Overturn the Third Party Doctrine

Faiz Surani

In early 2003, a man marched into a Target outside Minneapolis and demanded to speak to the manager. Why, he fumed, was Target sending his high school-aged daughter advertisements for maternity clothing and cribs? "Are you trying to encourage her to get pregnant?!"

Several days later, a rather more apologetic father called the store back. "I had a talk with my daughter. It turns out there's been some activities in my house I haven't been completely aware of. She's due in August."[1]

Awkward familial situation aside, this was not mere happenstance. The ads Target sent the man's daughter were the result of a concerted effort by the retail giant's statisticians to identify pregnant women based on purchasing patterns and cultivate them as loyal customers. Since 2003, tracking of consumer behavior has only grown vastly more sophisticated, and the explosion of the internet advertising industry has created entirely new methods to collect and analyze an individual's habits and choices. At the same time, the advent of cloud computing has led to the rise of popular consumer services like Google Drive, iCloud, and Dropbox where users store their photos, documents, and diaries among other sensitive data. Today, one thing is certain: we live our lives online.

Yet, the Supreme Court has thus far failed to reckon with this fact in its Fourth Amendment jurisprudence, holding that nearly all of the abovementioned data can be searched by the government without a warrant. Termed the "third-party doctrine," this approach was adopted by the Court in a pair of cases in the 1970's and has subsisted to the present day.[2] Whatever the doctrine's merits at time of establishment, its assertion that people have no

[1] Charles Duhigg, *How Companies Learn Your Secrets*, The New York Times (Feb. 16, 2012).

[2] *Smith v. Maryland*, 442 U.S. 735 (1979); *United States v. Miller*, 425 U.S. 435 (1976).

expectation of privacy to data held by a third party is fundamentally inapt for our modern age. To preserve the promise of the Fourth Amendment, the Court ought to set aside the principle and rebuild its search and seizure doctrine with modern expectations of privacy in mind.

The Fourth Amendment states: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[3] For nearly two centuries after the passage of the Bill of Rights, Fourth Amendment protections were largely limited to trespasses; that is, the government could not unreasonably search "[a] person…, his papers or tangible material effects ' ' or "physical[ly] inva[de]… his house for the purpose of making a seizure."[4]

Then came *Katz*. Concerning the wiretap of a public phone booth, *Katz v. United States* (1967) fundamentally reshaped Fourth Amendment jurisprudence. Writing for the majority, Justice Potter Stewart boldly declared that "the Fourth Amendment protects people, not places," thus overruling precedent that had limited the Fourth Amendment's reach to certain "constitutionally protected areas."[5] This alone was significant, but *Katz*'s enduring legacy stems from Justice John Marshall Harlan's concurring opinion, which put forward for the first time the "reasonable expectation of privacy" test.[6] Justice Harlan's proposed test had two requirements for Fourth Amendment protection: "first, that a person has exhibited an actual (subjective) expectation of privacy and, second, that expectation [is] one that society is prepared to recognize as reasonable.' "[7] In the years to come, the Court would formally codify Justice Harlan's test as the principal governing authority of Fourth Amendment law, dramatically expanding the scope of privacy protection in the United States.

[3] Fourth Amendment, U.S. Const. amend. IV.
[4] *Olmstead v. United States*, 277 U.S. 438, 466 (1928).
[5] *Katz v. United States*, 389 U.S. 347, 351 (1967).
[6] *Id.* at 360 (Harlan, J., concurring).
[7] *Id.* at 360 (Harlan, J., concurring) (internal quotations omitted).

Which takes us to the third-party doctrine. About a decade after *Katz*, the Court laid out the theory in a pair of cases: *United States v. Miller* (1976)[8] and *Smith v. Maryland* (1979).[9] The first case, *Miller*, concerned a defendant's financial records that were acquired from several banks with a grand jury subpoena, not a warrant. The second case, *Smith*, concerned warrantless police use of pen registers, electronic devices installed on telephone lines to record dialed numbers. In both cases, the defendant challenged their convictions on the grounds that the police's actions constituted an illegal search and seizure under the Fourth Amendment. And in both cases, the Supreme Court rejected those challenges out of hand. The *Miller* majority found "no legitimate expectation of privacy in… information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[10] In *Smith*, the Court found that the defendant "assumed the risk that the [phone] company would reveal to police the numbers he dialed… when he voluntarily conveyed that information to the company's equipment."[11] Combined, the two cases established a rigid rule of thumb: people do not possess a legitimate expectation of privacy under *Katz* to any data they provide to third parties.

