11-2020

Inescapable Surveillance

Matthew Tokson

INESCAPABLE SURVEILLANCE

Matthew Tokson[†]

Until recently, Supreme Court precedent dictated that a person waives their Fourth Amendment rights in information they disclose to another party. The Court reshaped this doctrine in *Carpenter v. United States*, establishing that the Fourth Amendment protects cell phone location data even though it is revealed to others. The Court emphasized that consumers had little choice but to disclose their data, because cell phone use is virtually inescapable in modern society.

In the wake of *Carpenter*, many scholars and lower courts have endorsed inescapability as an important factor for determining Fourth Amendment rights. Under this approach, surveillance that people cannot feasibly escape receives more Fourth Amendment scrutiny, while surveillance that can be avoided receives less, or none.

This Article offers the first systematic analysis of inescapability in Fourth Amendment law. It challenges the prevailing wisdom that inescapability is a desirable or workable basis for Fourth Amendment protection. Inescapability does not provide a conceptually coherent standard for courts to apply. It incentivizes consumers to forego beneficial technologies, creating substantial social harms. It fails to adequately protect the most sensitive forms of personal information. It creates doctrinal confusion and ignores established precedents that contradict the inescapability model. Moreover, inescapability analysis elides individual differences—technologies that are avoidable for most people may be unavoidable for others, including the

---

[†] Associate Professor, University of Utah S.J. Quinney College of Law. Thanks to Robin Craig, Brigham Daniels, Andrew Gilden, Thomas Haley, Emily Hughes, Cathy Hwang, RonNell Andersen Jones, Elizabeth Kronk Warner, Wayne Logan, Eric Miller, Cliff Rosky, Alan Rozenshtein, Ari Ezra Waldman, and all participants in the AALS Criminal Law Works in Progress Panel, The Privacy Law Scholars Conference, The Rocky Mountain Junior Scholars Conference, The University of Utah S.J. Quinney College of Law Faculty Workshop, and the University of Akron School of Law Faculty Workshop. Special thanks to Shenelle Salcido for excellent research assistance.

disabled, the poor, and other disadvantaged populations.

Inescapability threatens to limit privacy rights to a narrow set of digital technologies while making a mess of Fourth Amendment doctrine. This Article analyzes these issues in depth and explores several alternatives for determining Fourth Amendment protections in the digital age.

INTRODUCTION

Many modern technologies gather information about their users.[1] These technologies are often hard to avoid. Computers, the internet, and cell phones are ubiquitous and play an important role in most people's lives.[2] Yet many technologies are far less essential. Consider the Furbo, an interactive camera device that allows pet owners to remotely launch treats at their pets by pressing a button on their cell phones.[3] The Furbo may be useful for pet owners, but owning one is not a necessity of modern life.

This distinction between avoidable and unavoidable technologies arose recently in a landmark Fourth Amendment case involving cell phone location data. In *Carpenter v. United States*, the Supreme Court ruled that government officials must get a warrant before obtaining cell phone location data that would allow them to track users' movements over time.[4] The Court found that people have no choice but to disclose their location data, because cell phone use is virtually "inescapable" in modern life.[5] Accordingly, users

---

[1] *See, e.g.*, Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 812–18 (2016).

[2] *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (discussing the central importance of cell phones to modern life); Riley v. California, 134 S. Ct. 2473, 2484 (2014) (noting that cell phones are a "pervasive and insistent part of daily life"); Packingham v. North Carolina, 137 S. Ct. 1730, 1735–36 (2017) (describing the importance of the internet and social media to core First Amendment activity).

[3] FURBO DOG CAMERA, https://shopus.furbo.com/ [https://perma.cc/GYZ5-GWZJ?type=image] (last visited July 28, 2020). The Furbo also enables owners to communicate with their pets via a two-way audio system. *Id.* The latest version of the Furbo can capture videos whenever pet activity is detected and store those videos in the cloud. *Id.* It analyzes these videos using artificial intelligence and sends text alerts to owners regarding their pets' activities. *Id.* The Furbo records video and sound from the inside of owners' homes on a "24 hours event-based" protocol, potentially capturing sensitive data about the owner and their activities inside their home. *See id.* It also has several benefits, including the ability to monitor one's pet and to detect intruders or other emergencies. *Id.*

[4] *Carpenter*, 138 S. Ct. at 2221.

[5] *Id.* at 2223. Moreover, cell phone data is transmitted automatically when a phone is in use, without any input or permission from the user, making it impossible for even sophisticated users to escape the disclosure of their information. *Id.* at 2220.

do not voluntarily give up their information—and they retain a Fourth Amendment right in their cell phone location data.[6] The Court also reasoned that cell phone tracking reveals sensitive personal information and collects a great deal of data about people's lives.[7]

Carpenter was a huge development in Fourth Amendment law.[8] For the first time, it declared that the Fourth Amendment protected location data even if that data had been exposed to another party.[9] This raised the possibility that other forms of personal data disclosed to private parties might be protected as well.[10] This category includes nearly every form of digital information: websurfing data, emails, texts, search terms, app usage, video and audio recordings, medical and fitness information, smart home data, and much more.[11] Whether such data is ultimately protected may depend on whether its disclosure is "inescapable."[12]

In the wake of *Carpenter*, many lower courts have applied an inescapability standard, attempting to determine whether the digital surveillance at issue in a case was avoidable.[13] Several scholars have endorsed

---

[6] *Id.* at 2220.

[7] *Id.* at 2217–18.

[8] *See generally* Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357, 358 (2019) (contending that *Carpenter* represents a sea change in Fourth Amendment law governing new technologies).

[9] *Carpenter*, 138 S. Ct. at 2217 ("Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection."); *cf.* United States v. Karo, 468 U.S. 705, 721 (1984) (finding no Fourth Amendment search when agents used a beeper to monitor a truck on public highways); United States v. Knotts, 460 U.S. 276, 281–82 (1983) ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another," because he "voluntarily conveyed to anyone who wanted to look the fact that he was travelling over particular roads in a particular direction.").

[10] *See* Ohm, *supra* note 8, at 378–385.

[11] *See id.*; Matthew Tokson, *The Emerging Principles of Fourth Amendment Privacy*, 88 GEO. WASH. L. REV. (forthcoming 2020).

[12] *Carpenter*, 138 S. Ct. at 2223.

