IF THESE WALLS COULD TALK: THE SMART HOME AND THE FOURTH AMENDMENT LIMITS OF THE THIRD PARTY DOCTRINE

Imagine a not-so-distant future in which you can open the blinds, turn on your shower, start the coffee machine, turn on the lights, and change your thermostat, all without getting out of bed. You may be able to control these functionalities from your smart phone, or better yet, dictate your commands to a smart home "assistant" or hub, which will then implement these commands throughout your home. Your automated assistant recites your schedule for the day, along with directions for how to reach all your destinations. Once you've left the house, you can monitor your security cameras from a feed on your cell phone and lock your door from an application on your phone. Your refrigerator knows what groceries you have run out of and alerts you, or perhaps goes ahead and orders them for you.[1] If your home automation system is any good, it should also be able to "learn" about your habits and implement your preferences automatically.[2] The convenience is alluring.

The emergence of home automation — otherwise known as the "smart home" — is a natural step in the proliferation of everyday products that connect to the internet. Smart home technologies necessitate the sharing of personal information across a multitude of third-party service providers, which is disconcerting to privacy advocates.[3] Beyond possession of this information by private third parties, what looms largest is the threat of government collection and aggregation of this information from said third parties.[4] The detrimental effects of such unconstrained information gathering are well documented.[5] More generally, the collection of such information represents ever-

---

[1] *See* Monica Nickelsburg, *Microsoft Is Building a "Smart Fridge" for Not-So-Smart Grocery Shoppers, Like Me*, GEEKWIRE (Sept. 2, 2016, 1:22 PM), http://www.geekwire.com/2016/microsoft-building-smart-fridge-not-smart-grocery-shoppers-like/ [https://perma.cc/XGG5-3WCH].

[2] *See, e.g.*, Jacqui Cheng, *A Thermostat That Learns? Three Months with the Nest*, ARS TECHNICA (Aug. 2, 2012, 9:00 PM), https://arstechnica.com/gadgets/2012/08/a-thermostat-that-learns-three-months-with-the-nest/ [https://perma.cc/Y97X-MAYB].

[3] Andreas Jacobsson, *On Privacy and Security in Smart Homes*, MEDIUM (June 14, 2016), https://medium.com/@iotap/on-privacy-and-security-in-smart-homes-543f62aa9917 [https://perma.cc/EAH5-XZL4].

[4] *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1089–114 (2002).

[5] These negative consequences include making it easier for the government to exercise totalitarian control, chilling freedom of association and democratic activities, and increasing chances for abuse or misuse of personal information. *See* Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435, 436–37 (2008); Solove, *supra* note 4, at 1101–14.

growing intrusions into personal privacy. Our daily activities increasingly involve turning over information to third parties in order to undertake basic transactions, such as online banking, email, internet browsing, and cell phone use. Further, such advances in technology make it such that "those records are linked and shared more widely and stored far longer than ever before, often without the individual consumer's knowledge or consent."[6]

However, one may be surprised to learn that many of these personal digital records are not granted Fourth Amendment protection, simply because they have been shared with third parties.[7] Further, Fourth Amendment jurisprudence in this sphere has not adequately evolved to compensate for the rapid explosion in both the quantity and sensitive quality of the information shared in this way. In large part, the inadequacy of this response can be attributed to courts' continued application of the third party doctrine, under which the government is able to access such private information without a warrant, thereby effectively allowing the government access to large aggregations of personal data.[8] The doctrine has been used to allow warrantless collection of email records, internet browsing data, and cell phone location history, among others.[9] The basis for the rule is that information relinquished to a third party is no longer considered private.[10]

This Note argues that the current third party doctrine cannot adequately protect individuals' privacy rights that are implicated in the smart home context. Thus, the Supreme Court ought, and may be especially inclined, to update the doctrine. Further, the Court can do so in a way that is consistent with its own Fourth Amendment jurisprudence — by applying the context-based "reasonable expectation of privacy" test.[11] Namely, the Court should consider the voluntariness of the disclosure, the nature of the information shared, and the identity of the recipients, as it did when deciding the cases leading up to what is now the third party doctrine. The context of smart homes puts the modern absurdity of the third party doctrine into especially stark relief. "[I]f the machines [and the government] are watching, maybe the

---

[6] Cate, *supra* note 5, at 456; *see also* Rebecca Lipman, Note, *The Third Party Exception: Reshaping an Imperfect Doctrine for the Digital Age*, 8 HARV. L. & POL'Y REV. 471, 471–72 (2014).

[7] *See, e.g.*, 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.").

[8] *See* Solove, *supra* note 4, at 1085–86.

[9] Natasha H. Duarte, Recent Development, *The Home Out of Context: The Post-*Riley *Fourth Amendment and Law Enforcement Collection of Smart Meter Data*, 93 N.C. L. REV. 1140, 1142 (2015).

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

[11] *See* Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring) (establishing the test).

home is not really the home anymore?"[12] The home is the bedrock of the Supreme Court's Fourth Amendment jurisprudence, where individuals' privacy interests are at their peak.[13] It is difficult to imagine that the Court would countenance the third-party exception's working to provide the government warrantless entry into any home it wishes.

Part I discusses the evolution of the third party doctrine. Part II discusses modern applications of the third party doctrine. Part III explores the growing tensions between the doctrine and our shifting technological landscape. Part IV concludes by demonstrating how the application of the third party doctrine — and the outdated binaries that comprise it — is rendered especially absurd and problematic in the smart home context. It also posits that the application of the doctrine to the home, an area where the Court has been most unwilling to compromise Fourth Amendment protection, presents the ideal (and perhaps necessary) opportunity for the Court to reconsider the doctrine, which it can do by applying its own contextually mediated reasonable expectation of privacy test.

I. THE EVOLUTION OF THE THIRD PARTY DOCTRINE

A. Katz v. United States

The beginning point of the third party doctrine is *Katz v. United States*,[14] in which the Supreme Court established the reasonable expectation of privacy test.[15] In *Katz*, the Court held that wiretapping of telephone calls made in a public telephone booth constituted a search and therefore required a warrant.[16] The innovation of *Katz* was that physical intrusion was no longer necessary to constitute a search.[17] Up to this point, to be considered a search under the Fourth Amendment, searches typically had to occur inside someone's home.[18] In rejecting the Government's argument that such precedents should apply, the Court countered that "the Fourth Amendment protects people, not places . . . . [W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[19]

---

[12] Jacobsson, *supra* note 3.

[13] Daniel T. Pesciotta, Note, *I'm Not Dead Yet:* Katz*,* Jones*, and the Fourth Amendment in the 21st Century*, 63 CASE W. RES. L. REV. 187, 254 (2012).

[14] 389 U.S. 347.

[15] *See id.* at 361 (Harlan, J., concurring).

