2020

App Permissions and the Third-Party Doctrine

Michael Gentithes

The University of Akron, gentithes@uakron.edu

Recommended Citation

Michael Gentithes, 59 Washburn L. J. 35 (2020)

APP PERMISSIONS AND THE THIRD-PARTY DOCTRINE

Michael Gentithes[*]

INTRODUCTION

Apple's trademarked catchphrase "there's an app for that"[1] suggests that every app on a modern digital device is perfectly tailored to provide a specific, necessary convenience. Whether the user wants to check the weather, get updates on her favorite baseball team, find a coupon for her next purchase, or track her fitness and activity levels, she can use an app to fill gaps in her life that she may not have known existed. What the user might also not know, however, is that "permissions" either she or the phone's operating system have granted to the app allow it to access functions and information on her device entirely unrelated to the app's apparently straightforward purpose. The app's developers might then package and sell information collected through those permissions to commercial partners,[2] or, as this Article considers, divulge it to government investigators.

In the spirit of Professor Tokson's effort to consider the next wave of Fourth Amendment cases likely to reach the Supreme Court,[3] this essay addresses a looming technological challenge to the Court's third-party doctrine: the permissions that app developers obtain on our digital devices. Such permissions—which are either granted by the user upon installation of the app or permitted by the operating system without any user input—entitle app developers to access and send data from the device, such as the user's location services, motion sensors, contacts, calendars, social media accounts, camera, or microphone.[4]

Carpenter contracted the third-party doctrine when government investigators collect location information *emitted by* a citizen's cell phone to

[*] Author's note.

[1] Doug Gross, *Apple Trademarks "There's an App for That"*, CNN.COM, http://www.cnn.com/2010/TECH/mobile/10/12/app.for.that/index.html, Oct. 12, 2010.

[2] According to Norman Sadeh, a professor in the School of Computer Science at Carnegie Mellon University, app developers are "basically bundling a bunch of decisions together and forcing users to make impossible decisions . . . The apps might need it for functionality, but it might also share it with marketers and advertisers alike." Lauren Goode, *App Permissions Don't Tell Us Nearly Enough About Our Apps*, WIRED.COM, https://www.wired.com/story/app-permissions/, April 14, 2018.

[3] Matthew Tokson, *The Next Wave of Fourth Amendment Challenges After* Carpenter, ADD CITE

[4] Lauren Goode, *App Permissions Don't Tell Us Nearly Enough About Our Apps*, WIRED.COM, https://www.wired.com/story/app-permissions/, April 14, 2018.

connect with towers in the nearby area.[5] This Article considers what that decision portends for information government investigators might *collect from* a citizen's cell phone and the apps that make it both enormously convenient and potentially intrusive upon personal privacy.

This Article proceeds in three Parts. Part I quickly summarizes the history and limits of the third-party doctrine following *Carpenter*. Part II then provides a technical explanation of apps and the permissions they obtain from users, including the scope of those permissions and their often tenuous relationship to the app's purpose. Part III suggests how courts should apply the third-party doctrine to data that app developers collect through wide-ranging permissions, which government investigators later obtain without a warrant.

I. THE FOURTH AMENDMENT AND THE THIRD-PARTY DOCTRINE

As Professor Tokson helpfully summarizes,[6] the Fourth Amendment's road to *Carpenter* contains unexpected twists and turns that have led to widespread confusion amongst courts and law enforcement officers in the modern digital era.

The Supreme Court has long struggled to define the Fourth Amendment's provision of citizens' right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures"[7] To determine what constitutes an "unreasonable search and seizure," the Court has constructed a number of analytical artifices atop the sparse text, the most important of which is the reasonable expectation of privacy test.[8] Though the Court's early definitions of a "search" emphasized the amendment's relationship to common-law trespass,[9] the Court's focus slowly transformed throughout the 20th century into its present-day emphasis on "people, not places."[10] In his dissent in *Olmstead v. United States*, Justice Brandeis highlighted that "every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth

[5] Carpenter v. United States, 585 U.S. ___ (2018) (slip. op. at 15).

[6] Matthew Tokson, *The Next Wave of Fourth Amendment Challenges After* Carpenter, ADD CITE

[7] U.S. CONST., amend IV.

[8] Katz v. United States, 389 U.S. 347, 350-51 (1967).

[9] United States v. Jones, 565 U.S. 400, 405 (2012). Cases such as *Olmstead v. United States* exemplified this trend, holding that taps attached to telephone wires in public streets did not run afoul of the Fourth Amendment simply because none of the material things mentioned in the amendment—a citizen's person, house, papers or effects—were intruded upon by the government's action. Olmstead v. United States, 277 U.S. 438, 463-64 (1928).

[10] Katz v. United States, 389 U.S. 347, 351 (1967).

Amendment."[11] Brandeis's views were partially formalized nearly forty years later in *Katz v. United States*, a case concerning an eavesdropping device attached to a public telephone booth.[12] In a concurrence that the Court has since applied to innumerable cases, Justice Harlan suggested that government conduct amounts to a search triggering the Amendment's protections when it intrudes upon a citizen's "constitutionally protected reasonable expectation of privacy."[13] Harlan argued that in order for a citizen to demonstrate that government conduct has intruded upon such a reasonable expectation of privacy, she must in turn meet "a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[14]

That test is now the touchstone in determining whether government conduct constitutes a search. Through it, the Court can preserve traditional zones of privacy in the face of new governmental investigative techniques.[15] Because the society-wide aspects of the test are unstable and perhaps unknowable,[16] the Court's implementations of it freeze privacy protections

[11] Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting); *see also* Scott E. Sundy, *'Everyman's' Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1755-56 (1994) (emphasizing the importance of the founding principles of the Fourth Amendment that Brandeis elucidated in his dissent).

