a bank account cannot be considered voluntary if it is required to function in society. If that was the case, advancing technology could force whole swaths of information out of the Fourth Amendment's orbit with no inquiry into whether or not an individual can *ever* show an attempt to protect their reasonable expectation of privacy.

The Court hinted at this kind of analysis in *Riley*, arguing that cell phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[310] However, that case concerned a search incident to arrest; when the same issue arose as applied to the third-party doctrine, in *Carpenter*, the Court faced the exact same question regarding the voluntariness of owning a cell phone, as well as the related question of whether a reasonable cell phone owner understood that CSLI was gathered and stored in the first place. Instead, the Court focused on the amount of information that could be gleaned from CSLI.[311] This was a missed opportunity to give guidance on how "knowingly exposes" meaningfully applies in third-party doctrine analysis.

Despite the importance of the knowledge component in *Katz*, the Court frequently assumes knowledge with little analysis. In *Smith*, the Court's analysis of this component is filled with assumptions and logical leaps. For example, "[a]ll telephone users realize that they

308 Ciarabellini, *supra* note 226, at 138.

309 United States v. Miller, 425 U.S. 435, 442 (1976).

310 Riley v. California, 573 U.S. 373, 385 (2014).

311 *Id.* at 395–96.

must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed."[312] Yet the opinion later acknowledges that, even by 1979, this was done automatically, without human input.[313] Based on a half-page of these assumptions, the majority then assumes that this translates to knowledge: "it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret."[314] Knowledge was explored even less rigorously in *Miller*; the majority simply stated that Miller's financial statements and "deposit slips . . . are not confidential communications but negotiable instruments to be used in commercial transactions . . . exposed to their employees in the ordinary course of business," without addressing whether Miller or a reasonable banking services consumer would understand that the act of depositing a check would render it no longer a private paper.[315] Even after *Miller*, surveyed subjects considered that the government "perusing bank records" without a warrant would rank at 71.60 on a 0–100 rating of intrusiveness,[316] suggesting the unsoundness of the Court simply surmising knowledge and expectations, rather than looking to contractual terms and other like indicia of actual consumer understandings.

Some scholars attempt to address this concern by arguing that the Court should not equate knowing exposure with creating a risk of exposure.[317] As Professor Sherry Colb queries, if you whisper something in someone's ear and a passerby leans in to hear, have you really "exposed" that information, or has the passerby exposed it for you by breaking social norms?[318] But the problem with relying on a distinction between knowing exposure and risk of exposure is that this approach runs afoul of the plain view comparison cited in support for the knowing exposure doctrine in *Katz*.[319] One can knowingly expose

312 Smith v. Maryland, 442 U.S. 735, 742 (1979).

313 *Id.* at 744.

314 *Id.* at 743.

315 *Miller*, 425 U.S. at 442.

316 Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society,"* 42 DUKE L.J. 727, 738 (1993).

317 Colb, *supra* note 101, at 122.

318 *Id.* at 126.

319 *See* Katz v. United States, 389 U.S. 347, 351 (1976) (first citing Lewis v. United States, 385 U.S. 206, 210 (1966); and then citing United States v. Lee, 274 U.S. 559, 563 (1927)) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."); Lewis v. United States, 385 U.S. 206, 210 (1966); United States v. Lee, 274 U.S. 559, 563 (1927) (finding enough probable cause for a search, given the meeting in question took place in plain view).

without taking any affirmative action. For instance, if a person leaves a confession to a murder taped to their refrigerator, and the only way to see it is to walk up to their fence, stand on tiptoes, and crane one's neck, that is a clear violation of social norms. But can it really be argued that the confession was not knowingly exposed? To use the whisper analogy: What if you whisper your confession to a friend and someone does not have to lean in to hear you? Can this doctrine really rest on an evaluation of how far a passerby leaned in? *Katz* makes no such distinction: in fact, one of the central pillars of *Katz* was to reject such arbitrary distinctions, such as that between something being attached to a wall versus inserted into a wall.[320] Nor is such a distinction implied in the words "knowing[] expos[ure]."

Given the plain view roots of the test, a knowing risk of exposure should be sufficient to trigger the third-party doctrine, without complicating the matter by assessing how great the risk is. By instead keeping the test as knowing exposure as an informed choice, and not allowing it to be reduced to voluntariness—or even something less than voluntariness—the reach of the third-party doctrine is constrained in a way to avoid the problems articulated in Part II. Under our test, the *Smith* Court could not assume the defendant understood the inner workings of the phone company's billing practices, and the *Miller* Court could not force a person into a state of voluntariness. At the same time, it allows police and reviewing courts a simpler analysis, similar to the plain view doctrine. A court need only ask: Did the information sharer (or would a reasonable person in that position) know the risk that their information could be exposed? Not only are courts familiar with the knowing standard, they would merely need to examine publicly-accessible consumer terms of service and a general understanding of a particular technology's place in society to utilize that familiar test.

Returning to making the "knowingly expose[]" element substantive is the first key to fixing the third-party doctrine. If the state shows that the defendant knowingly exposed the information, the analysis then turns to step two.

2. To the Public

Katz knowingly exposed his conversation to the person on the other end of the line, yet he retained his expectation of privacy. Simply sharing information cannot be enough to trigger the third-party doctrine, otherwise all conversations would be unprotected. An analysis of the recipient—exactly who is "the public"—is the second

320 *Katz*, 389 U.S. at 352–53.

vital part of the inquiry. In *Katz*, the individual on the other end of the line was not "the public." The plain view doctrine analysis carries through to this step as well, by asking: Can the information be accessed by the government without compulsion or investigatory legerdemain? If so, it is essentially in plain view, and "the public" has been exposed. For instance, information shared to social media is shared with the public: even with privacy settings activated, an individual posting to a social media account is not simply having a private conversation but is making the information potentially available to multiple parties. This is not simply a question of numbers: a conversation between three people can be protected. But by knowingly exposing a post to a forum where the government or others can access it, even if nobody does, the poster has effectively exposed it to the public.