[16] *See id.* at 353 (majority opinion).

[17] *See id.* at 359.

[18] *Id.* at 352–53 ("It is true that the absence of such [physical] penetration was at one time thought to foreclose further Fourth Amendment inquiry, . . . for that Amendment was thought to limit only searches and seizures of tangible property." (citing Olmstead v. United States, 277 U.S. 438, 457, 464, 466 (1928); Goldman v. United States, 316 U.S. 129, 134–36 (1942))).

[19] *Id.* at 351–52.

Therefore, a person's individual expectations of privacy should affect the substantive reach of her Fourth Amendment protections.

Justice Harlan's concurrence articulated a two-part framework for the *Katz* test, first asking whether the individual manifested "an actual (subjective) expectation of privacy," and second, whether that expectation is one that "society is prepared to recognize as 'reasonable'" (objective).[20] He emphasized the personal aspect of privacy and how (subjective) expectations of privacy can be inferred from conduct. Applied to the phone booth context, he found it relevant that a phone booth user shuts the door behind him and generally can expect his call will be private.[21] The Court later endorsed this two-part test as central to the Fourth Amendment analysis.[22]

The *Katz* opinion was quite innovative, in that it was willing to overturn clearly binding precedent in response to social change.[23] As a result, the Court recognized that the interests sought to be protected by the Fourth Amendment were no longer tethered to property, as modern life often took one outside the home.[24] Shortly before the *Katz* opinion, commentators had expressed frustration with the increasingly outdated binary trespass doctrine. One year prior, one scholar had argued that "American society now seems ready . . . to face the impact of science on privacy and to restore the equilibrium among privacy, disclosure, and surveillance."[25] The Court's new approach provided for more individual-based privacy and a way to make more context-dependent determinations of Fourth Amendment protection that could adapt to new technologies. However, in rejecting the trespass binary, the *Katz* Court may have inadvertently laid the groundwork for another — that of secrecy as a proxy for privacy.

B. The Third Party Doctrine Begins to Take Shape

After *Katz*, the Court was faced with the task of squaring the resulting reasonable expectation of privacy test with prior decisions allowing the use of information told in confidence to undercover agents and informants. These prior decisions had held that Fourth Amendment protection does not apply to "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not re-

---

[20] *Id.* at 361 (Harlan, J., concurring).

[21] *See id.*

[22] *See, e.g.*, Bond v. United States, 529 U.S. 334, 338 (2000).

[23] *Katz* overturned *Olmstead v. United States*, 277 U.S. 438, which had limited the Fourth Amendment to property interests.

[24] *See Katz*, 392 U.S. at 359.

[25] Alan F. Westin, *Science, Privacy, and Freedom: Issues and Proposals for the 1970's — Part II: Balancing the Conflicting Demands of Privacy, Disclosure, and Surveillance*, 66 COLUM. L. REV. 1205, 1252 (1966).

veal it."[26] The Court later held that this formulation passed the *Katz* test, as "[h]owever strongly a defendant may trust an apparent colleague, his expectations in this respect are not protected by the Fourth Amendment when it turns out that the colleague is a government agent."[27] This "misplaced confidence" doctrine focused on the voluntary disclosure of the information and the fact that the risk of having one's personally relayed confidences betrayed is "the kind of risk we necessarily assume whenever we speak."[28]

The Court continued to apply this principle in a line of cases that would result in what is now the third party doctrine. First, in *Couch v. United States*,[29] the Court found that the defendant did not have a reasonable expectation of privacy in business records turned over to an accountant (who then turned them over to the IRS).[30] Notably, the Court focused on the *content* of the information disclosed to the accountant, the majority of which was subject to mandatory disclosure for income tax return purposes.[31] Similarly, in *United States v. Miller*,[32] the Court held that documents "voluntarily conveyed" to a bank could be shared with the government.[33] Again, the Court focused on the nature of the documents, citing *Couch* for the proposition that it "must examine the nature of the particular documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents."[34] While the Court relied on the criminal informant cases to support this contention, those cases had relied on the misplaced confidence doctrine to support their conclusions.[35] Such a reliance would have been untenable here. Instead, the Court had to emphasize the voluntariness of the disclosure and the nonsensitivity of the information contained therein. Had the information been more sensitive or substantively detailed (like the daily log of every activity undertaken by one's Nest device[36]), it is hard to say if the Court would have reached the same conclusion.

These very justifications could be used to find reasonable expectations of privacy in the increasingly sensitive and personal information we turn over to third parties. First, many, including Supreme Court

---

[26] Hoffa v. United States, 385 U.S. 293, 302 (1966).
[27] United States v. White, 401 U.S. 745, 749 (1971) (plurality opinion).
[28] Lopez v. United States, 373 U.S. 427, 465 (1963) (Brennan, J., dissenting).
[29] 409 U.S. 322 (1973).
[30] *See id.* at 335–36.
[31] *See id.* at 335.
[32] 425 U.S. 435 (1976).
[33] *Id.* at 442–43.
[34] *Id.* at 442 (quoting *Couch*, 409 U.S. at 335).
[35] *See* Lipman, *supra* note 6, at 474.
[36] *See* Cheng, *supra* note 2.

Justices,[37] have noted that this digital information contains much more detailed, expressive, and personal information than that imagined when the doctrine was established.[38] Furthermore, it's not clear that our modern consistent conveyance of personal information to third parties is as voluntary as that in *Couch* and *Miller*. Increasingly, disclosure of such information is necessary to participate in modern life. Insisting that personal privacy is coextensive with informational secrecy would necessitate the emergence of the "Information Age hermit[]," who, in order to maintain privacy, would have to be unwilling to participate in digital society.[39] Therefore, it is alarming that two major premises upon which the third party doctrine precedent is grounded — the nonsensitivity of the information conveyed and the voluntariness of the conveyance — are negated as the digital age progresses.

Lastly, the Court crystallized and strengthened the third party doctrine in *Smith v. Maryland*[40] in 1979. In *Smith*, the Court moved past bank records and held that law enforcement's use of a pen register — a device that records the numbers dialed by a phone — did not constitute a search.[41] Because Smith had "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business," he could "claim no legitimate expectation of privacy" in the numbers he dialed.[42] The Court made a point of first differentiating the information collected here from that in *Katz*: "[A] pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications."[43] Unlike the *Miller* Court, the *Smith* Court explicitly applied the two-part *Katz* test to the particular situation at hand.[44] In doing so, it held that there could not have been a reasonable expectation of privacy here due to the *voluntary* sharing of the information with a third party and the fact that Smith could not have had a reasonable expectation of privacy in something as nominally informative as the numbers he dialed.[45] Again, voluntariness and minimally sensitive information were key.