[13] *See, e.g.*, United States v. Hood, 920 F.3d 87, 92 (1st Cir. 2019); Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 527 (7th Cir. 2018); United States v. Kidd, 394 F. Supp. 3d 357, 358–59, 365–66 (S.D.N.Y. 2019); United States v. Maclin, 393 F. Supp. 3d 701, 708 (N.D. Ohio 2019); United States v. Diggs, 385 F. Supp. 3d

inescapability as an important factor for determining Fourth Amendment protection, along with the revealing and extensive nature of the surveillance at issue.[14] Others have argued that inescapability should be an absolute requirement for the Fourth Amendment to apply.[15] While disagreements remain, early interpretations of *Carpenter* generally place inescapability at the center of Fourth Amendment privacy going forward.[16]

This Article challenges the idea that inescapability is a coherent or normatively defensible basis for Fourth Amendment protection. Inescapability has several theoretical and practical flaws that existing accounts of the concept have overlooked. This Article offers the first detailed analysis of this new concept, exploring its theoretical underpinnings, its doctrinal structure, and its policy implications. It finds that the use of inescapability as a Fourth Amendment standard would lead to serious administrability problems and the underprotection of privacy in personal electronic data. The Article examines these issues in depth and interrogates the prevailing wisdom that inescapability is a viable model for Fourth Amendment law.

Inescapability is conceptually ambiguous. It cannot be taken literally, because virtually all information disclosures are escapable with sufficient effort. Internet data, for instance, can often be kept from third-party observation by using widely available software or by opting out of information collection.[17] Consumers can also bargain for greater privacy

---

648, 660–61 (N.D. Ill. 2019); United States v. Tolbert, No. 14-3761-JCH, 2019 WL 2006464 (D.N.M. May 7, 2019); United States v. Therrien, No. 2:18-CR-00085, 2019 WL 1147479 (D. Vt. Mar. 13, 2019); State v. Martinez, 570 S.W.3d 278, 288 (Tex. Crim. App. 2019); State v. Leonard, 923 N.W.2d 52, 57 (Minn. Ct. App. 2019). For additional cases and discussion, see *infra* subpart I.D.

[14] *See, e.g.*, Aaron L. Dalton, Carpenter v. United States*: A New Era for Protecting Data Generated on Personal Technology, or a Mere Caveat?*, 20 N.C. J.L. & TECH. ONLINE 1, 23 (2018); Ohm, *supra* note 8, at 376–78.

[15] *See* Orin S. Kerr, *Implementing* Carpenter, *in* THE DIGITAL FOURTH AMENDMENT (forthcoming 2020) (manuscript at 20), https://ssrn.com/abstract=3301257 [https://perma.cc/RUR4-2JBU].

[16] *See infra* subparts I.C–I.D; *see also* Evan Caminker, *Location Tracking and Digital Data: Can* Carpenter *Build a Stable Privacy Doctrine?*, 2018 SUP. CT. REV. 411, 451 (noting residual uncertainty about the role of inescapability while emphasizing its importance).

[17] *See infra* notes 100–104 and accompanying text.

protections, at least in theory.[18] Even when applied nonliterally, an inescapability standard puts individuals asserting privacy rights at a strategic disadvantage.[19]

Further, a more nuanced inescapability standard would be difficult to apply accurately. Courts could try to determine precisely how escapable a given technology is, granting protection whenever avoiding the technology is sufficiently difficult. But this would be an ambiguous and fact-heavy inquiry, with results that would change over time as technologies and social practices change. Such a standard would make adjudication more costly and less predictable while offering little offsetting benefit.[20] Adding to the confusion, it would also conflict with longstanding precedents still in force.[21]

The society-wide scope of the inescapability inquiry also threatens to overlook individual differences among users. A technology that most people can easily escape may be inescapable for others. For example, while ride-sharing apps might be avoidable for most people, they may be indispensable for disabled persons or those who cannot afford a car and lack access to public transit.[22] Failing to take individual differences into account is a serious flaw in existing concepts of inescapability. Yet varying Fourth Amendment protection among individuals based on their unique circumstances is not viable either—it would create massive administrability problems for courts and legal actors.

Concerns about inescapability extend beyond these conceptual and practical issues. Perhaps most seriously, an inescapability standard creates socially harmful incentives. It motivates consumers to avoid escapable technologies that collect information, lest they lose their privacy rights. But those technologies are often beneficial, and incentivizing people to avoid them creates substantial social harm. Optional technologies such as smart devices, dating apps, and navigation services can confer potentially enormous

[18] *See infra* notes 105–107 and accompanying text.
[19] *See infra* notes 108–109 and accompanying text.
[20] *See infra* notes 118–120 and accompanying text.
[21] *See infra* subpart II.D.
[22] *See infra* section II.A.3.

benefits on their users.[23] Deterring consumers from using such technologies would be disastrous. Yet if consumers continue to use these technologies, they may face comprehensive government surveillance unchecked by the Fourth Amendment.

This is especially concerning because inescapability fails to protect many forms of sensitive information. Optional technologies frequently capture intimate forms of data. Internet connected beds, wearable devices, and other "smart" items can record and transmit deeply personal details about people's lives.[24] DNA analysis services, dating apps, and other optional services can obtain sensitive information about an individual's biological and psychological traits.[25] An inescapability standard may leave this data exposed, while often requiring a warrant for far less sensitive data.[26] Inescapability fails to draw a normatively defensible line between protected and unprotected forms of digital information.

In light of these issues, this Article examines several alternative approaches that avoid reliance on inescapability. When the Supreme Court addresses the Fourth Amendment again, it might overtly reject inescapability and embrace factors like the intimacy, amount, and cost of surveillance, which find ample support in prior Fourth Amendment cases.[27] Or, it might adopt a more novel approach. In recent years, scholars have proposed looking to positive law, survey data, historical practice, or normative balancing in order to draw the boundaries of the Fourth Amendment. This Article analyzes these approaches and finds that most of them offer a more coherent and protective standard than inescapability.

In the meantime, lower courts applying *Carpenter* can plausibly

---

[23] *See infra* subpart II.B. Even the Furbo dog camera has substantially benefitted homeowners and their pets in some situations, including break-ins and medical emergencies. *Furbo's Barking Alerts Save Dogs from Fires and Gas Leaks*, FURBO, https://shopus.furbo.com/pages/save-dog-lives [https://perma.cc/MP6Q-GE7M?type=image] (last visited July 28, 2020).

[24] *See infra* notes 155–158 and accompanying text.

[25] *See infra* notes 140–144, 158 and accompanying text.

[26] *See infra* subpart II.C.

[27] *See* Tokson, *supra* note 11, at 13–26 (analyzing the more universal principles of intimacy of information sought, amount of information sought, and cost of surveillance).

minimize inescapability, while focusing on the other important factors identified in *Carpenter*—the revealing and extensive nature of surveillance.[28] Indeed, some lower courts have already begun to do so.[29] This interpretive process can help shape Supreme Court doctrine and point the way toward a more effective standard for Fourth Amendment protection.[30]

Part I of the Article describes the doctrinal and theoretical foundations of inescapability. It discusses the *Carpenter* case and examines how scholars and lower courts have endorsed inescapability as a determinant of the Fourth Amendment's scope. Part II challenges the premises of inescapability, detailing the conceptual, practical, and normative weaknesses of an inescapability standard. It also describes the doctrinal conflicts and the socially harmful incentives that inescapability would create. Part III analyzes several potential alternative regimes for setting the boundaries of the Fourth Amendment. It offers a roadmap for lower courts to minimize the use of inescapability when applying *Carpenter* and explores how both courts and scholars can effectively shape Fourth Amendment law going forward.