[12] Katz v. United States, 389 U.S. 347 (1967).

[13] *Id.* at 360 (Harlan, J., concurring).

[14] *Id.* at 361. Others have argued that modern employment of the REOP test has eliminated the subjective prong, rendering the test wholly objective. *See* Orin S. Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113, 113-14 (2015).

[15] "[E]xisting Supreme Court precedent may fairly be construed to suggest that where society has historically recognized a legitimate expectation of privacy, we must continue to do so for purposes of Fourth Amendment analysis, even if, in our modern world, we must now expose to [the public] information that we would have previously kept private, in order to continue to participate fully in society. If we do not, we will face the Hobson's choice of leaving our historically recognized Fourth Amendment rights at the door of the modern world or finding ourselves locked out from it. That the constitution will not abide." United States v. Davis, 785 F. 3d 498, 527 (11th Cir. 2015) (Rosenbaum, J., concurring) cert. denied, 136 S. Ct. 479 (2015) (quoted in Rachel Levinson-Waldman, *Hiding in Plain Sight, A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L. J. 527, 577 (2017)); *see also* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1016 (2010) ("New facts will trigger new rules, but the role of the Constitution should remain constant regardless of technology.").

[16] *See* Carpenter v. United States, 585 U.S. ___ (2018) (Thomas, J., dissenting) (slip. op. at 18-19) (discussing the circularity of a test that asks a descriptive question about society's expectations to answer a question that will actually shape those very expectations). Citizens vary widely in their mastery of new technology, and their understandings are in flux as they obtain new information or as new publicity about technological capabilities emerges. *See* Matthew Tokson, *Knowledge and the Fourth Amendment*, 111 NW. U. L. REV. 139, 164-

that the Justices themselves deem important enough to maintain—even if technology continues to advance.[17] Such judicial estimations provide needed flexibility as the Court aims to uphold privacy in the face of monumental advances in technology.

A. Development of the Third-Party Doctrine

But such flexibility is accompanied by a frustrating lack of clarity. At times, the Justices have sought greater predictability in Fourth Amendment jurisprudence.[18] Unfortunately, that approach has created bright lines that fail to respond to the modern world. One example is the current third-party doctrine,[19] which the Court has helpfully summarized as follows:

81 (2016) ("Societal knowledge is a complex, multilayered concept that does not lend itself to easy application in criminal cases. Knowledge typically spreads unevenly through the population, and attributing median societal knowledge to criminal defendants raises questions of fundamental fairness. Judges are societal elites who are systematically likely to overestimate the extent of societal knowledge. . . . Further, even if societal knowledge could be measured perfectly, anchoring the Fourth Amendment's scope to it will lead to a gradual erosion of Fourth Amendment protection. As an increasingly intelligent and educated population gains awareness and understanding of new technologies and threats to privacy, expectations of privacy and the sphere of Fourth Amendment protection will naturally shrink.").

Additionally, Society's understanding of what is reasonable changes as citizens decide whether the capabilities of a new technology are worth the tradeoff in how that technology reduces our privacy, giving the Court a moving target. "Dramatic technological change may lead to periods in which popular expectations are in flux, and may ultimately produce significant changes in popular attitudes." United States v. Jones, 565 U.S. 400, 427 (2012) (Alito, J., concurring). "[T]echnology itself—its ubiquity, and its convenience—can dynamically change [society's] expectations. As people become more reliant on their devices, the technology may seem less intrusive, making the apparent privacy risks recede as well. A test premised on the reasonable expectation of privacy must become more objective to account for that shift." Rachel Levinson-Waldman, *Hiding in Plain Sight, A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L. J. 527, 550 (2017).

[17] The Justices are cognizant of the need to look to the forward march of investigative capabilities given evolving technologies. "[T]he rule the court adopts 'must take account of more sophisticated systems that are already in use or in development.' " Carpenter v. United States, 585 U.S. ___ (2018) (slip. op. at 14) (quoting Kyllo v. United States, 533 U.S. 27, 36 (2001)).

[18] Riley v. California, 134 S.Ct. 2492 (2014) (arguing that police officers must have clear, workable rules created "'on a categorical basis—not in an ad hoc, case-by-case fashion.'") (quoting Michigan v. Summers, 452 U.S. 692, 705 n. 19 (1981)).

[19] I have described the evolution of this doctrine in great detail in other work. *See* Michael Gentithes, *Tranquility & Mosaics in the Fourth Amendment: How Our Collective Interest in Constitutional Tranquility Renders Data Dragnets Like the NSA's Telephony Metadata Program a Search*, 82 TENN. L. REV. 937, 943-48 (2015). There, I noted that the doctrine first emerged in cases concerning verbal statements made to third parties that turned

> the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[20]

The third-party doctrine is thus a blunt instrument. It provides a simple rule: government collection of information disclosed to non-governmental third parties does not constitute a search subject to Fourth Amendment requirements.[21]

The third-party doctrine evolved in two influential cases from the 1970s, *United States v. Miller*[22] and *Smith v. Maryland*.[23] First, in *Miller*, government investigators obtained financial records of two accounts from a defendant's bank via an admittedly defective subpoena.[24] The defendant challenged the admission of his bank records as the fruit of an unlawful search.[25] The Supreme Court held that because "[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," there was no reasonable expectation of privacy in those records, and thus the government did not

out to be government informants, situations where "the defendant presumably had exercised some discretion in deciding who should enjoy his confidential communications." Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting) (citing Lopez v. United States, 373 U.S. 427, 439 (1963); Hoffa v. United States, 385 U.S. 293, 302-03 (1966); United States v. White, 401 U.S. 745, 751-52 (1971)).