One of the reasons why courts have applied a simpler, more reductive third-party analysis is that the third-party doctrine has been inappropriately combined with the false-friend doctrine. As discussed in Part I, these doctrines are separate, and they inform each other. Without knowing exposure *to the public*, a person retains a reasonable expectation of privacy in information shared with a third party until or unless that third party shares that information, at which point they have proven themselves to be false. This is an important distinction, because to conflate the two doctrines into the simple sharing rule espoused in *Miller* and *Smith* assumes all friends are false and makes "the public" into any third party. But, if you share information with a true friend, as Katz did, the third-party doctrine should not be triggered.

But what about information shared with a non-person? Increasingly, information is shared with third-party entities in such a way that no human ever interacts with the data. According to *Smith*, that still triggers the third-party doctrine—the telephone operator no longer needed to be a person for Mr. Smith to have shared the numbers he dialed with the phone company.[321] But how can sharing numbers with an automated telephone operating system equate to knowing exposure to the public? Looking to expressive use theory in copyright law sheds light on this problem.[322] Under expressive use theory, inert use—like a web browser copying the information on a website for cache purposes—does not trigger a copyright violation as would an expressive use, such as copying a book in order to read it.[323]

321 Smith v. Maryland, 442 U.S. 735, 744–45 (1979).

322 Matthew Sag, *Copyright and Copy-Reliant Technology*, 103 NW. U. L. REV. 1607, 1607–10 (2009) (distinguishing between protected expressive use and unprotected non-expressive use in copyright law).

323 *Id.* at 1624–25; *see also* Matthew Sag, *Orphan Works as Grist for the Data Mill*, 27 BERKELEY TECH. L.J. 1503 (2012) (exploring other applications of the concept).

This distinction can also inform the third-party doctrine: if there is no expressive interaction by a third party or entity, it is hard to argue that information has been knowingly exposed to the public.

We can apply this concept to familiar digital applications: if you ask Alexa a question, and the device gives you an answer, your interaction with that inert device cannot constitute exposure to "the public." But change the facts slightly and it could constitute such exposure: it has been widely reported that Alexa records your voice for a short period of time after the "wake word" is spoken.[324] If those recordings are themselves transitory and inaccessible, then Alexa users are still not talking to the public. But if Alexa records and stores all such conversations, which are then accessible to the behemoth that is Amazon, then you are not simply having a conversation with a machine but rather you are sharing your conversation with a massive corporation in storable form. But change the facts again: Amazon still has all of your recordings, but it represents to its users that these recordings are not stored in a form identifying an individual speaker but are simply amassed for anonymous training of Alexa; then, once again, speaking to your machine comes with an expectation that such speech will not be overheard by "the public" in any identifiable way. Change the facts again: in headline news, it is revealed that Amazon does actually keep identification information, and in fact sells this information to Facebook for advertising purposes—then once again, the reasonable person knows that their conversations are effectively potentially public. But without these additional facts, it is not possible to say that talking to a machine is enough to constitute exposure "to the public"—there has to be a ghost in that machine who can meaningfully blab, and the reasonable person needs to know about it. This is an important distinction, one that is easy to determine by investigators using the same tools that courts use to analyze whether a person has a reasonable expectation of privacy. Yet, it is misunderstood by the current third-party doctrine.

D. The Fate of Miller *and* Smith *and the Role of Contracts*

Much has been said about the failings of *Miller* and *Smith*.[325] Yet, currently, they remain good law, and a court formulating a new rule would need to decide whether or not those cases could survive, appropriately narrowed, or if they would need to be overturned. Under our solution, it is likely that both would be overturned.

---

324 Josh Hendrickson, *How Alexa Listens for Wake Words*, HOW-TO GEEK (July 15, 2019), https://www.howtogeek.com/427686/how-alexa-listens-for-wake-words/ [https://perma.cc/8QV3-ZCQN].

325 *See supra* Part I.

Miller fails on both prongs. A bank account is required to operate in our modern world,[326] and exposure cannot be knowing if it is shoehorned into an activity required by society. Further, it is hard to argue that handing a deposit slip to a teller to be filed in your account is exposure to the public, let alone now when the teller is no longer even involved and a person can access their own account directly online without dealing with any person. Mr. Miller's person-to-person interaction with the bank teller is far more analogous to Mr. Katz's protected conversation than information exposed to the plain view of the public.

Smith similarly fails both prongs. First, as the dissent notes, use of a phone is not something a person can avoid,[327] and while this may no longer be true for landlines, it is even more so today for cell phones, as the Court has recognized.[328] And, despite the roughshod analysis in the majority opinion around the knowledge element, it is a leap to suggest that phone owners are aware of all the ways in which phone companies store and use their call information. The Court in *Carpenter* made the same mistake, listing all the ways in which cell phone companies store and share CSLI without addressing whether a reasonable user would have ever known about CSLI in the first place, let alone what companies do with that data. *Smith* fails on the second prong as well, as Mr. Smith's dialed numbers were shared only with an automated operator service. They also were not exposed to the public any more than when a person writes an email to a friend—i.e., has a private digital conversation—and doing so using Gmail does not mean that they have shared the information with the public.

Revitalizing *Katz*'s "knowing[] expos[ure] to the public" test returns individual choice to the analysis. A key component to *Katz*'s analysis is that Katz himself took steps to keep out unwanted listeners. By "shut[ting] the door behind him, and pay[ing] the toll," Katz demonstrated his desire to maintain his reasonable expectation of privacy.[329] By eliminating the categorical sharing rule, our solution allows individuals, similarly, to contract around their privacy needs. As users and third parties understand that shared information is no longer unprotectable, people who care about privacy would be able to choose platforms that offer better security.[330] Others can opt out of

326 Ciarabellini, *supra* note 226, at 138.

327 Smith v. Maryland, 442 U.S. 735, 746 (1979) (Stewart, J., dissenting).

328 Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

329 Katz v. United States, 389 U.S. 347, 352 (1967).

330 It is also true that while many people lack the sophistication to change their email platforms, there are many different hosting companies, some of which differentiate themselves by emphasizing their encryption services and privacy protection mechanisms.

that greater protection for cheaper platforms that might sell their information and so make it public. All parties could knowingly choose.