I. THE RISE OF INESCAPABILITY

This Part tracks the emergence of inescapability as a determinant of Fourth Amendment protection. Doctrinal concepts of privacy and voluntary disclosure laid the foundations for inescapability. The Supreme Court then analyzed inescapability in a landmark case involving cell phone tracking. Many scholars and lower courts have since adopted the concept of inescapability in applying the Fourth Amendment to new surveillance technologies. This Part examines each of these developments in turn.

A. The Third-Party Doctrine

The Supreme Court has held that a Fourth Amendment search occurs

[28] *See infra* subpart III.A.
[29] *See infra* note 93 and accompanying text.
[30] *See infra* notes 197–206.

when a government official physically intrudes on certain types of property[31] or violates a person's "reasonable expectation of privacy."[32] The Court has not clearly explained what makes an expectation of privacy reasonable, and it has given several conflicting interpretations of the standard.[33] It has been relatively clear, however, in addressing data that individuals reveal to other parties. In the 1970s, the Court developed the "third-party doctrine," which provides that a person waives their Fourth Amendment rights in information they voluntarily disclose to a third party.[34] For example, the Fourth Amendment does not apply to the phone numbers that a person dials, because they have disclosed those numbers to the phone company.[35] The

---

[31] *See* Florida v. Jardines, 569 U.S. 1, 7–10 (2013); United States v. Jones, 565 U.S. 400, 404-06 (2012). The physical intrusion test has so far added little to the reasonable expectation of privacy test, and the Supreme Court cases where it has been used may have come out similarly under *Katz v. United States*, 389 U.S. 347 (1967). *Jardines,* 569 U.S. at 12–16 (Kagan, J., concurring); *Jones*, 565 U.S. at 418–31 (Alito, J., concurring in judgment).

[32] This standard is often referred to as the *Katz* test, having first appeared in Justice Harlan's concurrence in 1967's *Katz v. United States*. 389 U.S. at 361. The Court has not fully defined the concept of a reasonable expectation of privacy, and scholars have interpreted the standard in different ways. *See* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 508 (2007) (positing that the Court applies multiple, conflicting models of the Fourth Amendment in different cases); Tokson, *supra* note 11, at 12 (contending that the Court applies an intuitive model of Fourth Amendment searches that looks to the intimacy, amount, and cost of the surveillance practice at issue).

[33] Kerr, *supra* note 32. In some cases, the Court looks to the probability that a person's privacy will be violated. *Id.* at 508–10. In others, it looks to other sources of law, to the private nature of the thing searched, or to the policy implications of the surveillance. *Id.* at 512–22.

[34] Cases holding that the Fourth Amendment did not apply to statements made to an undercover officer predate the reasonable expectation of privacy test, although the third-party doctrine itself was not established in its full form until the 1970s. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (concluding that a list of dialed phone numbers was not protected by the Fourth Amendment); United States v. Miller, 425 U.S. 435, 444–45 (1976) (holding that a bank customer had no reasonable expectation of privacy in his records because they were disclosed to third-party employees); Hoffa v. United States, 385 U.S. 293, 302 (1966) (ruling that testimony regarding statements to a secret government informant was allowable under the Fourth Amendment); Lopez v. United States, 373 U.S. 427, 437–40 (1963) (holding that an electronic recording device that was not unlawfully planted by physical invasion did not violate defendant's Fourth Amendment rights).

[35] *Smith*, 442 U.S. at 743–46.

police can accordingly obtain a list of anyone's dialed numbers without a warrant or probable cause.

The concept of voluntary disclosure is central to the third-party doctrine.[36] The earliest third-party doctrine cases involved suspects voluntarily sharing details of their crimes with government informants or undercover agents.[37] The Court held that the Fourth Amendment does not protect a person who "voluntarily confides his wrongdoing" to another.[38] The Court then expanded the doctrine to cover financial records and phone numbers disclosed to businesses.[39]

In the internet era, the third-party doctrine threatens to eliminate privacy protections for a vast swath of personal information, including web surfing data, cloud-stored documents, medical and biometric data, and location information.[40] These and many other forms of digital information are regularly disclosed to third-party service providers.[41] Accordingly, government investigators may be able to obtain enormous quantities of personal information without a warrant.[42]

---

[36] *Id.* at 742–45; *Miller*, 425 U.S. at 435, 442; United States v. White, 401 U.S. 745, 749 (1971) (plurality opinion).

[37] *White*, 401 U.S. at 746–47; *Lopez*, 373 U.S. at 428–29.

[38] *White*, 401 U.S. at 749 (quoting *Hoffa*, 385 U.S. at 302).

[39] *Miller*, 425 U.S. at 442 ("All 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."). Likewise, telephone customers, who know that telephone companies receive and record the numbers they dial, voluntarily disclose those numbers to their service provider and therefore waive any Fourth Amendment right in the numbers. *Smith*, 442 U.S. at 744 ("When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed.").

[40] *See, e.g.*, Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 585 (2011) (noting that third-party doctrine precedents are problematic in an age where individuals store enormous amounts of personal information on various third-party platforms).

[41] *See id.*; *see also* Tokson *supra* note 11, at 53.

[42] Such data is regularly stored in databases and made available to the government upon request or subpoena. *See* Tokson, *supra* note 40, at 585.

The third-party doctrine has been widely criticized,[43] and the Supreme Court has not applied it in a case since 1979.[44] Several states have repudiated the doctrine via constitutional or statutory law,[45] and Justice Sotomayor criticized it in an influential concurrence in *United States v. Jones*.[46] Yet most lower courts continued to vigorously enforce the doctrine in cases involving email to/from data, IP addresses, cell phone data, and more.[47] As government surveillance of digital information held by third parties proliferated, it became clear that the Supreme Court would have to reexamine the third-party doctrine and its application to new technologies.[48]

---

[43] *See, e.g.*, CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 151–64 (2007) (critiquing the third-party doctrine in the context of third-party subpoenas); Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 19–20 (2008) (characterizing Fourth Amendment protections for personal data as weak due to the third-party doctrine); Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975, 976–77 (2007) (contending that the third-party doctrine is one of the most serious threats to privacy in the digital age); Neil Richards, *The Third-Party Doctrine and the Future of the Cloud*, 94 WASH. U. L. REV. 1441, 1475–80 (2017) (asserting that the third-party doctrine as applied in a digital context undermines the core values of the Fourth Amendment).

[44] *Smith*, 442 U.S. 735 (1979).