In the era of the Internet, *Smith* and *Miller* have come to rest on a false premise: that one "voluntarily" provides their private information to a third party in any meaningful sense of the word. Sure, a person can choose to shun modern society altogether. They could refuse to open a bank account or use the Internet, and live off the grid altogether to avoid ever handing over personal information to another. But mostly we call that guy Unabomber, and understand that refusing to engage with society at large is not really a reasonable price to pay for one's right to privacy. As Justice Sotomayor noted in her 2012 concurring opinion in *United States v. Jones*, "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers they dial or

[8] 425 U.S. 435 (1976).
[9] 442 U.S. 735 (1979).
[10] *United States v. Miller*, 425 U.S. 435, 442 (1976).
[11] *Smith v. Maryland*, 442 U.S. 735, 744 (1979).

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."[12] It is frankly unreasonable for the Court to say that individuals have no expectation of privacy in any of these sensitive areas.

Even presuming that people willingly participate in this alleged privacy-for-convenience bargain, *Smith* and *Miller* run headlong into yet another fallacy: the idea that by doing so, people "assume the risk" that that data will be turned over by the third party to the police[13] Perhaps we are aware of the possibility that our data could be handed off to anyone else. But an assumption of risk does not follow from that awareness. We don't assume the risk of being hit by falling debris when we walk by a construction site, even though we are vaguely aware of the possibility. Knowing that our constitutional rights may be violated does not mean we acquiesce to that violation, and assumption of risk doctrine is little more than a walking, talking civil liberties violation.

Now, tech behemoths like Apple and Google have typically required warrants of law enforcement before turning over sensitive user data like browsing history or files stored in their respective cloud services.[14] But these companies have implemented such requirements of their own accord, and not because of federal law, which explicitly permits warrantless searches of cloud data with few exceptions.[15] This is not a tenable situation. The honor system is not an adequate substitute for constitutionally protected rights. Even assuming these companies always act in the best interests of their users (fact check: false), there is frighteningly little standing in the way of a legislative body that seeks to compel the provision of data from these companies without a warrant.[16]

---

[12] *United States v. Jones*, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

[13] *Smith*, 442 U.S. 744.

[14] David Kravetz, *Google Tells Cops to Get Warrants for User E-Mail, Cloud Data*, Wired (Jan. 23, 2013).

[15] *Id.*

[16] Steven J. Arango, *The Third-Party Doctrine in the Wake of a "Seismic Shift"*, American

So, if the third-party doctrine is broken, how do we fix it? Can we fix it? How do we protect privacy in the modern era while ensuring law enforcement agencies can perform their duty to keep Americans safe? As I see it, there are a few options.

The first approach is that of the Court in the 2018 case *Carpenter v. United States*.[17] The case concerned the FBI's warrantless use of historical cell site location information (CSLI), metadata stored by cell service providers that effectively allows for a detailed cataloguing of a cell phone's location. There, the majority found that use of historical CSLI did constitute a Fourth Amendment search, because "individuals have a reasonable expectation of privacy in the whole of their physical movements."[18] As such, the Court "decline[d] to extend *Smith* and *Miller*" to historical CSLI, finding that "the unique nature of cell phone location records" outweighed "the fact that the information [was] held by a third party."[19]

Even as a majority of the Court finally recognized that the third-party doctrine was not beyond reproach, it carefully circumscribed its own holding to the specific concerns presented by historical CSLI data and reaffirmed the core holdings of *Smith* and *Miller*. Ultimately, the *Carpenter* majority failed to muster either a compelling defense or repudiation of the theory. Instead, it layered on top of *Smith* and *Miller* another balancing test that might best be described as the "extra super-duper private doctrine," whereby some pieces of information are so sensitive that they demand elevation above even the typically uncompromising *Smith* standard. As Justice Gorsuch correctly noted in his dissent, the majority likely created more problems than they solved: "All we know is that historical cell-site location information (for seven days, anyway) escapes *Smith* and *Miller*'s shorn grasp, while a lifetime of bank or phone records does not. As to any other kind of information, lower courts will have to stay tuned."[20] It seems, then, that *Carpenter*'s des-

Bar Association (June 13, 2019).