This works in application: for example, Snapchat sold itself on the basis that its snaps self-destruct after being viewed—this created the kind of expectation of privacy that made the third-party doctrine inapplicable. However, once it is common knowledge that the snaps do not in fact disappear and are accessible, then users who are concerned with privacy may want to switch to another platform because that broad knowledge renders the snaps no longer protected. If Katz knew his conversations in the phone booth could be recorded and stored by the phone company to help improve call quality, yet he used the phone booth anyway, he would be hard-pressed to argue that he diligently protected his reasonable expectation of privacy. Likewise, if an Amazon rival created a home support device that did not record or store any information, but it also did not learn from users' speaking styles and habits, that would be a choice people could make.

There are dangers to expanding privacy protection because that protection extends to the criminally minded, who may make use of *Miller* being overturned to develop new schemes to conduct white-collar crime. But that is the nature of the security-privacy balance being recalibrated: the Fourth Amendment protects the guilty as well as the innocent from unreasonable searches and seizures. Also, we do not necessarily need the third-party doctrine to solve this problem. The fact that banks are heavily regulated would likely ensure that all banks would not immediately become hostile to white-collar investigators, and otherwise legislatures can provide further such regulations to ensure that banks do not become miniature Cayman Islands within the United States.

There are also potential negative consequences to changing the third-party doctrine in a way to permit contracts to vary expectations of privacy. Given the difficulty in detecting and investigating white-collar crime, being able to access banking records without a warrant can be particularly helpful.[331] Reorienting the third-party doctrine to the knowing exposure to the public test could result in less equitable financial institutions—if banks were no longer mandated to share information with government investigators, it is likely that wealthier people could pay for more security from banks that were willing to operate less openly with the government. But the alternative is that nobody has any privacy in their banking records.

See Stacy Fisher, *10 Best Free Email Accounts for 2021*, LIFEWIRE (Sept. 5, 2021) https://www.lifewire.com/best-free-email-accounts-1356641 [https://perma.cc/G3EN-P4RS].

331 *See* Applegate, *supra* note 277, at 194–98.

A system based on true knowing, voluntary exposure would allow people looking to deposit or invest money to have a clearer picture of their rights so they could decide whether to pay for more privacy or take the risk that their bank might be false. This is in line with *Katz*'s subjective expectation of privacy inquiry: courts want people to show that they have tried to keep their goods and information secure. That is, *Katz* encouraged individuals to try to maintain their privacy through their choice of actions. The knowing exposure to the public test provides more clarity for citizens, institutions, government agents, and reviewing courts.[332]

E. The Practicality of a Katz*ian Solution for the New Roberts Court*

The preceding analysis raises the question of whether a *Katz*ian solution to the third-party problem is likely to be adopted by the contemporary Roberts Court. The Court's new six-person conservative majority[333] may seem a pragmatic stumbling block to our proposal. However, this solid conservative majority does not translate to a solid originalist majority, and it is originalism that constitutes the only coherent viable alternative to our solution. The only other alternative is to build on the rather incoherent existing patchwork of ill-justified distinctions.[334] In this Section, we briefly describe why a structured return to *Katz* is more likely, albeit constituted by an ideologically motley collection of liberal justices and more moderate conservatives.

Katz was most vehemently criticized by Justice Scalia, who attempted to replace *Katz*ian reasonable expectation analysis with a return to trespass analysis for addressing whether a search or seizure has occurred.[335] He was unsuccessful in ousting *Katz* but, starting in *United States v. Jones*, Justice Scalia was able to reanimate the trespass doctrine as a co-equal partner of reasonable expectation analysis on this question.[336] However, note that his success in that case was itself

332 This clarity is important because, since it was introduced, the subjective prong has been acknowledged but never applied. As it stands, the subjective prong does no work. But, by giving substance to the objective prong, our test provides the individual protections envisioned by a subjective inquiry.

333 *See, e.g.*, Jason Windett, Jeffrey J. Harden, Morgan L.W. Hazelton & Matthew E.K. Hall, *Amy Coney Barrett Is Conservative. New Data Shows Us How Conservative*, WASH. POST (Oct. 22, 2020), https://www.washingtonpost.com/politics/2020/10/22/amy-coney-barrett-is-one-most-conservative-appeals-court-justices-40-years-our-new-study-finds/ [perma.cc/ZCA7-3FHT].

334 *See supra* Section III.A.

335 Kyllo v. United States, 533 U.S. 27, 34 (2001) ("While it may be difficult to refine *Katz* . . . there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*.").

336 United States v. Jones, 565 U.S. 400, 406 (2012) ("Fourth Amendment rights do not rise or fall with the *Katz* formulation. At bottom, we must 'assur[e] preservation of that

based on an unstable ideological coalition: Chief Justice Roberts and Justices Kennedy and Thomas joined the opinion, with the fifth vote being supplied by Justice Sotomayor, who wrote separately to emphasize that she had signed on to the originalist inquiry as an *additional* means of protection against overly-intrusive searches.[337]

Justice Scalia was replaced by the equally originalist-oriented Justice Gorsuch,[338] who has also indicated his preference for trespass over *Katz*ian analysis.[339] In addition, Justice Thomas[340] and Justice Barrett[341] are both strict originalists. But while some have tried to claim that Justice Kavanaugh is an originalist, there is little evidence for this.[342] At any rate, there are good reasons to believe that there can be a five-justice majority for a return to *Katz*ian analysis, with or without Justice Kavanaugh.

Chief Justice Roberts has never been an originalist: he generally favors a pragmatic conservatism that rejects formalism in favor of functionalism.[343] This is evidenced by his having authored both major

---

degree of privacy against government that existed when the Fourth Amendment was adopted.'" (quoting *Kyllo*, 533 U.S. at 34)).

337 *Id.* at 414 (Sotomayor, J., concurring) (stating that "the trespassory test applied in the majority's opinion reflects an irreducible constitutional minimum" but "even in the absence of a trespass, 'a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.'" (quoting *Kyllo*, 533 U.S. at 33)).

338 Neil M. Gorsuch, *Justice Neil Gorsuch: Why Originalism Is the Best Approach to the Constitution*, TIME (Sept. 6, 2019), https://time.com/5670400/justice-neil-gorsuch-why-originalism-is-the-best-approach-to-the-constitution/ [https://perma.cc/LXR9-6JMR].