[45] *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, 395–405 (2006) (reporting numerous states that have rejected the third-party doctrine in whole or in part, including California, New Jersey, and Pennsylvania, among others).

[46] United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring). In *Jones,* the Court held that attaching a GPS tracking device to the underside of a car was a Fourth Amendment search that required a valid warrant. *Id.* at 404.

[47] *See, e.g.*, *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (ruling that cell site data is not protected under the Fourth Amendment); United States v. Warshak, 631 F.3d 266, 330–31 (6th Cir. 2010) (finding that the third-party doctrine applies to e-mail metadata such as to/from addresses); United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2008) (holding that email to/from addresses and IP addresses are not searches according to the third-party doctrine); Freedman v. Am. Online, Inc., 412 F. Supp. 2d 174, 182–83 (D. Conn. 2005) (holding that there is no reasonable expectation of privacy in AOL subscriber information when the user permitted AOL to release the information to third parties).

[48] *See generally* Stephen E. Henderson, *After* United States v. Jones*, After the Fourth Amendment Third Party Doctrine*, 14 N.C. J.L. & TECH. 431, 432–33 (2013) (recounting

B. *Carpenter* and Cell Phone Tracking

Several times per minute, a cell phone emits radio waves that communicate with the antennae on cell phone towers.[49] Cell phone companies generally track which antennae and which towers receive a cell phone's signal. By doing so, they can generate a record of the user's location over time. They collect and store this data for various purposes, including network maintenance and applying roaming charges. They also sell this data to third parties for use in marketing and analytics.[50]

Over the past two decades, law enforcement officials have frequently sought to obtain cell phone location data for use in criminal investigations.[51] Lower courts mostly approved this tactic, holding that the Fourth Amendment did not apply to such data because users had knowingly exposed it to their cell phone companies.[52] Scholars and other observers were alarmed, raising concerns about pervasive, low-cost location tracking by the government.[53] After several federal appeals courts had weighed in, the Supreme Court decided to review a case where the government used cell

---

the history and application of the third-party doctrine and speculating that the changing nature of technology will require the Supreme Court to limit or avoid the doctrine).

[49] Carpenter v. United States, 138 S. Ct. 2206, 2211–12 (2018).

[50] *See id.* For further discussion of cell site location information (CSLI) and cell phone provider data retention practices, see Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 NW. U. L. REV. 139, 160–61 (2016).

[51] *See* Tokson, *supra* note 50, at 159.

[52] Indeed, the federal courts of appeal were virtually unanimous in declaring that cell phone location information could be obtained without a warrant. *See, e.g.*, United States v. Graham, 824 F.3d 421, 424 (4th Cir. 2016) (en banc); United States v. Davis, 785 F.3d 498, 511 (11th Cir. 2015) (en banc); *In re* Application of U.S. for Historical Cell Site Data, 724 F.3d 600, 612 (5th Cir. 2013). *But cf. In re* Application of 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) (stating that "it is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information" while resolving the case based on a statutory interpretation influenced by constitutional analysis).

[53] Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 709 (2011); Tokson, *supra* note 50, at 183; *Who Has Your Back?*, ELEC. FRONTIER FOUND., (2013), https://www.eff.org/who-has-your-back-2013?support_whyb=1&social=1 [https://perma.cc/8DPV-X8YQ].

phone location data to place a suspect at the scene of several robberies.[54]

In *Carpenter v. United States*, the Court held that the government's warrantless acquisition of Carpenter's cell phone location data violated the Fourth Amendment.[55] The Court expressly limited the third-party doctrine, making it inapplicable to cell phone location data stored by a third party. Cell phone tracking was so revealing, detailed, and low in cost that it "implicate[d] privacy concerns far beyond" those considered in previous cases.[56] Tracking a cell phone for long periods of time provides an all-encompassing record of an owner's activities.[57] It opens an "intimate window into a person's life," potentially revealing his familial, political, professional, religious, and sexual associations.[58] Such tracking is also "remarkably easy, cheap, and efficient," capable of accessing vast repositories of personal data at little cost to government inspectors.[59]

Moreover, the surveillance at issue was practically "inescapable."[60] Cell phones have become "such a pervasive . . . part of daily life that carrying one is indispensable to participation in modern society."[61] And cell phones transmit location data to service providers automatically, such that users have no opportunity to opt out. Accordingly, cell phone users do not voluntarily give up their information—they have no real choice but to disclose their location data to their service providers. Indeed, there was no feasible way to avoid the technology or to use it differently that would allow people to escape

---

[54] *Carpenter*, 138 S. Ct. at 2212–13.

[55] *Id.* at 2221, 2223.

[56] *Id.* at 2220. Cell phone records contain vast stores of historical location data and potentially allow the police to track suspects "every moment of every day for five years." *Id.* at 2218. Virtually every American could be tracked at any time. *Id.* ("Critically, because location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone."). And the cost of such monitoring had drastically decreased, removing an important barrier to excessive location tracking by the government. *Id.* at 2217 (quoting United States v. Jones, 565 U.S. 400, 429 (Alito, J., concurring)).

[57] *Id.* at 2217.

[58] *Id.*

[59] *Id.* at 2217–18.

[60] *Id.* at 2223.

[61] *Id.* at 2220 (internal quotation marks omitted).

disclosure.[62] For all of these reasons, the Court declined to extend the third-party doctrine to cell phone location information.

Carpenter is a landmark Fourth Amendment decision—it establishes a foundation for Fourth Amendment privacy in shared digital information. It limits the third-party doctrine and refines the concept of voluntary disclosure. At a minimum, when an information-collecting technology is inescapable, revealing, and comprehensive, the Court will no longer hold that using it eliminates a person's Fourth Amendment rights. Yet the Court's use of inescapability in its Fourth Amendment analysis threatens to undermine meaningful privacy protections for many forms of digital data. As an inescapability standard gains support among scholars and lower courts, its weaknesses have gone mostly overlooked.

C. Theories of Inescapability

The *Carpenter* decision represents a momentous change in Fourth Amendment law. But the precise contours of that change remain unclear. The Court's opinion is notably ambiguous,[63] and it does not directly apply its rationale to any form of information other than historical cell site data.[64] As with many major decisions, *Carpenter*'s meaning will ultimately emerge from lower court interpretations, scholars' analyses, and the Court's future cases.[65]

---

[62] *See id.* at 2211–12, 2220.

[63] *See, e.g.*, Caminker, *supra* note 16, at 451–53; Dalton, *supra* note 14, at 23; Laura K. Donohue, *Functional Equivalence and Residual Rights Post-*Carpenter: *Framing a Test Consistent with Precedent and Original Meaning*, 2018 SUP. CT. REV. 347, 372; Lior Strahilevitz & Matthew Tokson, *Ten Thoughts on Today's Blockbuster Fourth Amendment Decision*—Carpenter v. United States, CONCURRING OPINIONS (June 22, 2018), https://web.archive.org/web/20180721111755/https://concurringopinions.com/archives/2018/06/ten-thoughts-on-todays-blockbuster-fourth-amendment-decision-carpenter-v-united-states.html [https://perma.cc/U8UH-VHVG?type=image].