[20] United States v. Miller, 425 U.S. 435, 443 (1976).

[21] For a brief summation of critiques of the third-party doctrine, *see* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 n.5 (2009) (citing Ashdown, *supra* note 22, at 1315; Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-first Century*, 65 IND. L. J. 549, 564-66 (1990); Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 MICH. L. REV. 1229 (1983); Sundby, *supra* note 15, at 1757-58; CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 151-64 (2007); Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protectino for Shared Privacy Righst in Stored Transactional Data*, 14 J.L. & POL'Y 211 (2006); Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3; Henderson, *supra* note 6, at 975; Matthew D. Lawless, *The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth Amendment Protection*, 2007 UCLA J.L. & TECH 1, 3-4; Andrew J. DeFilippis, Note, *Securing Informationships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence*¸115 YALE L. J. 1086, 1092 (2006)).

[22] 425 U.S. 435 (1976).

[23] 442 U.S. 735 (1979).

[24] United States v. Miller, 425 U.S. 435, 438 (1976).

[25] United States v. Miller, 425 U.S. 435, 436 (1976).

conduct a search when it collected them.[26] The defendant assumed the risk that third-party bankers would reveal his sensitive financial information to the government, tacitly consenting to such disclosures.[27]

Three years later in *Smith*, police officers warrantlessly asked a telephone company to install a pen register device in its central offices to record the numbers dialed from the home phone of a man suspected of robbing and later harassing a Baltimore woman.[28] That device disclosed only the telephone numbers that the defendant dialed.[29] The Court held that the government's installation of that device did not constitute a search because the defendant had no reasonable expectation of privacy in the numbers he dialed and thereby disclosed to a third party.[30] Telephone users "typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes."[31] Thus, the government was not required to obtain a warrant prior to collecting such information through a pen register, because the defendant had no reasonable expectation of privacy in that information.[32]

B. Limits of the Third-Party Doctrine

These cases suggest an unlimited investigative technique for government investigators in today's world, but subsequent decisions have cabined the third-party doctrine's expansive reach. For instance, while investigators can warrantlessly collect dialed telephone numbers,[33] they cannot collect the words spoken in the subsequent conversation, which are also provided to

[26] United States v. Miller, 425 U.S. 435, 442 (1976).

[27] United States v. Miller, 425 U.S. 435, 443 (1976). Another rationale underlying *Miller* was the fact that banks traditionally kept these records, so the government's effort to collect them was not a "novel means designed to circumvent established Fourth Amendment rights." *Id.* at 444.

[28] Smith v. Maryland, 442 U.S. 735, 737 (1979).

[29] Smith v. Maryland, 442 U.S. 735, 741 (1979).

[30] Smith v. Maryland, 442 U.S. 735, 743-46 (1979) (citing U.S. v. Miller, 425 U.S. 435, 442-444, (1976))

[31] Smith v. Maryland, 442 U.S. 735, 743 (1979).

[32] Smith v. Maryland, 442 U.S. 735, 745-46 (1979). Justice Marshall vigorously dissented from the majority's assumption of the risk rationale in *Smith*. Marshall noted that "[i]mplicit in the concept of assumption of risk is some notion of choice . . . By contrast here, unless 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. It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative." *Id.* at 749-50 (Marshall, J., dissenting).

[33] Smith v. Maryland, 442 U.S. 735 (1979).

third parties.[34] Similarly, the government cannot warrantlessly collect medical information disclosed to third-party doctors: "The reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent."[35] Nor can investigators warrantlessly search a suspect's hotel room, despite the fact that third party housekeepers or maintenance people may have accessed the room or even moved the suspect's belongings.[36] Fourth Amendment protections also extend to a suspect's rental apartment, "even though his landlord has the right to conduct unannounced inspections at any time."[37]

Though it claimed to leave the third-party doctrine intact, *Carpenter* added to the growing list of exceptions to that once bright line. The *Carpenter* majority addressed the collection of cell site location information ("CSLI") generated by cell phone companies to show which cell tower a customer's phone accessed at particular times, and hence roughly where the customer was.[38] The *Carpenter* majority excepted a week's worth of CSLI from warrantless collection under the third-party doctrine, opening the door for varying applications of the doctrine to "distinct categor[ies] of

[34] "People disclose the content of telephone calls to third parties. But we said the government can't intrude without a warrant in that situation." Sotomayor, J., Transcript of Oral Argument at 50-51, Carpenter v. United States, No. 16-402.

[35] Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001); *see also* Sotomayor, J., Transcript of Oral Argument at 23, Carpenter v. United States, No. 16-402 ("We limited it when—in Bond and Ferguson when we said police can't get your medical records without your consent, even though you've disclosed your medical records to doctors at a hospital."); Or. Prescription Drug Monitoring Program v. DEA, 998 F. Supp. 2d 957, 964-65 (D. Or. 2014) (finding a reasonable expectation of privacy in diagnostic tests conducted at a hospital) (cited Price, *supra* note 6, at 298 n.323).

[36] "[T]he Supreme Court has held that '[a] hotel room can clearly be the object of Fourth Amendment protection as much as a home or an office.' This is so, even though housekeepers and maintenance people commonly have access to hotel rooms during a guest's stay and can view and even move around a guest's belongings in order to conduct their duties. But the fact that a hotel guest has exposed his or her belongings to hotel workers does not, in and of itself, entitle the government to enter a rented hotel room and conduct a warrantless search." United States v. Davis, 785 F. 3d 498, 527 (11th Cir. 2015) (Rosenbaum, J., concurring) *cert. denied*, 136 S. Ct. 479 (2015) (citing Hoffa v. United States, 385 U.S. 293, 301 (1966); Minnesota v. Carter, 525 U.S. 83, 95-96 (1998) (Scalia, J., concurring); Minnesota v. Olson, 495 U.S. 91, 96-97 (1990)); *see also* United States v. Warshak, 631 F.3d 266, 287 (6th Cir. 2010) ("Hotel guests, for example, have a reasonable expectation of privacy in their rooms. This is so even though maids routinely enter hotel rooms to replace the towels and tidy the furniture. Similarly, tenants have a legitimate expectation of privacy in their apartments. That expectation persists, regardless of the incursions of handymen to fix leaky faucets.") (citations omitted).