339 Carpenter v. United States, 138 S. Ct. 2206, 2244 (2018) (Gorsuch, J., dissenting) ("That the *Katz* test departs so far from the text of the Fourth Amendment is reason enough to reject it.").

340 Justice Thomas is the most extreme originalist to have served on the Court, willing to overturn any precedent he sees as conflicting with originalism, a position that Justice Scalia differentiated himself from, saying "I'm an originalist and a textualist, not a nut." *See* Jeffrey Rosen, *What Made Antonin Scalia Great*, ATLANTIC (Feb. 15, 2016), https://www.theatlantic.com/politics/archive/2016/02/what-made-antonin-scalia-great/462837/ [https://perma.cc/9MGB-9UUX] (quoting Scalia).

341 *Amy Coney Barrett Senate Confirmation Hearing Day 3 Transcript*, at 31:54, REV (Oct. 14, 2020), https://www.rev.com/blog/transcripts/amy-coney-barrett-senate-confirmation-hearing-day-3-transcript [https://perma.cc/Y4WK-VMA2] ("When I said Justice Scalia's philosophy is mine too, what I meant is that his jurisprudential approach to text as we've talked about originalism and textualism is the same that I would take.").

342 *See, e.g.*, Eric Posner, *Is Brett Kavanaugh an Originalist?*, ERIC POSNER BLOG (Jul. 18, 2018), http://ericposner.com/is-brett-kavanaugh-an-originalist/ [https://perma.cc/LST2-58UY] (describing both critics and supporters as claiming Kavanaugh is an originalist but finding "no evidence" for this and concluding Kavanaugh is a textualist and not an originalist).

343 Joshua B. Fischman & Tonja Jacobi, *The Second Dimension of the Supreme Court*, 57 WM. & MARY L. REV. 1671, 1709–11 (2016) (mapping the Court in two dimensions,

exceptions to *Miller* and *Smith* on pragmatic grounds that considered the reality of the ubiquity of smartphones in everyday life.[344] Yet, both exceptions were written as narrow carve-outs, suggesting that the Chief Justice may be more attracted to the patchwork approach.[345] However, there is reason to think the Chief Justice may favor a more structured approach in future. In crafting these exceptions, Chief Justice Roberts was attempting to hew a path that favored functionality over formality, retaining foundational analysis based on precedent without entering a potentially increasingly problematic quagmire. But in opting for exceptions, the Chief Justice created a different problem for himself. Most commentators agree that the Chief Justice is exceptionally concerned with Court legitimacy,[346] and pressure to keep up public appearances of impartiality has recently increased following numerous proposals for court-packing to mitigate the perceived disparities between the very conservative Court and the more moderate public.[347] By crafting exceptions to *Smith* and *Miller* for cell phones while maintaining those highly intrusive rules for other privacy applications, the Chief Justice left himself particularly vulnerable to critiques pertaining to legitimacy.

Scholars have pointed out that the Chief Justice promotes Fourth Amendment protections for people who resemble him, particularly those who are rich, white, and tend not to be harassed by the police, while showing little concern for privacy intrusions that mostly affect poorer people of color and more traditionally harassed minorities.[348]

---

ideological and methodological, and measuring Roberts as a pragmatist rather than formalist).

344 Riley v. California, 573 U.S. 373, 385 (2014) (modern cell phones "are now such a pervasive and insistent part of daily life" that they ought to be treated differently from physical objects); *Carpenter*, 138 S. Ct. at 2216–17 (reasoning that "cell phone location information is detailed, encyclopedic, and effortlessly compiled," and so the involvement of "a third party does not by itself overcome the user's claim to Fourth Amendment protection").

345 See *supra* Section III.A.

346 *See, e.g.*, Jeffrey Rosen, *John Roberts Is Just Who the Supreme Court Needed*, ATLANTIC (July 14, 2020), https://www.theatlantic.com/ideas/archive/2020/07/john-roberts-just-who-supreme-court-needed/614053/ [https://perma.cc/SAT2-B8NQ] (describing key Roberts votes in the 2019 term as driven by the need to protect the legitimacy of the Court).

347 *See, e.g.*, Sam Gringlas, *Asked About Court Packing, Biden Says He Will Convene Commission to Study Reforms*, NPR (Oct. 22, 2020), https://www.npr.org/2020/10/22/926607920/asked-about-court-packing-biden-says-he-will-convene-commission-to-study-reforms [https://perma.cc/5ZNT-7HSE].

348 *See* Franks, *supra* note 8, at 467–68 (stating that the *Jones* vehicle search "is clearly the kind of violation the Justices could imagine themselves experiencing, whereas they may have had a harder time contemplating the possibility of being an arrestee subjected to an invasive strip search before being admitted into the general population of a jail," as was permitted in *Florence v. Board of Chosen Freeholders*, 566 U.S. 318 (2012)); *see also* John W. Whitehead, *Strip-Searching America:* Florence v. County of Burlington, HUFFPOST (June 4,

Likewise, Justice Sotomayor has called out Court majorities for ignoring the disparate impact that Supreme Court Fourth Amendment rulings have on minorities traditionally targeted and harassed by the police.[349] As such, there is good reason to think that the Chief may feel pressure to embrace a more coherent approach to search and seizure jurisprudence, even if a more structured *Katz*ian approach may not be his first choice.

Justice Alito is likewise disinclined to originalism.[350] In *Jones*, he mocks Justice Scalia's originalist trespass analysis of the attachment and monitoring of a GPS device thus:

> [I]t is almost impossible to think of late-18th-century situations that are analogous to what took place in this case. (Is it possible to imagine a case in which a constable secreted himself somewhere in a coach and remained there for a period of time in order to monitor the movements of the coach's owner?)[351]

Similarly, Justice Alito is on record as being equally suspicious of maintaining the status quo with an ever-growing list of exceptions to *Smith* and *Miller*. In *Carpenter*, the Chief justifies his incrementalist approach by warning that "when considering new innovations . . . the Court must tread carefully in such cases, to ensure that we do not 'embarrass the future.'"[352] Justice Alito responds: "Although the majority professes a desire not to 'embarrass the future,'" that may mean that instead

> this Court will face the embarrassment of explaining in case after case that the principles on which today's decision rests are subject to all sorts of qualifications and limitations that have not yet been discovered . . . [and] inevitably end up "mak[ing] a crazy quilt of the Fourth Amendment."[353]

Accordingly, although Chief Justice Roberts and Justice Alito may share little in common with Justices Breyer, Sotomayor, and Kagan in

---

2012, 11:12 AM), https://www.huffpost.com/entry/supreme-court-strip-searches_b_1401063 [https://perma.cc/D7S7-YE7C].