[64] *Carpenter*, 138 S. Ct. at 2206, 2220.

[65] *See* Caminker, *supra* note 16, at 460. The meaning of *Katz v. United States*, the landmark decision that first applied the Fourth Amendment to intangible things like telephone conversations, only emerged over time as subsequent cases interpreted and applied *Katz*. *Katz v. United States*, 389 U.S. 347 (1967); *see, e.g.*, Oliver v. United States, 466 U.S. 170, 178 (1984) (clarifying that a Fourth Amendment search occurs when a

In general, inescapability doctrine can be theorized as based in concepts of fairness. It is less fair to eliminate a person's privacy rights on the basis of their disclosure of information when that disclosure could not have reasonably been avoided.[66] In addition, when disclosure is inescapable, a person cannot be said to have assumed the risk of the government obtaining the disclosed information.[67] Nor has the person made a fully voluntary choice to reduce their privacy.[68]

Many scholars place inescapability at the core of Fourth Amendment law going forward, although their specific approaches vary.[69] Some have interpreted *Carpenter* as establishing a multi-factor test in which inescapability is an important factor.[70] For example, Paul Ohm posits that *Carpenter* creates a broadly applicable test that examines 1) how revealing the information is; 2) its depth, breadth, and comprehensive reach, and

---

government act violates an individual's "reasonable expectation of privacy"); United States v. Guadalupe-Garza, 421 F.2d 876, 878 (9th Cir. 1970) (considering whether defendant had a "reasonable 'expectation of privacy'" when crossing the border from Mexico to California (quoting Terry v. Ohio, 392 U.S. 1, 9 (1968))); Terry v. Ohio, 392 U.S. 1, 9 (1968) ("We have recently held that . . . wherever an individual may harbor a reasonable 'expectation of privacy,' he is entitled to be free from unreasonable government intrusion." (quoting *Katz*, 389 U.S. at 361 (Harlan, J., concurring))); *see also, e.g.*, Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 384 (1974) (providing early analysis of the *Katz* test and noting the largely objective and normative nature of the test); William C. Heffernan, *Fourth Amendment Privacy Interests*, 92 J. CRIM. L. & CRIMINOLOGY 1, 37 (2001) (describing how the Court looks to social norms and practices to identify reasonable expectations of privacy).

[66] *See* Laura Moy, *The Underappreciated Role of Avoidability in U.S. Privacy Law* (unpublished manuscript) (on file with author).

[67] *Cf.* Smith v. Maryland, 442 U.S. 735, 744 (1979) (stating that the voluntary disclosure of information was an assumption of risk of further disclosure).

[68] *See* Ari Ezra Waldman, *Durkheim's Internet: Social and Political Theory in Online Society*, 7 N.Y.U. J.L. & LIBERTY 345, 409–10 (2013) (describing the concept of constructive involuntariness in the context of internet use).

[69] *See infra* notes 70–78 and accompanying text. Laura Donohue has criticized the Court's use of voluntariness concepts in *Carpenter* as part of her proposal for a property-based Fourth Amendment along the lines of Justice Gorsuch's *Carpenter* dissent. *See* Donohue, *supra* note 63, at 381–82. She argues that information created and stored by others due to a consumer's actions, such as cell phone location data, should be considered the consumer's property for Fourth Amendment purposes. *Id.* at 388–99.

[70] *See, e.g.*, Dalton, *supra* note 14, at 22; Ohm, *supra* note 8, at 369.

3) whether exposure of the information is inescapable.[71] Information is revealing when it is intimate or otherwise sensitive and its disclosure is likely to harm the individuals involved.[72] Depth, breadth, and comprehensive reach generally refer to the precision of the information, the duration of observation, and the number of people observed. With regard to inescapability, Ohm explains that "[s]ome forms of data collection are inescapable because they relate to services one needs to use to be a functioning member of today's society."[73] He also describes the intertwined concept of automatic information collection, which occurs when data is inevitably generated by a product or service and consumers have no opportunity to opt out. Ohm sees inescapability as a key factor to be weighed in each case rather than an ironclad requirement for Fourth Amendment protection.[74]

By contrast, Orin Kerr views inescapability as an absolute prerequisite for Fourth Amendment protection in data held by third parties.[75] He contends that *Carpenter* limited the third-party doctrine largely on the ground that people have no choice but to disclose their location information to cell phone providers.[76] Going forward, courts must determine whether individuals have a meaningful choice to refrain from certain activities or information disclosures. Information that is inevitably shared is safeguarded. But when consumers venture "beyond what the technology requires" for participation in modern life, their data is not protected.[77] Other scholars have noted the ambiguity of the *Carpenter* standard while emphasizing the central importance of inescapability to whichever standard ultimately

---

[71] Ohm, *supra* note 8, at 369–70. Ohm views this test as applicable in virtually all surveillance cases, not just those involving data held by third parties. *Id.* at 392–93.
[72] *Id.* at 371–73.[73] *Id.* at 376–77 (emphasis omitted).
[73] *Id.* at 376–77 (emphasis omitted).
[74] *See id.* at 380, 382–83 (weighing inescapability as an important but not essential factor in a multi-factor test).
[75] Kerr, *supra* note 15, at 20 ("This requirement . . . comes from *Carpenter* itself."); *id.* at 21 ("*Carpenter* has a compulsion requirement."); *see* Caminker, *supra* note 16, at 451 (noting the possibility of an inescapability requirement).
[76] Kerr, *supra* note 15, at 20–21.
[77] *Id.* at 22.

emerges.[78] Currently, the dominant conceptual frameworks for post-*Carpenter* Fourth Amendment law rely heavily on inescapability to determine privacy rights.

D. Inescapability in the Lower Courts

Many lower courts consider inescapability a core determinant of Fourth Amendment protection after *Carpenter*. These courts generally use inescapability as an important factor in applying *Carpenter*, and some regard it as essential to Fourth Amendment protection. However, lower courts' applications of *Carpenter* are hardly uniform or settled.[79] While the precise contours of post-*Carpenter* doctrine remain in flux, the inescapability of information disclosure is likely to play a major role in Fourth Amendment law going forward.

Numerous cases applying *Carpenter* have found that individuals lack a Fourth Amendment right in information disclosed as part of an optional or escapable activity. For example, in *United States v. Hood*, the First Circuit held that the government could warrantlessly collect a user's IP address data associated with a messaging app.[80] The court reasoned that the app was purely optional and thus people easily "could escape" any surveillance associated with the app.[81] In *United States v. Kidd*, a federal district court likewise held that the government could warrantlessly obtain IP address data associated with a cell phone service, even though this data might reveal a user's location for a period of 581 days.[82] The court concluded that the

---

[78] *See* Caminker, *supra* note 16, at 451 (positing that the Court may impose inescapability as a requirement while acknowledging the possibility that it may be only a factor).