[37] O'Connor v. Ortega, 480 U.S. 709, 730 (1987) (Scalia, J., concurring) (quoted in SCHULHOFER, *supra* note 7, at 131).

[38] Carpenter v. United States, 585 U.S. ___ (2018) (slip. op. at 1-2).

information."[39] The Court expressed trepidation about subjecting CSLI to the third-party doctrine in any amount given its "deeply revealing nature . . . its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection."[40] It also referenced the "unique nature" of CSLI's "intimate window" into a customer's life.[41] However, it failed to clearly delineate the difference "between cell-site records on the one hand and financial and telephonic records on the other."[42]

Carpenter's promise was for a categorical approach to information collected by third-parties. As I have argued elsewhere, informational sensitivity was also at the core of the *Carpenter* majority's discomfort with warrantless collection of CSLI, though it was not clearly expressed in the opinion.[43]

How, then, should the Court approach the information apps collect via "permissions" granted by the operating system on user's cell phones? As the following section outlines, such apps collect vast (and vastly different) categories of information, each of which will have its own valence of sensitivity. It will provide the reader with an understanding of how apps obtain and use permissions, before the final section outlines an appropriate response to warrantless collection of the information apps obtain through such permissions.

II. APPS AND PERMISSIONS

Apps on digital devices offer incredible convenience, but often at great risk to the user's privacy. Before performing their functions, apps obtain a wide variety of "permissions" to access and send data to a server without informing the user each time it does so. This Part provides a rough explanation of how those permissions work and their wide, and often unnecessary, scope.

A. How Permissions Work

Download any new app to your digital device, and that app will obtain permissions that allow it to access and send data in two ways. First, the app

[39] Carpenter v. United States, 585 U.S. ___ (2018) (slip. op. at 15).

[40] Carpenter v. United States, 585 U.S. ___ (2018) (slip. op. at 22).

[41] Carpenter v. United States, 585 U.S. ___ (2018) (slip. op. at 12, 17)

[42] CITE MY GEORGIA ARTICLE

[43] CITE GEORGIA ARTICLE. I thus recommended a two-step approach to determine the constitutional protection for new categories of information presented by future cases, which would account for both the inherent sensitivity of the information and the sheer volume of sensitive information the government has collected and potentially assembled into an informational mosaic of the citizen. CITE GEORGIA ARTICLE.

will send you pop-up messages indicating that it would like to access certain capabilities of your device—perhaps your location services or your camera—and offer you the choice to permit that access or decline it.[44] Second, without any input from you at all, the operating system on your device may allow the app to access some capabilities, and hence some data, that the system considers less sensitive.

The first, more well-known avenue through which apps gain permissions is through explicit requests to the user during the installation process. Though app platforms encourage app developers to explain why they want certain permissions,[45] those explanations are often vague, if not downright misleading. Most users—and even some security experts—find permission descriptions inscrutable.[46] Developers often use misleading techniques, such as simply tacking the phrase "and more" to permission explanations to conceal the true extent of those requests.[47] In addition, the consequences of

[44] "Obtaining permissions is a two-step process. First, an application developer declares that his or her application requires certain permissions in a file that is packaged with the application. Second, the user must approve the permissions requested before installation." Adrienne Porter Felt et al., *Android Permissions: User Attention, Comprehension, and Behavior*, in PROCEEDINGS OF THE 8TH SYMPOSIUM ON USABLE PRIVACY AND SECURITY (2012), available at https://cups.cs.cmu.edu/soups/2012/proceedings/a3_Felt.pdf.

[45] "Before your app requests a permission, you should consider providing an explanation to the user. Keep in mind that you don't want to overwhelm the user with explanations; if you provide too many explanations, the user might find the app frustrating and remove it." *Request App Permissions*, ANDROID.COM, https://developer.android.com/training/permissions/requesting.html; *See also* Lauren Goode, *App Permissions Don't Tell Us Nearly Enough About Our Apps*, WIRED.COM, https://www.wired.com/story/app-permissions/, April 14, 2018 ("A permission request from an app pops up, and it's on the smartphone user to decide whether to open that door. Sometimes they come with explanations; in fact, the app platforms encourage this. 'It's a good idea to explain to the user why your app wants the permissions before calling requestPermissions(),' the Android developer documentation says.").

[46] Lori Andrews, *A New Privacy Paradigm in the Age of Apps*, 53 WAKE FOREST L. REV. 421, 439 (2018) (citations omitted).

[47] "Some app makers just tack 'and more' onto its permissions explanations. Facebook's explanation for location says 'Facebook uses this to make some features work, help people find places, and more,' while Snapchat's explanation for using your microphone is 'to record audio for Snaps, video chat, and more.'" Lauren Goode, *App Permissions Don't Tell Us Nearly Enough About Our Apps*, WIRED.COM, https://www.wired.com/story/app-permissions/, April 14, 2018.