---

[37] *See* United States v. Jones, 132 S. Ct. 945, 954–57 (2012) (Sotomayor, J., concurring); *see also* Riley v. California, 134 S. Ct. 2473, 2489–91 (2014); *infra* text accompanying note 115.

[38] *See, e.g.*, Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. NAT'L SECURITY L. & POL'Y 247, 275–76 (2016).

[39] *See* DANIEL J. SOLOVE, THE DIGITAL PERSON 217 (2004).

[40] 442 U.S. 735 (1979).

[41] *Id.* at 745–46.

[42] *Id.* at 744.

[43] *Id.* at 741.

[44] *Id.* at 740–45.

[45] *Id.* at 742–44.

Justice Marshall dissented,[46] decrying the Court's binary conception of privacy: "Privacy is not a discrete commodity, possessed absolutely or not at all."[47] He also took issue with the Court's implicit assumption of risk rationale. He distinguished the facts of *Smith* from those of the undercover-agent cases in that the defendants in those cases "presumably had exercised some discretion in deciding" with whom to share their confidences.[48] "By contrast [in *Smith*], unless a person is prepared to forgo use of what for many has become a personal or professional necessity [like a phone], he cannot help but accept the risk of surveillance."[49] Justice Stewart also dissented.[50] He underscored the fact that the phone numbers collected by pen registers were actually quite informative. A wider network of information could be cobbled together from such large-scale collections of seemingly innocuous information like these telephone numbers.[51] Justice Stewart's words seem prophetic in hindsight.

II. THE THIRD PARTY DOCTRINE TODAY

The third party doctrine has remained relatively undisturbed in the years since *Smith*. But as surveillance methods have become increasingly sophisticated, and the amount of information we share with third-party service providers has exponentially increased, this divergence between doctrine and technology has only become more pronounced. This disjunction is particularly so in the smart home context, as the information relayed to smart home service providers is of perhaps the utmost personal and intimate nature.

A. Modern Applications of Smith

Over the thirty-three years following *Smith*, courts applied the third party doctrine with relative consistency. Recently, courts have applied it to information disclosed to internet service providers,[52] including the to/from addresses of users' emails or the IP addresses of the websites they visit.[53] Historical cell site data (used in the aggregate to track someone's whereabouts over time) was also recently found to

---

[46] *Id.* at 748 (Marshall, J., dissenting). Justice Marshall was joined by Justice Brennan.

[47] *Id.* at 749.

[48] *Id.*

[49] *Id.* at 750 (citing Lopez v. United States, 373 U.S. 427, 465–66 (1963) (Brennan, J., dissenting)).

[50] *Id.* at 746 (Stewart, J., dissenting). Justice Stewart was joined by Justice Brennan.

[51] *Id.* at 748.

[52] *E.g.*, Guest v. Leis, 255 F.3d 325, 335–36 (6th Cir. 2001).

[53] United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008).

fall under the third party doctrine.[54] According to one district court, the exception has been applied to: "(1) bank records; (2) credit card statements; (3) kilowatt consumption from electric utility records; (4) motel registration records; (5) cell phone records; and (6) employment records."[55]

Over time, it seems that the *Smith* inquiry and its application has calcified into a binary one, in which any information disclosed to a third party for any reason is public and does not merit Fourth Amendment protection.[56] In this view, privacy becomes equivalent to secrecy, in that even information that is only narrowly disclosed is no longer considered private.[57] Furthermore, this view conflates disclosure to a private third party with disclosure to the entire world (including the government).[58] While it has the benefit of administrability, this binary approach is increasingly anachronistic and problematic in the digital age.[59] Even if one reveals information "*confidentially* and on the assumption that it will be used only for limited purposes," Fourth Amendment protection is lost.[60] Further, this view does not allow for degrees of privacy; it is not difficult to imagine that one would want and expect to be able to keep some information private in certain respects but not in others. For example, you might be willing to share the contents of your emails with Google while expecting them to be private in other respects. As more of our personal information is electronically stored on third-party servers, this exception threatens to nullify the Fourth Amendment.[61]

B. Stepping Away from the Third Party Doctrine: United States v. Jones

The Supreme Court finally indicated that it might embrace a more flexible interpretation of the third party doctrine with Justice Sotomayor's notable concurrence in *United States v. Jones*.[62] The majority held that extended GPS monitoring constituted a search because

---

[54] *See, e.g.*, United States v. Guerrero, 768 F.3d 351, 359–61 (5th Cir. 2014); *see also In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013).

[55] United States v. Suarez-Blanca, No. 1:07-CR-0023, 2008 WL 4200156, at *8 (N.D. Ga. Apr. 21, 2008) (citations omitted).

[56] *See* 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); Duarte, *supra* note 9, at 1141.

[57] Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1107 (2002).

[58] *See* Colb, *supra* note 56, at 122.

[59] *See* Shaun B. Spencer, *The Surveillance Society and the Third-Party Privacy Problem*, 65 S.C. L. REV. 373, 376 (2013); Duarte, *supra* note 9.

[60] United States v. McIntyre, 646 F.3d 1107, 1112 (8th Cir. 2011) (emphasis added) (quoting United States v. Porco, 842 F. Supp. 1393, 1398 (D. Wyo. 1994)).

[61] Duarte, *supra* note 9, at 1142–43.

[62] 132 S. Ct. 945 (2012).

the placement of the GPS monitoring device on the suspect's car constituted a physical intrusion (trespass).[63] Concurring in the judgment, Justice Sotomayor wrote separately to highlight that, in light of advancing technology, physical intrusion is increasingly unnecessary to conduct surveillance, and that societal expectations of privacy may shift concurrently, thereby implicating the *Katz* test.[64] Reminiscent of Justice Stewart's dissent in *Smith*,[65] Justice Sotomayor also pointed out that in the aggregate, GPS tracking information could reveal comprehensive, detailed personal information about a person's life.[66] This so-called mosaic theory was also identified and discussed in the circuit court opinion of this case — *United States v. Maynard*.[67] In *Maynard*, the D.C. Circuit reversed Jones's conviction because it found that the government's extended warrantless GPS surveillance violated Jones's reasonable expectation of privacy.[68] Particularly, it noted that "[a] person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient, [and so forth.]"[69]

Justice Sotomayor's *Jones* concurrence is perhaps most notable for its explicit call to rethink the third party doctrine, as "[t]his 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."[70] She also referred to Justice Marshall's *Smith* dissent to highlight her discomfort with the binary approach to privacy that treats all voluntarily disclosed information as outside the scope of Fourth Amendment protection.[71] Joined by three Justices, Justice Alito[72] wrote separately to highlight the changing expectations of privacy that advancing technology may bring.[73]

---

[63] *Id.* at 949–51, 953.

[64] *Id.* at 955 (Sotomayor, J., concurring). Justice Alito also discussed this issue in his opinion concurring in the judgment. *See id.* at 962–63 (Alito, J., concurring in the judgment).