[79] Some courts have largely ignored inescapability and focused on the other factors identified in *Carpenter*, especially the revealing and extensive nature of the data sought. *See infra* note 93.

[80] United States v. Hood, 920 F.3d 87, 92 (1st Cir. 2019).

[81] *Id.* (quoting United States v. Carpenter, 138 S. Ct. 2206, 2218 (2018)). The court likewise noted that the app only generated IP address information when the user made "the affirmative decision to access [the] website or application." *Id.*

[82] *See* United States v. Kidd, 394 F. Supp. 3d 357, 358–59, 365–66 (S.D.N.Y. 2019) (discussing the potential for cell phone IP address information to reveal location, although noting that it is generally less revealing than CSLI data).

service, which provided voice-over-internet-protocol (VOIP) phone calls, was not "ubiquitous" or inescapable and it therefore received less Fourth Amendment protection.[83] In *United States v. Sigouin*, a magistrate judge found that requesting files via a peer-to-peer service was not "indispensable to participation in modern society" like cell phone use, but was entirely voluntary and avoidable.[84] Accordingly, the government could record an internet user's peer-to-peer requests without a warrant.[85] In *United States v. Cox*, the judge ruled that the FBI could obtain Facebook activity records because the defendant had not established that Facebook was ubiquitous or "as indispensable as the cell phone" and because record generation "require[s] affirmative action by the user."[86] In *United States v. Morel* and several other cases, circuit and district courts have held that subscriber information was unprotected because, unlike cell phone location data, an individual affirmatively chooses to provide it to an internet service.[87] State courts have

[83] *Id.* at 365–67. The court noted that the data collection might violate the Fourth Amendment if the defendant could demonstrate that the data collection was automatic and thus inescapable or that the location data collected was detailed and extensive. *Id.* at 367–68.

[84] United States v. Sigouin, No. 19-80136-CR, 2019 WL 7373045, at *6 (S.D. Fla. Dec. 19, 2019) (quoting *Carpenter*, 138 S. Ct. at 2220), *report and recommendation adopted*, No. 9:19-CR-80136, 2019 WL 7372958 (S.D. Fla. Dec. 31, 2019).

[85] *Id.* at *7; *see also* United States v. Shipton, No. 0:18-CR-202-PJS-KMM, 2019 WL 5330928, at *14 (D. Minn. Sept. 11, 2019) (concluding that "[t]he P2P software user makes an intentional choice to connect to a network and has deliberately selected the files she is willing to share in a designated folder" and therefore "[t]he peer-to-peer file sharer plainly assumes the risk that anyone using the software could see the files she is sharing while a cell phone user has not engaged in any sort of comparable voluntary act"), *report and recommendation adopted*, No. 18-CR-0202 (PJS/KMM), 2019 WL 5305573 (D. Minn. Oct. 21, 2019).

[86]United States v. Cox, No. 1:18-CR-83-HAB, 2020 U.S. Dist. LEXIS 97326, at *6, *10 (N.D. Ind. June 3, 2020).

[87] *Id.*; United States v. Morel, 922 F.3d 1, 9 (1st Cir. 2019) ("[A]n internet user generates the IP address data . . . only by making the affirmative decision to access a website or application." (alteration in original) (quoting United States v. Hood, 920 F.3d 87, 92 (1st Cir. 2019)); United States v. Maclin, 393 F. Supp. 3d 701, 708 (N.D. Ohio 2019) ("Subscriber information requires an individual's active participation – the subscriber only captures information when the platform is used."); United States v. Tolbert, No. 14-3761 JCH, 2019 WL 2006464, at *3 (D.N.M. May 7, 2019) ("[T]he subpoenaed data appears to have been generated from Tolbert's own affirmative actions in utilizing CenturyLink

likewise held that information that a defendant could have withheld but nonetheless disclosed when he entered into a transaction was not protected by the Fourth Amendment.[88]

Other cases have upheld Fourth Amendment rights because the surveillance at issue was automatic or otherwise inescapable. In *Naperville Smart Meter Awareness v. City of Naperville*, the Seventh Circuit held that a city's collection of data from its citizens' smart utility meters was a Fourth Amendment search.[89] Citizens had "no choice at all" but to install the required meters and therefore did not voluntarily disclose their data.[90] In *United States v. Diggs*, the federal district court held that GPS data generated by a device installed before the sale of a vehicle was protected by the Fourth Amendment because the data disclosure was involuntary and occurred without the owner's knowledge.[91] In *State v. Martinez*, the government's testing of a patient's blood sample violated the Fourth Amendment because the patient did not voluntarily give his blood to be tested and could not have avoided having his blood drawn.[92]

To be sure, not all lower court cases applying *Carpenter* rely on inescapability. Some cases instead focus on other factors, such as the revealing and extensive nature of the data at issue.[93] The tension between

---

and AOL, and in this way is distinguishable from the CSLI data in *Carpenter*."); United States v. Therrien, No. 2:18-CR-00085, 2019 WL 1147479, at *2–3 (D. Vt. Mar. 13, 2019) ("In this case, law enforcement obtained information that an account holder voluntarily turned over to Google.").

[88] State v. Leonard, 923 N.W.2d 52, 57–58 (Minn. Ct. App. 2019) (holding that appellant lacked a Fourth Amendment right in the information he gave when securing a hotel room because, unlike a cell phone user, he "chose . . . to provide identifying information to the hotel as a means of securing a hotel room").

[89] Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 527 (7th Cir. 2018).

[90] *Id.*

[91] United States v. Diggs, 385 F. Supp. 3d 648, 660–61 (N.D. Ill. 2019).

[92] State v. Martinez, 570 S.W.3d 278, 288 (Tex. Crim. App. 2019) (evaluating voluntariness and explaining that the patient was incoherent when hospitalized and was unable to consent to or refuse the blood draw).

[93] United States v. Howard, No. 1:19-CR-54-WKW, 2019 WL 6048885, at *6 (M.D. Ala. Nov. 15, 2019) (holding that one-day warrantless GPS tracking did not violate the Fourth Amendment because it was shorter in duration and less revealing than cell phone tracking);

these cases and the cases that depend on inescapability highlights the uncertain nature of Fourth Amendment law post-*Carpenter*. Nonetheless, numerous courts and several prominent scholars have relied on inescapability, and it appears likely to shape Fourth Amendment law for years to come. The next Part casts a critical eye on this development and identifies several reasons to doubt that inescapability can function effectively as a determinant of Fourth Amendment protection.