349 *See, e.g.*, Utah v. Strieff, 136 S. Ct. 2056, 2071 (2016) ("We must not pretend that the countless people who are routinely targeted by police are 'isolated.' They are the canaries in the coal mine whose deaths, civil and literal, warn us that no one can breathe in this atmosphere.").

350 For instance, Justice Alito mockingly commented in a First Amendment case, "Well, I think what Justice Scalia wants to know is what James Madison thought about video games." Transcript of Oral Argument at 17, Brown v. Ent. Merchs. Ass'n, 564 U.S. 786 (2010) (No. 08-1448).

351 United States v. Jones, 565 U.S. 400, 420 (2012) (Alito, J., concurring) (footnote omitted).

352 Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (quoting Nw. Airlines, Inc. v. Minnesota, 322 U.S. 292, 300 (1944)).

353 *Id.* at 2260–61 (Alito, J., dissenting) (quoting Smith v. Maryland, 442 U.S. 735, 745 (1979)).

terms of preferred outcomes in search and seizure cases, there is good reason to think that there is a five-justice majority for finding a solution to the problems of the third-party doctrine beyond stitching together that Frankensteinian quilt of exceptions and carve-outs. Our proposal is the most feasible, as well as the most jurisprudentially well-buttressed, non-originalist solution available. Those five justices may apply the approach differently, meaning our proposal does not guarantee outcomes. But we are not arguing for particular outcomes, rather for a coherent and well-grounded approach, and there are potentially five votes for taking that route.

CONCLUSION: THE THIRD-PARTY DOCTRINE IN SHAPING RESPONSES TO PANDEMICS AND OTHER CRISES

In the United States, the COVID-19 pandemic has claimed over 620,000 lives and strained the health care system to its breaking point.[354] Nations around the world have tried a variety of measures to slow the spread of the disease, some utilizing aggressive testing and tracing regimes.[355] In the United States, the response has been state-driven, with a variety of approaches leading to mixed results; some states have implemented strategies like contact tracing,[356] location tracking,[357] and self-reporting and quarantining, which have been shown to be successful at limiting the spread—and subsequent damage—of the disease.[358] These responses raise serious concerns of how to balance public health and individual privacy and are greatly complicated by the third-party doctrine. These dilemmas are not going to disappear even with broad distribution of the coronavirus

354 *COVID Data Tracker*, CDC (as of Aug. 26, 2020), https://covid.cdc.gov/covid-data-tracker/#cases_casesper100klast7days [https://perma.cc/8X3C-HAK2].

355 Ian Bremmer, *The Best Global Responses to the COVID-19 Pandemic, 1 Year Later*, TIME (Feb. 23, 2021), https://time.com/5851633/best-global-responses-covid-19/ [https://perma.cc/QG9U-GABC] (detailing the initial success of Taiwan, Singapore, Germany, and New Zealand in large part due to aggressive testing and tracing regimes).

356 Frances Stead Sellers & Ben Guarino, *Contact Tracing Is 'Best' Tool We Have Until There's a Vaccine, Health Experts Say*, WASH. POST (June 14, 2020), https://www.washingtonpost.com/national/contact-tracing-is-best-tool-we-have-until-theres-a-vaccine-say-health-experts/2020/06/13/94f42ffa-a73b-11ea-bb20-ebf0921f3bbd_story.html [https://perma.cc/24UX-DBQ4].

357 Dave Muoio, *Google Mobilizes Location Tracking Data to Help Public Health Experts Monitor COVID-19 Spread*, MOBIHEALTHNEWS (Apr. 6, 2020), https://www.mobihealthnews.com/news/google-mobilizes-location-tracking-data-help-public-health-experts-monitor-covid-19-spread [https://perma.cc/X5WN-KXUE].

358 *See* Christie Aschwanden, *Contact Tracing, a Key Way to Slow COVID-19, Is Badly Underused by the U.S.*, SCI. AM. (July 21, 2020), https://www.scientificamerican.com/article/contact-tracing-a-key-way-to-slow-covid-19-is-badly-underused-by-the-u-s/ [https://perma.cc/G78U-JLLY].

vaccine—experts warn that due to "increased contact between humans and wild animals and global transportation networks," large-scale infectious disease outbreaks are increasingly likely to arise again.[359] As such, resolving the third-party doctrine is vital to ensuring that the United States can effectively respond to this and likely future pandemics. Likewise, it will affect responsiveness to other crises, such as terrorism, climate change, and any challenges that require tracking or other public cooperation.

Manual contact tracing, which is widely viewed as one of the most important tools for combating the spread of COVID-19, has involved tens of thousands of investigators calling the recently infected and asking for sensitive information about their health and potential contacts.[360] The investigators then must call those contacts and suggest they self-quarantine.[361] If any of the contacts begin showing symptoms, investigators must continue the process until there are no more new cases.[362] Consensus has grown around the need for smart testing and tracing based on digital tools and devices, but the process is limited by people's willingness to report,[363] which is understandably constrained given the third-party doctrine deeming such highly personal information "voluntarily" shared, and so left unprotected by the Fourth Amendment, if they cooperate.

Tech companies like Apple and Google have partnered with state and federal governments to create contact tracing apps,[364] track

359 Milana Boukhman Trounce & George P. Shultz, *COVID-19 and Future Pandemics*, HOOVER INST. (July 30, 2020), https://www.hoover.org/research/covid-19-and-future-pandemics [perma.cc/8R4K-V3ZY]; *Future Pandemics Likely to Be Deadlier and More Frequent, Warns UN Panel*, FRANCE24 (Oct. 30, 2020), https://www.france24.com/en/environment/20201030-future-pandemics-likely-to-be-deadlier-and-more-frequent-warns-un-panel [perma.cc/BB5K-XTMT] ("Future pandemics will happen more often, kill more people and wreak even worse damage to the global economy than Covid-19 . . . . [due to] deforestation, agricultural expansion, wildlife trade and consumption—all of which put humans in increasingly close contact with wild and farmed animals and the diseases they harbour.").