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

[66] *See Jones*, 132 S. Ct. at 955–56 (Sotomayor, J., concurring).

[67] 615 F.3d 544, 562–63 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 132 S. Ct. 945.

[68] *See id.* at 563–65.

[69] *Id.* at 562.

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

[71] *Id.* (citing Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting)).

[72] Justice Alito was joined by Justices Ginsburg, Breyer, and Kagan. These Justices did not join the majority opinion.

[73] *See Jones*, 132 S. Ct. at 962–63 (Alito, J., concurring in the judgment).

III. THE FUTURE OF THE THIRD PARTY DOCTRINE

A. An Ever-Growing Anachronism

Although the third party doctrine has long been misguided,[74] it (and its binary implementation) only becomes more anachronistic as the digital age progresses.[75] Notably, even Stephen Sachs, the former Maryland Attorney General who argued on behalf of the state in *Smith*, has said that he believes modern applications of *Smith* go far beyond what he argued for in 1979.[76] With new technologies emerging, like the Amazon Echo and Google Home, which record conversation within the home, people risk inviting the government into their homes and giving it a front-row seat to their most intimate conversations.[77]

In terms of the sheer amount of personal data and information that is now mediated through third parties, the current third party doctrine regime is untenable. "Whatever its merits in the 1970s, this doctrine makes little sense in the modern world, in which almost all digital communications are sent through third parties and enormous amounts of personal data are stored by third parties."[78] Furthermore, the types of information turned over, like historical location data, emails, and internet browsing history, are far more complex and detailed than simple phone numbers.[79] Such information also comprises a larger proportion of our personal information: "We are becoming a society of records, and these records are not held by us, but by third parties."[80] With the emergence of smart home devices, the most intimate of data is on the line.

Moreover, we have diminishing meaningful choice when it comes to "voluntarily" turning over this data. It has become increasingly difficult to opt out of providing such kinds of data in the Information Age because "[w]e must 'plug in' to join in. . . . [W]e must establish rela-

---

[74] *See* Kerr, *supra* note 10, at 563.

[75] *See* Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 585 (2011); *see also* Kerr, *supra* note 10, at 563 n.5 (collecting sources).

[76] *All Things Considered: 1979 Supreme Court Ruling Becomes Focus of NSA Tactics*, NPR (Dec. 21, 2013, 5:13 PM), http://www.npr.org/2013/12/21/256114227/1979-supreme-court-ruling-becomes-focus-of-nsa-tactics [https://perma.cc/5775-KRBW] ("The current situation is really a far cry from the world in 1979. . . . The massive intrusion now is world's [sic] apart from what we argued in 1979. . . . I don't even like the notion that this is part of my legacy.").

[77] Recent revelations from WikiLeaks make clear that the CIA already has the capacity to listen in to private homes by hacking into computers and internet-connected televisions. *See* Scott Shane et al., *WikiLeaks Releases Trove of Alleged C.I.A. Hacking Documents*, N.Y. TIMES (Mar. 7, 2017), https://www.nytimes.com/2017/03/07/world/europe/wikileaks-cia-hacking.html [https://perma.cc/VAW3-RU7M].

[78] Ric Simmons, *The Missed Opportunities of* Riley v. California, 12 OHIO ST. J. CRIM. L. 253, 258 (2014).

[79] *See* Solove, *supra* note 4, at 1092–93.

[80] *Id.* at 1089.

tionships with a panoply of companies."[81] This notion also touches on another critique of the third party doctrine — that the assumption of risk rationale of *Smith* rests on a false premise that individuals truly have a choice in whether to participate in such activities — giving Justice Marshall's *Smith* dissent renewed salience in the digital age. Recall that the cases upon which *Smith* is based (and *Smith* itself) relied on the voluntariness of the particular disclosures at hand.

B. Cracks in the Foundation

Though courts periodically declined to extend *Smith* before *Jones*,[82] after *Jones*, "the drumbeat of [commentator] criticism has intensified,"[83] and "state and federal courts have increasingly rejected the government's attempts to extend *Smith* to new forms of data."[84] For example, in *United States v. Graham*,[85] the Fourth Circuit held that warrantless, extended collection of the defendants' cell site data was an unconstitutional search,[86] though this holding was later reversed en banc.[87] In *United States v. Davis*,[88] the Eleventh Circuit found that there is a reasonable expectation of privacy in "even one point of cell site location data,"[89] though the holding was later vacated en banc as well.[90] Further, eleven state supreme courts have explicitly rejected the third party doctrine, and ten others have indicated a possibility of doing so in the future.[91] Though both major federal opinions in this regard were reversed en banc due to their rejection of the still-binding *Smith* precedent, they demonstrate an inclination on the part of these courts to take a more contextual approach when the third party doctrine implicates novel technologies. For example, the *Graham* court noted that the *Smith* Court itself had conducted a context-based *Katz*

---

[81] *Id.*

[82] *See, e.g.*, United States v. Warshak, 631 F.3d 266 (6th Cir. 2010) (reasonable expectation of privacy in emails stored with internet service provider); *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317 (3d Cir. 2010) (declining to apply *Smith* to cell site location information since cell phone customers don't "voluntarily" share that information).

[83] Tokson, *supra* note 75, at 585.

[84] Hanni Fakhoury, Smith v. Maryland *Turns 35, but Its Health Is Declining*, ELEC. FRONTIER FOUND. (June 24, 2014), https://www.eff.org/deeplinks/2014/06/smith-v-maryland-turns-35-its-healths-declining [https://perma.cc/Z79N-QBSN]; *see* Lucas Issacharoff & Kyle Wirshba, *Restoring Reason to the Third Party Doctrine*, 100 MINN. L. REV. 985, 992 (2016).

[85] 796 F.3d 332 (4th Cir. 2015), *rev'd en banc*, 824 F.3d 421 (4th Cir. 2016).

[86] *Id.* at 360–61.

[87] *Graham*, 824 F.3d at 424.

[88] 754 F.3d 1205 (11th Cir. 2014), *rev'd en banc*, 785 F.3d 498 (11th Cir. 2015).

[89] *Id.* at 1216.

[90] *See Davis*, 785 F.3d at 500, 507–09 (relying on strict application of *Smith*).

[91] *See* Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373, 376, 395–405 tbls.1, 2 & 3 (2006).

analysis.[92] However, their reversal indicates that the Supreme Court will have to be the first to reimagine the third party doctrine (and perhaps validate a more conceptual approach) before lower courts are able to do so.