It is worth noting that there is some variation in the stringency of permissions granted between the two largest app ecosystems, Google's Android and Apple's iOS. "Apple in general has been much more stringent than Google has been with app developers. As with Android, you can control iOS permissions both in privacy settings and at the app level. With the rollout of iOS 11 . . . Apple offered a "Write Only" option for app developers using Photos, so they wouldn't have to request Read access to camera rolls. It also started cracking down on location permissions: app makers are now forced to show the 'Only when using the app' option when requesting location access. And as ArsTechnica pointed out, the company declining a request for permissions are often unclear. In their literature describing best practices for app developers, both the Android and iOS platforms suggest that developers clearly explain the need for their permission requests; they also suggest designing "exceptions" for the app, so that even if the user declines some permissions, the app can continue to perform some or all of its tasks.[48] But in at least some cases, when the user declines an app's permission request, the app will not work.[49] Indeed, for many apps the choice is binary: either grant all of the app's permission requests, or cancel the installation.[50]

has never given iOS developers access to call logs." Lauren Goode, *App Permissions Don't Tell Us Nearly Enough About Our Apps,* WIRED.COM, https://www.wired.com/story/app-permissions/, April 14, 2018.

[48] *See App Permissions Best Practices*, ANDROID.COM, https://developer.android.com/training/permissions/usage-notes ("Users can deny access to individual permissions at the time they're requested and in settings, but they may still be surprised when functionality is broken as a result. It's a good idea to monitor how many users are denying permissions (e.g. using Google Analytics) so that you can either refactor your app to avoid depending on that permission or provide a better explanation of why you need the permission for your app to work properly. You should also make sure that your app handles exceptions created when users deny permission requests or toggle off permissions in settings."); *Protecting the User's Privacy*, APPLE.COM, https://developer.apple.com/documentation/uikit/core_app/protecting_the_user_s_privacy ("Request access to sensitive user or device data—like location, contacts, and photos—at the time your app needs the data. . . . Provide reasonable fallback behavior in situations where the user doesn't grant access to the requested data."); *see also Requesting Permission*, APPLE.COM, https://developer.apple.com/design/human-interface-guidelines/ios/app-architecture/requesting-permission/ ("Users must grant permission for an app to access personal information, including the current location, calendar, contact information, reminders, and photos. Although people appreciate the convenience of using an app that has access to this information, they also expect to have control over their private data. For example, people like being able to automatically tag photos with their physical location or find nearby friends, but they also want the option to disable such features.").

[49] "That's how all permissions for Android apps work. An app will ask for permission when it needs something it can't access without it, and if you choose to refuse, that part of the app will not work. This can have little effect on the rest of the app, or it can be show-stopping and the app won't work." Jerry Hildenbrand, *What Happens When I Decline an App Permission?*, ANDROIDCENTRAL.COM, May 30, 2018, https://www.androidcentral.com/what-happens-when-i-decline-app-permission.

[50] Indeed, prior versions of Android's permission system gave users "a binary choice: they [could] cancel the installation, or they [could] accept all of the permissions and proceed with installation." Adrienne Porter Felt et al., *Android Permissions: User Attention, Comprehension, and Behavior*, in PROCEEDINGS OF THE 8TH SYMPOSIUM ON USABLE PRIVACY AND SECURITY (2012), available at https://cups.cs.cmu.edu/soups/2012/proceedings/a3_Felt.pdf. Researchers have posited that users frequently make their decision to purchase an app when they download it; thus, permissions presented to the user at installation—after they have already made that purchase decision—will almost always be granted. *See* Patrick Gage Kelley et al., *Privacy as Part of the App-Decision Making Process*, 3 (2013) (available at

The second avenue through which apps obtain permissions occurs without user input. A device's operating system may allow apps to obtain some permissions automatically upon installation.[51] For instance, in Google's Android platform, certain "normal" permissions are immediately granted upon installation, without the app making any requests to the user.[52] "The system doesn't prompt the user to grant normal permissions, and users cannot revoke these permissions."[53] Google limits such automatically granted "normal" permissions to information that it considers less sensitive because "there's very little risk to the user's privacy or the operation of other apps."[54] But users might be surprised to know that automatically-granted "normal" permissions include allowing an app to discover and pair with nearby Bluetooth devices without their approval,[55] change their network or wifi

https://apps.dtic.mil/dtic/tr/fulltext/u2/a579375.pdf).

[51] As the remained of this paragraph demonstrates, this is a feature of the Android operating system without a clear parallel in the iOS operating system.

[52] *See Request App Permissions*, ANDROID.COM, https://developer.android.com/training/permissions/requesting.html. "Android 2.2 defines 134 permissions, categorized into three threat levels: 1. Normal permissions protect access to API calls that could annoy but not harm the user. For example, SET_WALLPAPER controls the ability to change the user's background wallpaper. 2. Dangerous permissions control access to potentially harmful API calls, like those related to spending money or gathering private information. For example, Dangerous permissions are required to send text messages or read the list of contacts. 3. Signature/System permissions regulate access to the most dangerous privileges, such as the ability to control the backup process or delete application packages. These permissions are difficult to obtain: Signature permissions are granted only to applications that are signed with the device manufacturer's certificate, and SignatureOrSystem permissions are granted to applications that are signed or installed in a special system folder. These restrictions essentially limit Signature/System permissions to pre-installed applications, and requests for Signature/System permissions by other applications will be ignored." ADRIENNE PORTER FELT ET AL., ANDROID PERMISSIONS DEMYSTIFIED 628 (2011), https://people.eecs.berkeley.edu/~dawnsong/papers/2011%20Android%20permissions%20demystified.pdf

[53] *Protection Levels*, Android.com, https://developer.android.com/guide/topics/permissions/overview.html#normal-dangerous.

[54] *Protection Levels*, Android.com, https://developer.android.com/guide/topics/permissions/overview.html#normal-dangerous.