II. CHALLENGING THE PREMISES OF INESCAPABILITY

This Part questions the conventional account of inescapability in Fourth Amendment law. It examines the theoretical, practical, and normative flaws of inescapability as a Fourth Amendment standard. Inescapability is conceptually ambiguous and difficult for courts to assess. It does a poor job of protecting the most intimate forms of personal electronic data. Further, the incentives that an inescapability standard creates would cause substantial social harm, as consumers either forego beneficial technologies or lose privacy rights in their personal information. Finally, it would create doctrinal confusion because several longstanding Fourth Amendment precedents conflict with the inescapability model. This Part analyzes these issues and challenges the premise that inescapabilty is an effective paradigm for Fourth Amendment protection.

United States v. Kelly, 385 F. Supp. 3d 721, 726–27 (E.D. Wis. 2019) (holding that the government could warrantlessly capture video from the hallway of an apartment building which was not the defendant's residence because the camera collected little information and the information captured was not sensitive); United States v. Jenkins, No. 1:18-CR-181-MLB-CMS, 2019 WL 2482171, at *2 (N.D. Ga. Feb. 5, 2019) (finding that the basic subscriber information associated with a user's internet accounts was less revealing and involved far less data than cell phone tracking, and was therefore not a Fourth Amendment search), *report and recommendation adopted*, No. 1:18-CR-00181, 2019 WL 1568154 (N.D. Ga. Apr. 11, 2019); People v. Tafoya, 2019 COA 176, ¶¶ 42–48 (ruling that video surveillance of the curtilage of a suspect's home for a three-month period violated the Fourth Amendment because such monitoring captured a great deal of information over time and could reveal sensitive details about a person's life). These opinions do not overtly reject the concept of inescapability, but they do resolve novel Fourth Amendment questions without addressing it.

A. Conceptual and Practical Issues

The first set of issues surrounding inescapability involve the difficulty of defining it as a concept or assessing it in real-world cases. Inescapability cannot be taken literally because virtually all forms of information disclosure are avoidable in theory. On the other hand, a more nuanced inquiry into how escapable a technology is would create severe administrability problems and doctrinal unpredictability. In addition, the society-wide nature of the inescapability inquiry overlooks individual differences and ignores disadvantaged and disabled individuals. This section explores these issues.

1. Everything Is Escapable in Theory

An "inescapability" standard for Fourth Amendment protection is conceptually problematic. It cannot mean what it says. Virtually every form of digital surveillance is escapable with sufficient effort. Technologies regularly arise that allow users to avoid surveillance as they use the internet or communicate electronically with each other.[94] Even unavoidable disclosures to third parties can be bargained around, at least in theory.[95]

Take internet data, for example. Internet use is a central part of modern life.[96] Records of the websites that a user visits are often collected by the user's internet service provider (ISP)[97] or by affiliated groups of websites that collect the URLs of each page a user sees within their group.[98] Because these

---

[94] *See infra* notes 100–104 and accompanying text.
[95] *See infra* notes 105–107 and accompanying text.
[96] Kerr, *supra* note 15, at 47.
[97] Peter Segrist, *How the Rise of Big Data and Predictive Analytics Are Changing the Attorney's Duty of Competence*, 16 N.C. J.L. & TECH. 527, 542–43 (2015); Matthew Tokson, *The Next Wave of Fourth Amendment Challenges After* Carpenter, 59 WASHBURN L.J. 1, 13 (forthcoming 2020). For instance, ISPs often maintain logs of the IP addresses of each website a user visits along with the volume of data transmitted to and from the user. *See* Tokson, *supra* note 40, at 603. Some ISPs retain the URL of each individual page visited by a user. Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417, 1424–25, 1432–38.
[98] *See, e.g.*, Omer Tene, *What Google Knows: Privacy and Internet Search Engines*, 2008 UTAH L. REV. 1433, 1447–48. In addition, some third-party entities place "web beacons" on affiliated websites that track in the user's activity on a particular site. Segrist, *supra* note

records are created whenever a user visits a website, revealing one's internet habits may seem inescapable.[99] But there are relatively low-cost steps that users can take to prevent the disclosure of their internet data.

Users can set up a Virtual Private Network to hide their internet activity from their ISP and remain largely anonymous as they surf the web.[100] They can use the well-known and free TorBrowser to hide their IP address and encrypt their web traffic.[101] They can simply opt out of Google's collection of their search term history.[102] And they can send messages through free services like TorMessenger, TorChat, SecureDrop, or other services that allow users to conceal their communications metadata and IP addresses.[103]

---

97. These various entities can use websurfing information to target advertisements to the individual user or sell the information to third-party advertisers. Tokson, *supra* note 40, at 603.

[99] *See* Kerr, *supra* note 15, at 47.

[100] For example, users can download the Express VPN app at https://www.expressvpn.com [https://perma.cc/SA5H-9X8X]. Note that websites may be able to compromise VPN-based anonymity via "fingerprinting"—the practice of tracking visitors to websites based on the unique characteristics of their computers such as screen resolution, internal network address, and downloaded fonts. *See* Geoffrey A. Fowler, *Think You're Anonymous Online? A Third of Popular Websites Are "Fingerprinting" You*, WASH. POST (Oct. 31, 2019), https://www.washingtonpost.com/technology/2019/10/31/think-youre-anonymous-online-third-popular-websites-are-fingerprinting-you/?arc404=true [https://perma.cc/B89L-F72X].

[101] Andy Greenberg, *The Grand Tor: How to Go Anonymous Online*, WIRED (Dec. 9, 2017), https://www.wired.com/story/the-grand-tor/ [https://perma.cc/B89L-F72X]. Tor browsers are also effective against "fingerprinting." *See* Fowler, *supra* note 100.

[102] Kristin Burnham, *5 Google Opt-Out Settings to Check*, INFORMATIONWEEK (Jan. 11, 2014), https://www.informationweek.com/software/social/5-google-opt-out-settings-to-check/d/d-id/1113405 [https://perma.cc/BPX9-BSWC] ("Unless you consistently delete it, Google tracks and logs all your web history, including your image, news, map, and video searches. You can remove all or some of your search history, or opt out of Google tracking you entirely."). Users could also use the DuckDuckGo search engine, which by default does not collect IP addresses or user information. DUCKDUCKGO, https://duckduckgo.com/privacy [https://perma.cc/NH3V-L388] (last visited July 28, 2020).

[103] *See* Greenberg, *supra* note 101; *see also* Dan Goodin, *New Signal Privacy Feature Removes Sender ID from Metadata*, ARS TECHNICA (Oct. 30, 2018, 1:00 AM), https://arstechnica.com/information-technology/2018/10/new-signal-privacy-feature-removes-sender-id-from-metadata/ [https://perma.cc/6D9X-E3DX] (noting that Signal will continue to map senders' IP addresses but will offer a service placing most user information inside the encrypted message rather than in the header).