C. Riley v. California

Enter *Riley v. California*.[93] In *Riley*, the Supreme Court unanimously held that the warrantless search of an arrestee's cell phone was not a reasonable search, as it did not fall within the incident-to-arrest exception of the Fourth Amendment.[94] In so holding, the Court highlighted that cell phones are distinct from other physical objects that typically fall within the search-incident-to-arrest domain.[95] The Court examined and explicitly differentiated several precedents that govern such searches and their application to the case at hand, including *United States v. Robinson*.[96] In declining to extend the holding in *Robinson* — which deemed arrestees' privacy interests significantly diminished by the arrest itself[97] — to searches of cell phones,[98] it noted that "neither of [*Robinson*'s] rationales has much force with respect to digital content on cellphones."[99] The Court emphasized that "[cell] phones are based on technology nearly inconceivable just a few decades ago, when . . . *Robinson* w[as] decided."[100] The Court differentiated *Robinson* on the grounds that cell phones implicate greater privacy concerns than those implicated by the ordinary objects envisaged in *Robinson* (like wallets, purses, cigarette packs, and so forth).[101]

In distinguishing cell phones from ordinary physical objects that can be searched incident to arrest without a warrant, the Court primarily focused on the quantitative and qualitative aspects that differentiate cell phones.[102] In terms of quantitative differences, the Court underscored the enormous storage capacity of cell phones; the fact that cell phones can store so much personal information transforms what was once a minor search into a much more intrusive one.[103] Beyond sheer data capacity, the Court also noted that cell phones can store

---

92 United States v. Graham, 796 F.3d 332, 352–53 (4th Cir. 2015), *rev'd en banc*, 824 F.3d 421 (4th Cir. 2016).

93 134 S. Ct. 2473 (2014).

94 *Id.* at 2493.

95 *Id.* at 2491–93.

96 414 U.S. 218 (1973).

97 *See id.* at 235.

98 *Riley*, 134 S. Ct. at 2485.

99 *Id.* at 2484.

100 *Id.*

101 *Id.* at 2488–89.

102 *See id.* at 2489–91.

103 *Id.* at 2489.

many different *types* of information — including calendars, internet browsing history, text messages, detailed location history, photos, personal apps, and so on — which, taken together, can offer a rather comprehensive portrait of someone's private life.[104] The Court also rejected the United States' contention that an officer should be able to search an arrestee's call log; the United States had based its argument on *Smith*. The Court differentiated *Smith* on the grounds that cell phone call logs contain more detailed information than just phone numbers.[105]

D. Riley*'s Implications for the Third Party Doctrine*

To some, *Riley* seemed like the long-awaited update the Court's Fourth Amendment jurisprudence had desperately needed. It was praised as bringing the Court into "the digital age and fundamentally chang[ing] how the Constitution protects our privacy."[106] However, it is important to remember that while its language may be somewhat sweeping, the holding of the opinion is relatively narrow. Likely anticipating the potentially far-reaching consequences of its language, the Court expressly limited its holding to searches incident to arrest by noting that its decision "do[es] not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances."[107] Regardless, the language of *Riley* touches on the above concerns about the third party doctrine in a way that is hard to ignore.

First, Chief Justice Roberts grounded his discussion of *Robinson*'s inapplicability by pointing out the span of time that had elapsed between the opinions and the intervening change in the technological landscape.[108] Courts that have declined to strictly apply *Smith* have also used similar language and framing.[109] Furthermore, Chief Justice Roberts's exposition of the qualitative and quantitative differences of cell phone data that implicate arrestees' privacy interests could also be read to implicate the third party doctrine. Though the Court in *Riley* did not conduct a *Katz* reasonable expectation of privacy inquiry, its

---

104 *See id.* at 2489–90.

105 *See id.* at 2492–93.

106 *How the Supreme Court Changed America This Year*, POLITICO MAG. (July 1, 2014), http://www.politico.com/magazine/story/2014/07/how-the-supreme-court-changed-america-this-year-108497?o=2 [https://perma.cc/DC9A-7HSJ] (comments of Professor Stephen Vladeck).

107 *Riley*, 134 S. Ct. at 2489 n.1.

108 *Id.* at 2484.

109 *See, e.g.*, Klayman v. Obama, 957 F. Supp. 2d 1, 37 (D.D.C. 2013), *vacated*, 800 F.3d 559 (D.C. Cir. 2015) ("[T]he *Smith* pen register and the ongoing NSA Bulk Telephony Metadata Program have so many significant distinctions between them that I cannot possibly navigate these uncharted Fourth Amendment waters using as my North Star a case that predates the rise of cell phones.").

reasoning was based on balancing "the degree to which [a search] intrudes upon an individual's privacy" and government interests.[110]

While *Riley* did not explicitly address reasonable expectations of privacy, its underlying intuitions are quite similar. Again, its language is reminiscent of the criticisms leveled against modern applications of *Smith*. For example, one could analogize the Court's emphasis on the "immense storage capacity"[111] of cell phones to *Smith* critics' discomfort with the ever-growing amount and kinds of information shared with third parties.[112] Also, the Court's discussion of the "pervasiveness" of cell phones[113] further implicates *Smith* criticisms that highlight the growing extent to which detailed personal information must be shared with third parties to participate in modern life.[114] Furthermore "[t]he Court's analysis of the *qualitative* differences with data implies . . . that certain types of information are deserving of special protection."[115] Again, the Court's contention that the capability of cell phones to amass many different *types* of information implicates heightened privacy interests is suggestive of the concern that the third party doctrine increasingly captures types of information it was not meant to.

Perhaps most telling of the connection between *Riley* and the reasonable expectation of privacy framework is the Court's reasoning in denying the Government's argument that it should be able to search arrestees' call logs. The Government relied on *Smith* for this proposition, but the Court differentiated *Smith* by saying that "call logs typically contain more than just phone numbers; they include any identifying information that an individual might add."[116] The Court's reasoning implies that different (more informative) kinds of information should be entitled to greater Fourth Amendment protection than that granted in *Smith*, as they implicate greater privacy concerns.

Lastly, the Court in *Riley* used language very similar to that of *Maynard* and Justice Sotomayor's exposition of the mosaic theory in her *Jones* concurrence (which the Court in fact cited[117]) when discussing the kinds of detailed, personal information cell phone data could

---

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

111 *Id.* at 2489.

112 *See supra* section III.A, pp. 1933–34.

113 *Riley*, 134 S. Ct. at 2490.

114 *See supra* section III.A, pp. 1933–34.

115 Marc Rotenberg & Alan Butler, *Symposium: In* Riley v. California*, a Unanimous Supreme Court Sets Out Fourth Amendment for Digital Age*, SCOTUSBLOG (June 26, 2014, 6:07 PM), http://www.scotusblog.com/2014/06/symposium-in-riley-v-california-a-unanimous-supreme-court-sets-out-fourth-amendment-for-digital-age/ [https://perma.cc/9XCS-BCQB].

116 *Riley*, 134 S. Ct. at 2493.