[17] 585 U.S. ___ No. 16-402 (2018).

[18] *Carpenter v. United States*, 585 U.S. ___ No. 16-402, slip op. at 12 (2018).

[19] *Id.* at 11.

[20] *Id.* slip. op at 12 (Gorsuch, J., dissenting).

perate attempt to save *Smith* and *Miller* will fail, like any attempt to reconcile the pair of cases with modern privacy expectations.

The next option is one posed by Justice Gorsuch in that same dissent: abandon *Katz* and its descendants altogether and start over from a property rights perspective. The justice's theory is premised on the idea that people own their own data much like their physical possessions and that "the fact that a third party has access to or possession of your papers and effects does not necessarily eliminate [their] interest in them."[21] Justice Gorsuch's proposal is well taken, and likely prudent policy even for reasons not pertaining to the 4th Amendment. Its proposition that a person's data is their "modern day papers and effects" has considerable textualist allure, too.[22]

Unfortunately, Justice Gorsuch's property rights approach suffers from the same flat footedness that ails Smith and Miller. Yes, it deals with cases like Carpenter quite elegantly. But when we excise *Katz*'s reasonable expectation test from Fourth Amendment law entirely, we find messier results once we muddy the waters a bit. Take the Target pregnancy predictor mentioned earlier. Could Target provide the government without a warrant a list of all the pregnant women it knew of, even if it derived that information from private individual data like browsing and shopping trends? Lest we get mired in even more esoteric debates about where a company's data ends and an individual's data begins, it seems unwise to go down this path of analysis.

That leaves us with one final approach: jettison *Smith* and *Miller*, and rework search and seizure doctrine from *Katz* on up to accurately reflect modern expectations of privacy. To be clear, *Katz* is by no means perfect. As many legal scholars have remarked, the "reasonable expectation" test is inherently somewhat circular.[23] Further, its imposition on judges to ascertain

[21] *Id.* at 14.

[22] *Id.* at 15.

[23] *See, e.g.*, Richard A. Posner, *The Uncertain Protection of Privacy by the Supreme Court*, 1979 Sup. Ct. Rev. 173 ("[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.").

the prevailing expectations of privacy in their society lends itself to the same amateur historical and sociological analysis that so often leads originalist thought astray.[24]

But *Katz* is well-suited to keeping with the moving target of evolving privacy norms. Free from the constriction of the third-party doctrine, the Court could determine the *kinds* of information subject to the warrant requirement, rather than being short-circuited in its analysis by the *medium*. It could establish an intellectually honest framework with which to distinguish, say, bank records from CSLI data, and uphold the Fourth Amendment's intent to prevent wanton government incursion upon private information. Many of the warrantless surveillance and collection methods used by law enforcement currently permitted by the third-party doctrine can and should continue to be legal, just on different grounds. That's precisely the point. In the long term, mothballing *Smith* and *Miller* will allow for a more consistent, coherent jurisprudence that better serves both governmental reliance interests and individual privacy.

As Winston Churchill once said of buildings, we shaped the Internet and thereafter the Internet has shaped us. It has fundamentally altered almost every aspect of our lives, from how we do business to how we find romantic partners. It has changed how we view our friends, our political opponents, and even ourselves. Perhaps the Internet will guide us towards a post-privacy era, one where people no longer expect anything but the thoughts in their head to be free from prying eyes. If that day comes, so be it. But it has not come. We still expect our data to be ours and not the property of some faceless server host. We still expect our closest-held secrets and thoughts to be free from unreasonable searches, regardless of the medium in which they exist. And we ought to expect the Court's Fourth Amendment doctrine to reflect those essential truths.

[24] *See* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 Stanford Law Review 503, 505 (2007) ("Among scholars, [the] state of affairs [surrounding the 'reasonable expectation of privacy' test] is widely considered an embarrassment. The Court's handiwork has been condemned as 'distressingly unmanageable,' 'unstable,' and 'a series of inconsistent and bizarre results that [the Court] has left entirely undefended.' ").