360 Mike Reicher, David Gutman & Ryan Blethen, *Despite Army of Workers, Coronavirus Contact Tracing in Washington State Is Challenging*, SEATTLE TIMES (June 16, 2020), https://www.seattletimes.com/seattle-news/times-watchdog/despite-army-of-newly-trained-workers-challenges-with-coronavirus-contact-tracing-in-washington-state-remain/ [https://perma.cc/4DFH-RRGL].

361 *Id.*

362 *See id.*

363 VI HART ET AL., EDMOND J. SAFRA CTR. FOR ETHICS, OUTPACING THE VIRUS: DIGITAL RESPONSE TO CONTAINING THE SPREAD OF COVID-19 WHILE MITIGATING PRIVACY RISKS 29 (2020).

364 *See* Mike Feibus, *Are Coronavirus Contact Tracing Apps Doomed to Fail in America?*, USA TODAY (June 25, 2020), https://www.usatoday.com/story/tech/columnist/2020/06/24/apple-google-contact-tracing-apps-privacy/3253088001/ [https://perma.cc/V2SR-22FE].

contacts through Bluetooth-enabled devices,[365] and track anonymized location data on a larger scale to determine movement trends.[366] While the motivation may be benevolent, the risks are obvious. In an attempt to show the difficulties in containment and the dangers of ignoring social distancing requirements, mobile technology company X-Mode fed cellular location data collected during spring break into mapping platform Tectonix.[367] In a video released on Twitter, X-Mode and Tectonix were able to map every active device from a single Florida beach and track where those devices ended up.[368] This information is typically anonymized, and the companies involved maintain that privacy is a top concern, yet researchers have repeatedly shown that it is possible to re-identify members of anonymized datasets with only a handful of data points, such as gender, zip code, or date of birth.[369]

The reliance on big data and tech companies to facilitate contact tracing through smart device applications has significant implications for the third-party doctrine. Traditionally, contact tracing information was gathered manually and given voluntarily to a third party, which clearly activates the third-party doctrine.[370] If such tracking was made mandatory, for instance through a required phone app download directed by the government, as was done in South Korea,[371] that would run afoul of the resurgent trespass doctrine articulated in *Jones*.[372] What creates a murkier constitutional issue is the current situation, where data is gathered, processed, and shared with the government by third parties. Under the Court's current post-*Carpenter* jurisprudence, it can be argued that knowingly sharing information with another reduces, but does not eliminate, constitutional privacy interests

365 HART ET AL., *supra* note 363, at 12–20.

366 Jason Murdock, *Mobile Phone Location Data of Florida Beachgoers During Spring Break Tracked to Show Potential Coronavirus Spread*, NEWSWEEK (March 27, 2020), https://www.newsweek.com/x-mode-tectonix-coronavirus-heat-map-tracking-mobile-data-covid-19-spring-break-1494663 [https://perma.cc/P995-6GLL].

367 *Id.*

368 *Id.*

369 *See* Natasha Lomas, *Researchers Spotlight the Lie of 'Anonymous' Data*, TECHCRUNCH (July 24, 2019), https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/ [https://perma.cc/2YX3-3GGWL] (showing that, outside of strict access controls, no current tools can protect anonymized data from re-identification).

370 Alan Z. Rozenshtein, *Disease Surveillance and the Fourth Amendment*, LAWFARE (Apr. 7, 2020, 1:54 PM), https://www.lawfareblog.com/disease-surveillance-and-fourth-amendment [https://perma.cc/Y2C5-ZHXH].

371 Aaron Holmes, *South Korea Is Relying on Technology to Contain COVID-19, Including Measures That Would Break Privacy Laws in the US—and So Far, It's Working*, BUS. INSIDER (May 2, 2020), https://www.businessinsider.com/coronavirus-south-korea-tech-contact-tracing-testing-fight-covid-19-2020-5#a-mandatory-government-run-smartphone-app-tracks-the-location-of-all-new-arrivals-to-the-country-1 [perma.cc/SVH9-HAGL].

372 *See* United States v. Jones, 565 U.S. 400, 409 (2012).

depending on the type of information, but that is far from a sure winning argument because technically that ruling only applies to historical cell phone location information.[373] Information that would normally be outside the scope of the Fourth Amendment under the third-party doctrine may now retain constitutional protection based on its sensitive or revealing nature—but what constitutes adequately sensitive or revealing information, and how broad the revelation needs to be, is an inquiry that can vary from court to court and judge to judge.[374]

Under the current standard, a key factor in determining whether the Fourth Amendment applies is the voluntariness of the sharing. Yet this analysis, too, is woefully underutilized; according to the Court's reasoning in *Smith*, it is likely that merely owning a cell phone would be enough to indicate knowledge.[375] But, as Justice Marshall queried in dissent, if a piece of technology is necessary to function in society, can its use convey a willingness to share information?[376] In *Smith*, the majority said "yes"; in *Carpenter*, the majority seemingly said "no"—or at least "not always." This also begs the further question: Can it be considered "knowing" if people do not truly understand what is being gathered and how the information is being used, or if the prompted explanations are vague or misleading?[377] This is precisely why the Court in *Katz* expanded Fourth Amendment protections to cover actions outside the home—because as technology changed, the ways people conveyed information changed, and the privacy standards protected by the Fourth Amendment needed to be adaptive to those changes.[378]

While people may support sacrificing their rights temporarily to combat a global pandemic,[379] it is unlikely the majority of Americans

373 *See* Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

374 *Id.* at 2217; *see supra* Section III.A.

375 Smith v. Maryland, 442 U.S. 735, 742–43 (1979).

376 *Id.* at 750 (Marshall, J., dissenting) ("[U]nless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance.").

377 Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller & Aaron Krolik, *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html [https://perma.cc/LD46-C5MM].