117 *Id.* at 2490.

reveal in the aggregate.[118] Interestingly, in *Riley*, it is in this discussion where the footnote disclaiming any direct application to the third party doctrine is found.[119]

IV. A WAY FORWARD: A "SMART HOME" CASE STUDY INTO HOW THE THIRD PARTY DOCTRINE CAN (AND MUST) BE BROUGHT INTO THE TWENTY-FIRST CENTURY

So where does this leave us? While some contend that *Riley* "takes clear aim" at the third party doctrine,[120] others are not so sure.[121] Courts also seem to have taken notice of *Riley*'s implications for the doctrine. For example, in her dissenting opinion in *Davis*, Judge Martin underscored *Riley* to support her contention that the court should not have mechanically applied *Smith* in light of extraordinary technological advances.[122]

A. The Third Party Doctrine is Here to Stay . . . for Now

The sweeping language of *Riley* likely indicates a willingness on the part of the Court to reimagine the doctrine in the near future — though not abandon it completely. Several factors demonstrate this unwillingness to abandon the doctrine. First, the Court disclaimed *Smith* implications in *Riley*.[123] Also, the Court has passed up opportunities to directly address the doctrine before.[124] Regardless of its inclination concerning the doctrine, the Court will not have to decide the issue until a relevant case is before it. Aside from the *Jones* concurrence, the fact that lower courts show increased willingness to substitute the doctrine's current binary application with a more contextual approach (though such opinions have been later reversed on stare decisis grounds),[125] along with the exponential proliferation of technology that necessitates third-party information sharing for daily life, underscores the necessity of a rethinking of the doctrine by the Court. The smart home context represents an area that is especially problematic and presents an ideal opportunity to do so.

---

118 *See id.* at 2489–90.

119 *Id.* at 2489 n.1.

120 Rotenberg & Butler, *supra* note 115.

121 *See How the Supreme Court Changed America This Year*, POLITICO MAG. (July 1, 2014), http://www.politico.com/magazine/story/2014/07/how-the-supreme-court-changed-america-this-year-108497?o=2 [https://perma.cc/DC9A-7HSJ] (comments of Professor Barry Friedman).

122 *See* United States v. Davis, 785 F.3d 498, 537–38 (11th Cir. 2015) (Martin, J., dissenting).

123 *See Riley*, 134 S. Ct. at 2489 n.1, 2492–93.

124 *See* Simmons, *supra* note 78, at 265–66.

125 *See supra* section III.B, pp. 1934–35.

B. Smart Homes and the Third Party Doctrine

1. What is a Smart Home? — The emergence of home automation — otherwise known as the smart home — is a natural step in the rapid growth of the "Internet of Things" — the proliferation of everyday products that connect to the internet.[126] Unsurprisingly, the rise of the Internet of Things has alarmed many privacy and security advocates, as hackers could be privy to — and possibly gain control of — the information gathered by an ever-ballooning array of devices, from vehicles to appliances to pacemakers.[127] This alarm is magnified in the smart home context, as the data to be protected is of a much more personal and sensitive nature. Especially alarming is the fact that this information is disseminated across a multitude of third parties.[128]

Smart home devices, and the technology that supports them, have experienced a boom in popularity over the past couple years.[129] For the purposes of this discussion, I will focus on two types of smart home technologies: voice assistants and video security. Voice assistants like the Amazon Echo or Google Home act as smart home "hubs," from which one can control lighting and temperature, conduct internet searches, and order groceries, among other things, all by using only one's voice.[130] Smart security cameras, like the Nest Cam, "begin recording and transmitting audio [and video] when turned on, and are designed to continue recording and transmitting data 100% of the time or until manually turned off."[131] The user can then remotely watch a live stream of the security footage from an application on their mobile device and may purchase longer-term cloud-based video storage.[132]

2. Third Party Doctrine Implications. — Whenever you make a voice request, your voice assistant device wakes up and records your

---

[126] *See* Bill Wasik, *In the Programmable World, All Our Objects Will Act as One*, WIRED (May 14, 2013, 6:30 AM), https://www.wired.com/2013/05/internet-of-things-2 [https://perma.cc/2XJC-ULY4].

[127] Andreas Jacobsson, *IoT, Security and Privacy*, MEDIUM (June 14, 2016), https://medium.com/@iotap/internet-of-things-security-and-privacy-78bc0a41881b [https://perma.cc/EW83-CXK8]; Wasik, *supra* note 126.

[128] *See* Jacobsson, *supra* note 127.

[129] Ry Crist, *Home Automation Buying Guide*, CNET (Mar. 3, 2015, 3:33 PM), https://www.cnet.com/news/smart-home-buying-guide-home-automation/ [https://perma.cc/7TTN-P33Q].

[130] *See* Rich Jaroslovsky, *Google Home vs. Amazon Echo Is a Battle of Smarts and Skills*, OBSERVER (Jan. 17, 2017, 7:00 AM), http://observer.com/2017/01/google-home-versus-amazon-echo-review/ [https://perma.cc/KGM7-4VE3].

[131] STACEY GRAY, FUTURE OF PRIVACY FORUM, ALWAYS ON: PRIVACY IMPLICATIONS OF MICROPHONE-ENABLED DEVICES 6 (2016) (emphasis omitted), https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf [https://perma.cc/W3SR-SNXB].

[132] Brian Barrett, *Nest Cam Outdoor Fixes the Security Camera's Biggest Fault,* WIRED (July 14, 2016, 2:06 PM), https://www.wired.com/2016/07/nest-cam-outdoor [https://perma.cc/S6AN-S2NQ].

utterance and transmits that recording file to its home base (be that a server run by Amazon, Google, or others) to process your request. For this function to work, each product needs a specific "wake word" (for the Amazon Echo, that's "Alexa") so it knows when to begin recording.[133] Otherwise, even though it is always listening, it is constantly overwriting any background chatter it may hear.[134] Recorded utterances and requests are stored on that respective company's servers and associated with the user's account, so as to enable the device to better recognize a user's voice or speech patterns and respond to commands more seamlessly.[135] This data is stored unless the user deletes it. Microsoft's Cortana assistant takes it a bit further and is always listening (and includes cloud storage of data).[136]

The third party doctrine implications here should be somewhat self-evident by this point. The Echo and devices like it offer law enforcement a window into your home. It is not hard to argue that Echo users voluntarily conveyed this information to a third party. The concerns expressed in *Riley* and Justice Sotomayor's *Jones* concurrence are also reflected — if not magnified — in this context. First, this technology was inconceivable at the time of *Smith* and its antecedents. Second, echoing Chief Justice Roberts's critique in *Riley*, this information is light years beyond the types and amounts of information being shared during the time of *Smith* and *Miller*, both quantitatively and qualitatively speaking. "With dozens of daily interactions recorded in the app's history it grows to quite an archive . . . ."[137] Use of this device can allow companies like Amazon to create a comprehensive profile of the user and her activities, including — but not limited to — her health profile (health monitoring apps), whereabouts (calendar), activities (to-do lists), political leanings (which news sites she frequents), and even possibly her innermost thoughts (think of the one-off Google or WebMD searches you would prefer not to broadcast). One Echo user muses that "[a] few days after my wife and I discussed ba-

---

133 Richard Baguley & Colin McDonald, *Appliance Science: Alexa, How Does Alexa Work? The Science of the Amazon Echo*, CNET (Aug. 4, 2016, 5:00 AM), https://www.cnet.com/news/appliance-science-alexa-how-does-alexa-work-the-science-of-amazons-echo/ [https://perma.cc/TFS2-FNW3].