[55] *See Protection Levels*, Android.com, https://developer.android.com/guide/topics/permissions/overview.html#normal-dangerous (describing the permissions Android classifies as "normal"); https://developer.android.com/reference/android/Manifest.permission.html#BLUETOOTH_ADMIN (describing the "BLUETOOTH_ADMIN" permission).

connectivity state,[56] or access their device's fingerprint hardware.[57]

B. The Scope of Permissions

Permissions—which users often must grant in order to use the app for its intended, and quite possibly necessary, purposes—allow apps to perform functions on a digital device that may include elements of highly personal data about the user. Often, this includes access to information unrelated to the app's intended functions.[58] As an example, consider mobile health apps, which might manage a user's chronic physical or mental conditions like diabetes, bipolar disorder, or anorexia. Medical practitioners often recommend the use of these apps to their patients; one recent study found that approximately 7% of primary care physicians have recommended a health app to a patient.[59] Furthermore, mobile health apps are increasingly a required component of workplace wellness programs that employers pressure employees to join, sometimes with financial consequences in the form of higher insurance premiums for non-participants.[60]

[56] *See Protection Levels*, Android.com, https://developer.android.com/guide/topics/permissions/overview.html#normal-dangerous (describing the permissions Android classifies as "normal"); https://developer.android.com/reference/android/Manifest.permission.html#CHANGE_NETWORK_STATE (describing the "CHANGE_NETWORK_STATE" permission); https://developer.android.com/reference/android/Manifest.permission.html#CHANGE_WIFI_STATE (describing the "CHANGE_WIFI_STATE" permission).

[57] *See Protection Levels*, Android.com, https://developer.android.com/guide/topics/permissions/overview.html#normal-dangerous (describing the permissions Android classifies as "normal"); https://developer.android.com/reference/android/Manifest.permission.html#USE_FINGERPRINT (describing the "USE_FINGERPRINT" permission).

[58] A 2014 study found that "96% of iOS apps require email permissions, 92% require address book, 84% require location permissions, 52% require camera permissions, and 32% require calendar permissions." Jina Kang et al., *Analyzing Unnecessary Permission Requests by Android Apps Based on Users' Opinions*, in INFORMATION SECURITY APPLICATIONS 68, 68 (2014) (citing John Leyden. *The Truth about Leaky, Stalking, Spying Smartphone Applications*, THE REGISTER, Jan. 31, 2014, https://www.theregister.co.uk/2014/01/31/smartphone_app_spy_risks/).

[59] Amy M. Bauer et al., *Use of Mobile Health (mHealth) Tools by Primary Care Patients in the WWA.MI Region Practice and Research Network (WPRN)*, 27 J. AM. BOARD FAM. MED. 780, 784 (2014) (cited in Lori Andrews, *A New Privacy Paradigm in the Age of Apps*, 53 WAKE FOREST L. REV. 421, 429 (2018)).

[60] "In addition, medical apps and wearables like Fitbit that monitor an employee's activities and health are becoming increasingly common in the workplace. Employees are sometimes pressured into participating in a workplace wellness program; for example, Houston city employees were required to pay an extra three hundred dollars a year for medical coverage if they declined to participate in the workplace wellness program. The company Houston hired to collect health data from the program had the power to share the

Mobile medical apps often request extremely broad permissions, and often in areas wholly unrelated to their intended purposes. In 2018, Lori Andrews conducted a study on 211 diabetes apps downloaded from Google's Play Store.[61] Nearly 15% of those apps requested access to the user's precise GPS location, while over 12% requested access to the user's approximate location; nearly 6% requested permission to directly call phone numbers, while another 4% requested permission to modify the user's contacts, and still another 4% requested permission to read the user's call log; nearly 4% requested permission to record audio; and more than 11% requested permission to take pictures and videos.[62] Andrews also studied 63 Bipolar disorder apps, finding that 17% requested permission to access the user's precise GPS location and 16% requested permission to access the user's approximate location; 5% requested permission to directly call phone numbers or access the user's call log; 5% requested permission to record audio; and 13% requested permission to take pictures and videos.[63]

Mobile medical apps are not alone in overreaching for permissions unrelated to their intended purposes. One study of 940 Android apps found that about one-third obtained more permissions than needed for the app to perform its intended function.[64] The most common unnecessary permissions that apps obtained included several capabilities that the Android platform considers dangerous, including: reading the status of any ongoing calls and any phone accounts registered on the device (unnecessarily requested by 16% of the apps studied); initiating phone calls (6%); accessing the device's camera (6%); and accessing the user's approximate location (6%).[65]

Studies of Android apps have also found that free apps are more likely to request unnecessary or dangerous permissions than paid apps.[66] Researchers

data with third-party vendors and even post the data in areas "that are reviewable to the public." Lori Andrews, *A New Privacy Paradigm in the Age of Apps*, 53 WAKE FOREST L. REV. 421, 429 (2018) (citations omitted).

[61] Lori Andrews, *A New Privacy Paradigm in the Age of Apps*, 53 WAKE FOREST L. REV. 421, 432 (2018).

[62] Data from Lori Andrews on file with author.

[63] Data from Lori Andrews on file with author.

[64] ADRIENNE PORTER FELT ET AL., ANDROID PERMISSIONS DEMYSTIFIED 637 (2011), https://people.eecs.berkeley.edu/~dawnsong/papers/2011%20Android%20permissions%20demystified.pdf (cited in Lori Andrews, *A New Privacy Paradigm in the Age of Apps*, 53 WAKE FOREST L. REV. 421, 440 (2018)).