378 Katz v. United States, 389 U.S. 347, 352 (1967) ("To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.").

379 "There is often a general willingness on the part of the public to accept greater civil liberties deprivations in the face of a specific threat . . . ." Fletcher N. Baldwin, Jr. & Daniel Ryan Koslosky, *Mission Creep in National Security Law*, 114 W. VA. L. REV. 669, 671 (2012) (analyzing how deference to the executive during times of crisis can lead to medium- and long-term unintended consequences involving civil liberties).

understand the potential post-COVID privacy risks. Under the third-party doctrine, it is unclear whether or not sharing information during the pandemic means one loses one's privacy rights in that information forevermore. The government might use location information and contact tracing during a pandemic, but once that information is given over to government health officials, what is to stop government investigators from using that same information to locate someone during a criminal investigation, or monitor large-scale movements during widespread public protesting? Police in Minneapolis are already using "contact tracing for who [arrested protestors] are associated with, [and] what platforms are they advocating for."[380] And while the Minneapolis police department was not referring to using medical contact tracing as part of its investigations,[381] there is little legal protection for that information once it is given to third parties.

Without a clearer standard for what kind of shared information is and is not protected by the Fourth Amendment's warrant requirement, it is left to third parties and the government to govern their own actions and abide by suggestions offered by interest groups and academics.[382] For-profit companies do not have a great track record with this sort of self-governance.[383] Since 1999, Google's privacy policy has changed dramatically, often adding difficult-to-find clauses that opt users in to dramatically increased third-party sharing programs.[384] Google was also forced to pay a $22.5 million fine to the Federal Trade Commission (FTC) for placing "tracking cookies" on certain users' computers despite assurances to the contrary.[385] And the FTC fined Facebook $5 billion for using "deceptive disclosures and settings" that "allowed the company to share users' personal information with third-party apps that were downloaded by the user's

380 Alfred Ng, *Contact Tracers Concerned Police Tracking Protestors Will Hurt COVID-19 Aid*, CNET (June 1, 2020), https://www.cnet.com/news/contact-tracers-concerned-police-tracking-protesters-will-hurt-covid-19-aid/ [https://perma.cc/9AU2-C3DJ].

381 *Id.*

382 *See, e.g.*, Jessica Davis, *ACLU, Scientists Urge Privacy Focus for COVID-19 Tracing Technology*, HEALTHITSECURITY (Apr. 20, 2020), https://healthitsecurity.com/news/aclu-scientists-urge-privacy-focus-for-covid-19-tracing-technology [https://perma.cc/458M-U25X].

383 Valentino-DeVries et al., *supra* note 377 (describing how mapping the path of a consumer from home to work could reveal a person's preferences); *see supra* Part II.

384 Charlie Warzel & Ash Ngu, Opinion, *Google's 4,000-Word Privacy Policy Is a Secret History of the Internet*, N.Y. TIMES (July 10, 2019), https://www.nytimes.com/interactive/2019/07/10/opinion/google-privacy-policy.html [https://perma.cc/TWS8-YA2B].

385 Press Release, Fed. Trade Comm'n, Google Will Pay $22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented [https://perma.cc/6FY3-782B].

Facebook 'friends.'"[386] Since the information was gathered from apps used by other people, many users were unaware their information was being collected at all and did not take the necessary steps to opt out.[387] This only changed when European regulations required users opt in to being tracked across apps and websites, and only under threat of fines.[388]

Further, as studies begin to show that other smart devices like Apple Watches, Fitbits, and Oura Rings can potentially provide early warnings for COVID-19 infections, it is increasingly unclear whether or not this information can and should also be provided to the government.[389] There is little doubt that contact tracing and quarantining would be far more effective if the government, through a Fitbit, could tell whether a person was infected while they were still asymptomatic, and thus at the greatest risk of spreading the disease.[390] But once the government has access to such location information, associational contacts, and health information, it has little incentive not to continue to use it and to provide that information to other government agencies, including for the purposes of criminal investigation. This phenomenon is known as "mission creep," or in this context, "surveillance creep": when information gathered for one legitimate purpose is used for another, less legitimate purpose.[391] Mission creep is a valid fear. Information gathered by the NSA largely for the purposes of national security from foreign threats was used by a secretive U.S. Drug Enforcement Administration which funneled

386 Press Release, Fed. Trade Comm'n, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions [https://perma.cc/3GXD-7Q7E].

387 *Id.*

388 *What Does the GDPR Mean for Business and Consumer Technology Users*, GDPR.EU, https://gdpr.eu/what-the-regulation-means-for-everyday-internet-user/ [https://perma.cc/2DSQ-DV5E] (describing new rules prohibiting sending of marketing emails or collecting personal information "unless you explicitly grant permission").

389 Geoffrey A. Fowler, *Wearable Tech Can Spot Coronavirus Symptoms Before You Even Realize You're Sick*, WASH. POST (May 28, 2020), https://www.washingtonpost.com/technology/2020/05/28/wearable-coronavirus-detect/ [https://perma.cc/2WGK-HPR7].

390 *See* Anuja Vaidya, *COVID-19 Patients Most Infectious Before, Right After Symptom Onset, Study Finds*, BECKER'S HOSP. REV. (May 5, 2020), https://www.beckershospitalreview.com/infection-control/covid-19-patients-most-infectious-before-right-after-symptom-onset-study-finds.html [https://perma.cc/P4V7-GQRE].

391 Wendy K. Mariner, *Mission Creep: Public Health Surveillance and Medical Privacy*, 87 B.U. L. REV. 347, 348–50 (2007) (describing that disease surveillance was originally created at the end of the nineteenth century to contact, trace, and prevent contagious diseases like smallpox, but today is largely used for "statistical analysis, planning, budgeting, and general research").

"information from intelligence intercepts, wiretaps, informants and a massive database of telephone records to authorities across the nation to help them launch criminal investigations of Americans."[392]

As well as mission creep, we must consider potentially endless missions. People might be more willing to provide access to private information during the pandemic if access to such data and the continuing gathering of it ends once the threat of COVID has passed. However, access to such useful information makes the government historically disinclined to give it up. For instance, the PATRIOT Act was passed in 2001 to respond to the 9/11 attacks;[393] until 2020, that legislation continued to blur the line between intelligence gathering and criminal investigations in ways that now implicate domestic crime wholly excluded from terrorist threats.