134 Christopher Mele, *Bid for Access to Amazon Echo Audio in Murder Case Raises Privacy Concerns*, N.Y. TIMES (Dec. 28, 2016), https://www.nytimes.com/2016/12/28/business/amazon-echo-murder-case-arkansas.html [https://perma.cc/5J7L-TK35].

135 Joseph Jerome, *Alexa, Is Law Enforcement Listening?*, CDT (Jan. 4, 2017), https://cdt.org/blog/alexa-is-law-enforcement-listening/ [https://perma.cc/F3X5-ZFCH].

136 Michael Justin Allen Sexton, *Cortana Is Listening*, TOM'S HARDWARE (Aug. 10, 2015, 2:00 PM), http://www.tomshardware.com/news/cortana-is-watching,29791.html [https://perma.cc/P65D-FETG].

137 Rory Carroll, *Goodbye Privacy, Hello "Alexa": Amazon Echo, the Home Robot Who Hears it All*, THE GUARDIAN (Feb. 21, 2017, 12:42 PM), https://www.theguardian.com/technology/2015/nov/21/amazon-echo-alexa-home-robot-privacy-cloud [https://perma.cc/VM8A-CYUD].

bies, my Kindle showed an advertisement for Seventh Generation diapers."[138] It is important to recall that the *Smith* Court stressed the contentless nature of the information collected by pen registers in holding there was no reasonable expectation of privacy.[139]

This thought exercise is not pure conjecture. Law enforcement has already tried to obtain Echo recordings from Amazon. In late 2015, a police department issued a warrant to Amazon for Echo audio recordings to facilitate a murder investigation; the Echo was located at the home where the victim's body was found.[140] "This appears to be a first-of-its-kind case and we are sure to see many more of these types of inquiries in the future."[141] While Amazon staunchly refused to turn over the data here, that may not always be the case.[142] It is also important to note that, had the police been able to obtain the information without a warrant, that likely would not have constituted a search under the third party doctrine as it stands.[143] In this vein, police did not need a warrant to obtain evidence of the suspect's water usage — which turned out to be pivotal — from his utility company as recorded by his smart water meter.[144]

Similar concerns apply in the smart-security-camera context. The innovation of smart security cameras is that they can stream live footage of your home (via an app) to a mobile device. They also offer the option to store footage on the cloud for a certain period of time. One of the Echo's saving graces, at least from a consumer privacy standpoint, is that it is not continuously recording (and relaying this information to Amazon). By contrast, smart security cameras have to constantly record in order to perform their function. It goes without saying that this state of affairs takes the above *Riley* considerations and magnifies them by orders of magnitude. Now, you don't just have voice snippets. You have a high-fidelity audiovisual feed of the inside of someone's home. This technology renders the mosaic theory redundant: why piece together a mosaic when you can have a high-resolution 3D image delivered? One could argue that users could just opt out of cloud storage, but one primary feature of having a security camera system is being able to review recorded footage at a later time, and local data storage is becoming less and less common as companies

---

138 *Id.*

139 *See supra* text accompanying notes 43–45.

140 Mele, *supra* note 134.

141 Sarah Buhr, *An Amazon Echo May Be the Key to Solving a Murder Case*, TECHCRUNCH (Dec. 27, 2016), https://techcrunch.com/2016/12/27/an-amazon-echo-may-be-the-key-to-solving-a-murder-case/ [https://perma.cc/LJ4L-A9EU].

142 *See* Jerome, *supra* note 135.

143 *See id.*

144 *See* Buhr, *supra* note 141; Jerome, *supra* note 135. *See generally* Duarte, *supra* note 9 (analyzing smart meter use and implications).

like Apple increasingly nudge users toward use of the cloud.[145] Use of Apple's new Home app, which serves as a smart home control hub and is automatically included on mobile devices running iOS 10, also requires the use of iCloud.[146]

C. Back to Basics: Katz *and* Smith *as a Way Forward*

The foregoing case study of smart homes in a post-*Riley* world where the third party doctrine still persists is not meant to serve as a mere parade of horribles. Rather, it is useful in two respects: First, it puts the increasingly untenable stature of the present binary interpretation of *Smith* into stark relief. Second, it demonstrates a confluence of factors that may be impossible for the Court to ignore, forcing it to bring the third party doctrine into the twenty-first century.

1. The Home. — Under Fourth Amendment jurisprudence, the home has always reigned supreme. The Supreme Court has repeatedly underscored this fact. As recently as 2013, Justice Scalia noted, "when it comes to the Fourth Amendment, the home is first among equals. At the Amendment's 'very core' stands 'the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'"[147] Increased attention paid to more *Katz*-like conceptions of privacy as tied to the individual has not compromised the primacy of the home in the Court's eyes.

The natural question, then, is what is the Court to make of the smart home? Not only are the *Riley* concerns directly implicated (and magnified) in this context, but the inner sanctum of the home, bit by bit, has also been voluntarily conveyed to third parties. This state of affairs seems like the zenith of the conflict between the third party doctrine and the digital age. Given the foregoing discussions of *Riley* and the seeming willingness of the Court to apply more contextual privacy analyses here, it is unlikely that, when confronted with such a case, the Court would apply the simplistic third party doctrine binary and move on.

That is not to say that the Court would revert to a pre-*Katz* property binary in its stead by holding that smart homes, as opposed to other modern technologies, are deserving of exemption from the third party doctrine because of the special status of the home. The *Katz* opinion itself, while recognizing expectations of privacy within the

---

[145] *See* Ryan Watzel, Riley*'s Implications for Fourth Amendment Protection in the Cloud*, 124 YALE L.J.F. 73, 78 (2014).

[146] Jeff Benjamin, *iOS 10: How to Use the New Home App to Control HomeKit Devices*, 9TO5MAC (Sept. 23, 2016, 3:22 PM), https://9to5mac.com/2016/09/23/ios-10-how-to-use-new-home-app-control-homekit-devices-video/ [https://perma.cc/4U5T-QDE2].