[65] ADRIENNE PORTER FELT ET AL., ANDROID PERMISSIONS DEMYSTIFIED 635 (2011), https://people.eecs.berkeley.edu/~dawnsong/papers/2011%20Android%20permissions%20demystified.pdf; https://developer.android.com/reference/android/Manifest.permission.html#constants_2 (describing the "READ_PHONE_STATE," "CALL_PHONE," "CAMERA," and "ACCESS_COARSE_LOCATION" permissions).

[66] Lori Andrews, *A New Privacy Paradigm in the Age of Apps*, 53 WAKE FOREST L.

attribute the difference to the fact that many free apps rely upon advertising revenue, acting primarily as data collectors for third parties rather than service providers.[67] This can lead to the disclosure of personal information to a variety of third parties,[68] which, as the next section discusses, potentially includes law enforcement.

III. SHOULD THE THIRD-PARTY DOCTRINE APPLY TO INFORMATION APPS COLLECT THROUGH PERMISSIONS?

Suppose that government investigators subpoena an app developer for information the developer collected about a user, who also happens to be a suspect in a criminal investigation. The developer collected that information via permissions from the user. Some of those permissions were entirely ancillary to the purposes of the app—say, access to the user's contacts or microphone for the kinds of mobile medical apps described above. The user granted them as a reluctant exchange for app functionality, while her operating system granted others automatically without any user input at all.

The third-party doctrine seemingly permits the government to collect any information apps obtain via permissions without a warrant. As discussed above, the third-party doctrine presents a bright-line rule: whenever a citizen disclosed information to a third-party service provider, government investigators can in turn warrantlessly collect that information, because such

REV. 421, 441 (2018) (citing Adrienne Porter Felt et al., *Android Permissions: User Attention, Comprehension, and Behavior*, in PROCEEDINGS OF THE 8TH SYMPOSIUM ON USABLE PRIVACY AND SECURITY (2012), available at https://cups.cs.cmu.edu/soups/2012/proceedings/a3_Felt.pdf; Jina Kang et al., *Analyzing Unnecessary Permissions Requested by Android Apps Based on Users' Opinions*, in INFORMATION SECURITY APPLICATIONS 68, 76 (2014)).

[67] Lori Andrews, *A New Privacy Paradigm in the Age of Apps*, 53 WAKE FOREST L. REV. 421, 441 (2018) (citing Jina Kang et al., *Analyzing Unnecessary Permissions Requested by Android Apps Based on Users' Opinions*, in INFORMATION SECURITY APPLICATIONS 68, 78 (2014)). "These permissions go well beyond any relevant purpose of the app. But the information collected through the app can be a goldmine to the developer if sold for marketing purposes." Lori Andrews, *A New Privacy Paradigm in the Age of Apps*, 53 WAKE FOREST L. REV. 421, 440 (2018).

[68] Discussing mobile medical apps in particular, Andrews notes that "the information from medical apps can be collected, disclosed, and sold to the user's disadvantage in various ways. The app developer (or data aggregator that contracts with the developer) can collect and market the information. Or an unrelated data aggregator can collect the information via tracking mechanisms (such as cookies, web beacons, and bots) from other mobile apps, websites the person visits, or the phone itself. The entity with access to medical app data can use it to market products and services to the individual, entice the individual to participate in a medical study, or make a social, moral, or medical judgement about the eligibility of a person for a benefit such as insurance or a job." Lori Andrews, *A New Privacy Paradigm in the Age of Apps*, 53 WAKE FOREST L. REV. 421, 430 (2018) (citations omitted)

collection does not amount to a search subject to Fourth Amendment requirements.[69] Thus, the government's request to the app developer through a subpoena or other legal process would not amount to a search that requires a warrant based upon probable cause.

But *Carpenter* acknowledges that there may be exceptions to the third-party doctrine's apparent bright line for "unique" or "intimate" categories of information.[70] In the spirit of the *Carpenter* majority, I thus propose some categorical exceptions to the third-party doctrine for information apps collect through permissions.

First, the third-party doctrine should not apply to information collected through a permission if that permission that lacks a sufficient nexus to the app's intended purposes. When developers obtain unnecessary permissions—such as mobile medical apps that seek unnecessary access to the user's contacts or microphone—the user does not voluntarily disclose information in exchange for a helpful convenience. Instead, given the incomprehensibility of permission requests and the user's limited understanding of them,[71] developers clandestinely collect information about users, which they can later use to tailor in-app advertising or disclose to commercial partners.

Information collected through such unnecessary permissions should not be subject to the traditional third-party doctrine. The user did not knowingly and voluntarily disclose information to the app developer; nor did they meaningfully, freely consent to that developer's data collection. In cases where the government warrantlessly seeks information apps obtained through permissions, I propose a standard familiar to Fourth Amendment theory to determine whether the third-party doctrine applies: such information can only be warrantlessly collected where the permissions had a clear, articulable connection to the app's intended purposes.

This test would allow users to maintain meaningful control over their private information in the face of confusing, often unnecessary permission requests from app developers. It would also allow app developers to maintain

[69] United States v. Miller, 425 U.S. 435, 443 (1976).

[70] Carpenter v. United States, 585 U.S. ___ (2018) (slip. op. at 12, 17)

[71] *See, e.g.*, Patrick Gage Kelley et al., *A Conundrum of Permissions: Installing Applications on an Android Smartphone*, in PROCEEDINGS OF THE 16TH FINANCIAL CRYPTOGRAPHY AND DATA SECURITY CONFERENCE 68 (2012).

Others have noted that privacy policies from major tech and media platforms are similarly incomprehensible. A recent New York Times study of 150 such privacy policies found that the average policy took 18 minutes to finish and required a college-level reading ability. Kevin Litman-Navarro, *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster*, N.Y. TIMES, June 12, 2019, https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html?action=click&module=Opinion&pgtype=Homepage.

functionality without constantly pestering users with additional requests to access functions on their devices. At the same time, it would not burden users with an unrealistic expectation to parse confusing permissions requests for each app they download and to make meaningful choices to protect private information on their digital devices.