It is not uncommon for techniques and procedures to be developed during a time of crisis and remain in place long after the crisis has ended. Disease surveillance—of which contact tracing is a type—began at the end of the nineteenth century as a way to track smallpox.[394] Today, disease surveillance and compulsory reporting is suggested for twenty-nine newborn genetic conditions, more than sixty infectious diseases, and to track potentially contaminated food.[395] This information now provides public health researchers with data unburdened by consent and the rigors of an academic study.[396] The income tax, first introduced in Great Britain in 1799, began as a temporary war measure.[397] Similarly, daylight saving time originated as a way to save fuel during World War I, yet it has slowly been extended over the ensuing decades.[398] There are no structural limitations that ensure the use of third-party data gathered during this emergency will be limited to this emergency only. And the Court has only provided an admittedly narrow type of third-party information that cannot be

392 John Shiffman & Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, REUTERS (Aug. 5, 2013), https://www.reuters.com/article/us-dea-sod/exclusive-u-s-directs-agents-to-cover-up-program-used-to-investigate-americans-idUSBRE97409R20130805 [https://perma.cc/52WW-D8LH].

393 Baldwin & Koslosky, *supra* note 379, at 670–71.

394 Mariner, *supra* note 391, at 349.

395 *Id.* at 350; *Report a Problem with Food*, FOODSAFETY.GOV (Sept. 3, 2019), https://www.foodsafety.gov/food-poisoning/report-problem-with-food [https://perma.cc/3DEZ-YAZN].

396 Mariner, *supra* note 391, at 350–51.

397 *Income Tax*, POLITICS.CO.UK, https://www.politics.co.uk/reference/income-tax [https://perma.cc/P9WU-ZLRH].

398 Olivia B. Waxman, *The Real Reason Why Daylight Saving Time Is a Thing*, TIME (Nov. 1, 2017), https://time.com/4549397/daylight-saving-time-history-politics/ [https://perma.cc/GHV9-VX9N].

gathered without a warrant—how to fit other kinds of information into this standard is unclear.[399]

The Court's categorical third-party doctrine rendered this type of information unprotected long before COVID. The COVID crisis merely accelerated the expansion of data already potentially available to the government and the issues the third-party doctrine raises in terms of government responsiveness go well beyond COVID. The government had potential access to health data through Fitbit, Garmin, and other health tracking devices; to images of a person's private property through front door cameras; and to internet call transcripts through providers.[400] COVID simply illustrates the problem of the third-party doctrine in stark, highly personal terms. But the reverse problem is potentially even more severe: the third-party doctrine's stringency could hamper the ability of the U.S. to effectively combat COVID and future crises by making people unwilling to share their data, essential to tracking the spread of the disease, out of fear of loss of privacy—a fear that is very much justified. And COVID is actually likely to make the problem worse, as these two effects reinforce each other.

Without a stronger, clearer rule of what information given to a third party can be accessed by the government, a circularity problem is created: the government starts tracking location information to respond to COVID; that action is reasonable in light of the global pandemic; the government begins to use that tracking information for other health crises and natural disasters; it becomes commonplace and its use reasonable, and expectations of privacy recede as a result.[401] Add to that a stringent rule that any information given to a third party means we can skip even that circular analysis, and assume the information is unprotected, then the Supreme Court might just be creating a major stumbling block for solving the pandemic in the U.S. Either, contrary to its assumptions, individuals do not understand the significance of sharing their information with the government, and so the presumptions of the third-party doctrine are wrong; or else, they do understand, and are unlikely to be willing to make that sacrifice,

399 Rozenshtein, *supra* note 370 ("Unfortunately the court did not provide much guidance on how to apply *Carpenter*'s reasoning to different fact patterns . . . .").

400 *See supra* Part II.

401 Scholars and judges alike have recognized the circularity danger in *Katz*'s reasonable expectation of privacy test. *See* Richard A. Posner, *The Uncertain Protection of Privacy by the Supreme Court*, 1979 SUP. CT. REV. 173, 188 ("[I]t is circular to say that there is no invasion of privacy unless the individual whose privacy is invaded had a reasonable expectation of privacy; whether he will or will not have such an expectation will depend on what the legal rule is."); Erwin Chemerinsky, *Rediscovering Brandeis's Right to Privacy*, 45 BRANDEIS L.J. 643, 650 (2007) ("The government seemingly can deny privacy just by letting people know in advance not to expect any.").

meaning that people will be less willing to provide information that could actually stop this deadly disease.[402] The Supreme Court might carve out one of its few exceptions, specifically curtailing application of the third-party doctrine for COVID information, but that will come too late to be useful in responding to this fast-changing pandemic and will not answer the same conundrum as applied to future crises.

The COVID pandemic provides a stark illustration of just how inappropriate the assumptions made by the Supreme Court are in the third-party doctrine, and how inadequate it is to provide protection by carving out narrow exceptions, years after state action has occurred. But the problem has always been there since the Court made the third-party doctrine artificially categorical, ignoring the mandate of *Katz* to actually examine the circumstances of each case, ascertaining whether there truly is a reasonable expectation of privacy. Perhaps the breadth of the governmental response required to combat the COVID pandemic will inspire the Supreme Court to reform this problematic doctrine. Our solution provides a roadmap for doing so in a way that provides appropriate protection for private information while giving third parties and the government the flexibility to deal with an impending crisis. Under the correct reading of *Katz*'s third-party rule, information is outside the scope of the Fourth Amendment when it is "knowingly expose[d] to the public." Those words need to be given genuine meaning, not simply assumed to be met simply by the fact that a person has given information to a third party, however unknowingly, unwillingly, or inadvertently, and regardless of the role of that third party.

402 A majority (58%) of U.S. adults say they would be "very or somewhat likely to speak with a public health official who contacted them by phone or text message to speak with them about the coronavirus outbreak" but a minority (49%) "say they would be similarly comfortable sharing location data from their cellphone." Colleen McClain & Lee Rainie, *The Challenges of Contact Tracing as U.S. Battles COVID-19*, PEW RSCH. CTR. (Oct. 30, 2020), https://www.pewresearch.org/internet/2020/10/30/the-challenges-of-contact-tracing-as-u-s-battles-covid-19/ [https://perma.cc/L7FC-7ZK7].