[147] Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013) (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)).

home as reasonable, explicitly provided for an exception for things "knowingly expose[d]" to the outside world.[148] Therefore, using the home aspect of smart homes as the doctrinal solution here gets us into some murky territory.

The merit of the "home" angle in this context is not its usefulness as a potential doctrinal hook for the Court. Rather, it takes the third party doctrine concerns the Court has already expressed, magnifies them, and applies them to an area the Court is most willing to protect. This juxtaposition arranges a constellation of factors in a way that would be hard for the Court to overlook. It may very well be the catalyst that finally pushes the Court to directly confront the increasingly untenable third party doctrine. That said, we still need an account of how it could go about doing that.

2. One Step Backward, Two Steps Forward. — It is interesting to note that *Katz*, and by extension *Smith*, came out of a needed response to shifting technology and social norms.[149] Fortunately, if the Court did wish to update the third party doctrine accordingly, it would not have to look further than its own precedent in *Smith*, and by extension *Katz*. In doing so, the Court can undo the slow calcification of the disclosure binary that took place from *Katz* to *Smith* and beyond.

Understanding how precedent may enable a path forward requires recalling that the *Smith* Court still applied the two-pronged *Katz* reasonable expectation of privacy test to a particular set of facts. As the Fourth Circuit has noted: "[W]hether an individual has a reasonable expectation of privacy . . . is '[t]he "touchstone" of Fourth Amendment analysis[.]' . . . [T]he third-party doctrine was not devised to side-step this question . . . ."[150] This decision was subsequently vacated for its refusal to apply the *Smith* binary as understood, further underscoring the fact that the Supreme Court will have to be the one to propose a new framework for the third party doctrine.[151]

In reexamining the third party doctrine, it will be important to trace the doctrinal underpinnings of *Smith*. Upon further examination, it becomes clearer that the current binary conception of the third party doctrine was cobbled together from a line of cases that took differing aspects of personal privacy into account and applied them to specific circumstances. "*Katz* was supposed to restore the equilibrium between the individual and his government that had existed . . . .

---

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

149 *See supra* text accompanying notes 23–25.

150 United States v. Graham, 796 F.3d 332, 360 (4th Cir. 2015) (third and fourth alterations in original) (quoting United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010)), *rev'd en banc*, 824 F.3d 421 (4th Cir. 2016).

151 *Graham*, 824 F.3d at 437–38 (citing United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring)).

Ironically, *Katz* . . . has become the theoretical basis for ratifying the government's expanded ability to gather information about us."[152]

It is important to recall that the *Smith* Court itself applied the *Katz* test and explained why Smith's expectation of privacy was unreasonable, focusing on voluntariness of disclosure and nonsensitivity of the information.[153] In addition, it relied on *Miller* and other government informant cases for the contention that voluntary disclosure forfeited Fourth Amendment protection in that case.[154] Therefore, in keeping with the *Smith* opinion, the Court can (and should) apply the reasonable expectation of privacy test when evaluating whether the third party doctrine should apply to a particular situation. Doing so does not have to be especially burdensome either. As discussed, the Court's analysis of the reasonability of the privacy expectation proceeded along three main axes in the cases underlying the modern third party doctrine — the nature and sensitivity of the information conveyed; the voluntariness of the conveyance; and the identity of the third-party recipient. It is not clear why the Court should not be able to weigh such considerations again.

First, the cases upon which the modern third party doctrine has been built often focused on the content of the information shared.[155] It is difficult to imagine that the Court would have reached the same conclusion had the bank shared private letters from Miller's safe deposit box (or, say, security camera footage from inside his home). In both cases, the Court seems to be touching on the sensitivity of the information conferred to justify its conclusion that no reasonable expectation of privacy existed. It is worth noting that the Court in *Katz* specified that the content to be protected was "the words [a phone booth user] utters into the mouthpiece."[156] Lastly, even the *Smith* Court highlighted the lack of informational content and nonsensitivity of the phone numbers collected. In fact, it made a point to specify this fact at the beginning of its analysis and differentiate the situation at hand from *Katz* in that the phone call's content was not recorded.[157]

Furthermore, the assumption of risk rationale — upon which *Smith*, and the government informant cases on which it relied, are based — implicitly took into account the identity of the third party with whom information was shared. This misplaced confidence doc-

---

[152] Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-First Century*, 65 IND. L.J. 549, 563 (1990).

[153] *See supra* text accompanying notes 44–45.

[154] *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

[155] *See* United States v. Miller, 425 U.S. 435, 442–43 (1976); Couch v. United States, 409 U.S. 322, 335–36 (1973).

[156] *See* Katz v. United States, 389 U.S. 347, 352 (1967).

[157] *See Smith*, 442 U.S. at 741.

trine[158] makes sense in the context of interpersonal relations. Someone can never really know whether a personal confidant will relay her secrets. However, it's not clear the same can necessarily be said of the business institutions with which one interacts as a consumer. Recall that in *Miller*, the misplaced confidence doctrine would not have supported the Court's holding as well without their downplaying the sensitivity of the information conveyed.[159]

Therefore, it is important not only to look at (and blindly parrot) the holdings of these cases but also to apply their reasoning — especially when *Smith* and *Miller* were based on the very idea of contextual analysis. The innovation of *Katz*, upon which *Smith* was based, is lost if the reasonable expectation of privacy test is not applied to the specific facts of each case. Therefore, the Court, when examining cases that implicate the third party doctrine, can — and should — apply the *Katz* test in each instance. Moving forward, the Court is free to argue that the third party doctrine does not apply in certain contexts (for example, for types of information) where expectations of privacy are reasonable without overruling *Smith*, if it so wishes.

CONCLUSION

The third party doctrine has run its course and risks swallowing the Fourth Amendment whole. As the sharing of information becomes increasingly necessary to participate in modern life, and as such technologies creep into our homes, Fourth Amendment protection should not be held hostage by an outdated binary rule fashioned during the time of phone booths and pen registers. Furthermore, one should not be forced to make the choice to either participate in modern life or maintain complete secrecy of one's information in order to attain Fourth Amendment protection. This state of affairs becomes even more absurd if one considers the fact that the third party doctrine arose from opinions in which the Court had conducted fact-sensitive inquiries as to the reasonability of the privacy expectation at hand. It is difficult to imagine that the *Smith* Court would countenance the modern applications of the third party doctrine seen in *Graham* and *Davis*. Will the Court be so willing to stick to the third party doctrine as articulated and in effect remove Fourth Amendment protection from activity inside the home? The Court ought to take advantage of the opportunities this period of rapid technological change is sure to offer to faithfully apply its own precedent and return to a context-dependent privacy inquiry, restoring the proper equilibrium between individual privacy and warrantless surveillance.

---

158 *See supra* text accompanying notes 26–28.

159 *See supra* text accompanying notes 35–36.