Importantly, this test would also allow law enforcement officers to collect most information apps obtain through permissions. The majority of permissions are necessary for the apps to perform the convenient functions the designers intended. The rule I have proposed only applies to permission overreach. So long as permissions are related to the app's intended purposes, the third-party doctrine applies; no warrant is necessary to obtain information obtained via those permissions. Additionally, even if government investigators were unable to collect specific information from one app developer because it was collected through an unnecessary permission, they may be able to obtain the very same information about the very same user from another app on that user's device, so long as the permission was sufficiently related to the purpose of that second app.

I would add a second categorical exception to the third-party doctrine's application in cases involving data obtained via permissions. The third-party doctrine should not apply when the app developer's request for permission fails to explain how that permission is related to the app's intended function—even if there is the sort of clear, articulable connection mentioned above. For instance, permissions that seek access to the device's camera or microphone to perform a specific task "and more" might not trigger the third-party doctrine. The user's response to such vague requests might not amount to voluntary disclosure of information to a third party. Thus, the government should not be permitted to collect it from that third party without a warrant.

My position parallels critiques of the "assumption of the risk" rationale for the third-party doctrine offered by the dissenting Justices at the beginning of the third-party doctrine's history. For instance, in his dissent in *Miller*, Justice Brennan noted that "[f]or all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account."[72] Thus, Brennan asserted that bank customers reasonably believe that the financial information they disclose "will be utilized by the bank only for internal banking purposes," absent compulsion by legal process.[73] The assumption of the risk rationale met similar resistance from some Justices in *Smith* three years later. There, Justice Marshall argued that

> [i]mplicit in the concept of assumption of risk is some notion

[72] United States v. Miller, 425 U.S. 435, 451 (1976) (Brennan, J., dissenting).
[73] United States v. Miller, 425 U.S. 435, 449 (1976) (Brennan, J., dissenting).

> of choice. . . . By contrast here, unless 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. It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative.[74]

The rationale that Brennan and Marshall espoused is even stronger in the case of permissions that an app developer fails to describe in understandable detail. If the permission request does not explain the extent to which the app will access the user's data, the user cannot knowingly assume the risk that the app will collect private details about them and disclose them to government investigators.

The categorical exceptions I have proposed also align with critiques of the notice-and-consent privacy regime, especially given how convoluted and unclear permission requests can be. Such regimes offer services on a take-it-or-leave-it basis; accept the conditions about which the service provider notifies you, or decline the service altogether.[75] Where such services are a practical necessity, convoluted notices provides little value to users.[76] Notice-and-consent regimes also place unrealistic burdens upon users to read, understand, and incorporate the myriad notices they receive constantly from service providers. One study estimated that it would take a user thirty days to read the privacy statements of the apps and websites that she commonly uses.[77] Rather than rely upon such voluminous and convoluted notices to protect user privacy against government intrusion, courts should apply some straightforward exceptions to otherwise applicable Fourth Amendment rules.

[74] Smith v. Maryland, 442 U.S. 735, 749–50 (1979) (Marshall, J., dissenting) (citations omitted). In the years since *Smith*, these critiques have been repeated in the academic literature. *See, e.g.*, BARRY FRIEDMAN, UNWARRANTED: POLICING WITHOUT PERMISSION 236 (2017) ("'Voluntarily' is the trick word here . . . . [I]n today's world we have little choice but to give our most intimate information to third parties all the time."); Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. NAT'L SEC. L. & POL'Y 247, 267 (2016) ("It is . . . impossible to fully participate in modern economic life without involving a bank to execute transactions. Because this third-party interaction is unavoidable, it undermines the assumption of risk rationale."); Orin Kerr & Greg Nojeim, *The Data Question: Should the Third-Party Records Doctrine Be Revisited?*, A.B.A. J., Aug. 2012, http://www.abajournal.com/magazine/article/the_data_question_should_the_third-party_records_doctrine_be_revisited/ ("If you want to communicate efficiently today, your communications likely will go through your ISP's servers. The alternative means of communication either involve conveying information to other third parties, or traveling to the other communicant so you can have a personal chat. Consent in this context has little meaning.").

[75] Lori Andrews, *A New Privacy Paradigm in the Age of Apps*, 53 WAKE FOREST L. REV. 421, 462 (2018).

[76] Lori Andrews, *A New Privacy Paradigm in the Age of Apps*, 53 WAKE FOREST L. REV. 421, 462-63 (2018).

[77] Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: A J. L. & POL'Y FOR INFO. SOC'Y 543, 562-63 (2008) (cited in Lori Andrews, *A New Privacy Paradigm in the Age of Apps*, 53 WAKE FOREST L. REV. 421, 464 (2018)).

CONCLUSION

Carpenter presents courts and theorists with both a conundrum and an opportunity. It opens the door to a categorical approach to data collected by third parties and later obtained warrantlessly by government investigators. Some such data may be excepted from the third-party doctrine, and hence suppressed absent a warrant, under *Carpenter*'s holding. This Article considered one such data type, information that apps collect via permissions, which are often tenuously related to the app's ordinary functions. I suggest some clear exceptions to the third-party doctrine when the government accesses such information. First, such information can only be warrantlessly collected where the permissions had a clear, articulable connection to the app's intended purposes. Second, the third-party doctrine should not apply when the app developer's request for permission fails to explain how that permission is related to the app's intended function. These exceptions to the third-party doctrine would serve user privacy well, applying the kind of fluidity that *Carpenter* introduced in a helpful way for modern citizens.