Few internet users actually avail themselves of these options, perhaps because of concerns about cost, speed, or convenience, or because they are unaware of them.[104] But the disclosure of internet data to private parties is largely escapable, in theory.

To take this point even further, consider that users can in theory bargain with any service provider for more privacy, no matter how unavoidable the underlying technology may be.[105] In a Coasian world with no transaction costs, customers could simply pay their service providers to immediately delete any information collected about them.[106] Of course, this might be difficult to negotiate in the real world.[107] But it points up a conceptual failure

---

[104] *See, e.g.*, *Users*, TOR METRICS, https://metrics.torproject.org/userstats-relay-country.html?start=2019-11-07&end=2020-02-05&country=us&events=off [https://perma.cc/2JPA-N38K] (last visited Feb. 5, 2020) (displaying an estimate of roughly 800,000 American Tor users as of February 2020).

[105] Even cell phone tracking itself might in theory be avoided through bargaining. Typically, a user's location information is deleted after several years of storage. *See* United States v. Carpenter, 138 S. Ct. 2206, 2210 (2018); *Cell Phone Location Tracking Request Response—Cell Phone Company Data Retention Chart*, ACLU, https://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart [https://perma.cc/RT7D-5WLK] (last visited July 31, 2020). Hypothetically, nothing prohibits a cell phone user from paying their service provider to immediately delete any location information gathered from their cell phone. However, the cell phone companies contacted for this article either stated that they would not be willing to negotiate the deletion of user data (Sprint, Verizon) or declined to comment on the matter (AT&T, T-Mobile, U.S. Cellular). Note that it may be possible to avoid location tracking by purchasing a Blackphone or other VOIP-based phone and run it on Wi-Fi networks, avoiding cell signal disclosure entirely. *See* Jill Scharr, *Blackphone vs. FreedomPop's Privacy Phone: Security Showdown*, TOM'S GUIDE (Mar. 8, 2014), https://www.tomsguide.com/us/blackphone-vs-freedompop-privacy-phone,news-18427.html [https://perma.cc/R2Z9-4YXF]. While phones might be traced via Wi-Fi network, secure phones use a VPN to connect to the internet in order to preserve user anonymity. *Id.*; Martin Beltov, *Cell Phones Can Easily Be Traced via WiFi*, BEST SECURITY SEARCH, https://bestsecuritysearch.com/cell-phones-can-easily-traced-via-wifi [https://perma.cc/9EWH-28A7] (last visited July 31, 2020).

[106] The Coase theorem, developed by Nobel Prize winner Ronald Coase, posits that in a world with no transaction costs, initial allocations of property rights would not matter because parties would bargain efficiently to distribute property to the highest value user. *E.g.*, R. H. Coase, *The Problem of Social Cost*, 3 J.L. & ECON. 1, 1–2 (1960); Herbert Hovenkamp, *Marginal Utility and the Coase Theorem*, 75 CORNELL L. REV. 783, 783–84 (1990);.

[107] *See supra* note 105.

of the inescapability standard: everything is escapable, for a price.

This is not to say that every lower court judge will apply the inescapability standard literally. Many will take a more nuanced approach.[108] But there is serious risk in establishing a standard that, taken literally, would render the Fourth Amendment inapplicable to most forms of digital information. Lower courts often apply Fourth Amendment standards literally, even when doing so exposes sensitive information to government surveillance.[109] And judges applying a more lenient concept of inescapability will nonetheless be influenced by arguments demonstrating how feasible it is in many cases to avoid information disclosure. An inescapability standard puts individuals asserting privacy rights at a rhetorical and practical disadvantage.

2. Administrability Problems in Practice

Courts applying an inescapability standard might engage in a more subtle inquiry into precisely how escapable a given technology is.[110]

---

[108] *See infra* section II.A.2.

[109] For example, lower courts attempted to ascertain whether cell phone users had a reasonable expectation of privacy by trying to estimate their knowledge regarding how cell phones operate and the information disclosures inherent in cell phone use. United States v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2016) ("[A]ny cellphone user who has seen her phone's signal strength fluctuate must know that, when she places or receives a call, her phone 'exposes' its location to the nearest cell tower and thus to the company that operates the tower."); *In re* Application of U.S. for Historical Cell Site Data, 724 F.3d 600, 612 (5th Cir. 2013) ("[U]sers know that they convey information about their location to their service providers when they make a call . . . ."); *In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. §§ 2703(c)–(d), 42 F. Supp. 3d 511, 518 (S.D.N.Y. 2014) ("[S]ubscribers are aware that use of their cell phones necessitates disclosure of the information sought."); United States v. Madison, No. 11-60285-CR, 2012 WL 3095357, at *8 (S.D. Fla. July 30, 2012) (stating that it is "common knowledge that communications companies regularly collect and maintain all types of non-content information regarding cell-phone communications, including cell-site tower data, for cell phones for which they provide service"). Subsequent empirical studies found that most courts' estimates of societal knowledge were erroneous. *See* Tokson, *supra* note 50, at 176–79 (reporting survey results indicating that the vast majority of cell phone users were unaware that their phones could be tracked using cell phone signals).

[110] *See* Kerr, *supra* note 15, at 21.

Surveillance could be deemed inescapable whenever avoiding it would be sufficiently difficult or costly for the average consumer.[111] But this would be an ambiguous and fact-heavy inquiry, with results that would change over time as technologies and social practices change.[112] Making it a part of Fourth Amendment analysis would render adjudication more difficult and less predictable while providing minimal offsetting benefit.[113]

Consider the assessment of whether a technology is "indispensable to participation in modern society" and thus unavoidable.[114] Professor Kerr, interpreting *Carpenter*'s standard, envisions this as a "philosophical question" involving three further inquiries: "First, what does modern society look like; second, what does it mean to participate in that society; and third, what technologies are needed to achieve that participation."[115] These are difficult, abstract questions bound up with complex technological and sociological issues. Such questions may be especially difficult for courts to resolve effectively.[116] Indeed, many lower court rulings on inescapability post-*Carpenter* reach questionable conclusions about whether individuals can actually avoid the use of certain technologies or practices.[117]

---

[111] *Cf.* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (discussing the ubiquity of cell phones and their indispensable nature in modern society).

[112] As the petitioner's brief in *Carpenter* noted, the cell phone has gone from a niche technology to the primary means of technological communication in the United States. *See* Brief for Petitioner at 39–42, Carpenter v. United States, 138 S. Ct 2206 (2018) (No. 16-402). Cell phones now dominate the field of voice communication devices. *Id.* at 40. ("A majority of American homes now do not have a landline telephone, as residents rely exclusively on cell phones."). Moreover, cell phones enable several other types of electronic communication that play a central role in modern life, including texts, emails, messaging, social media, and more. *Id.*

[113] *See infra* subpart II.C (discussing the normative undesirability of the inescapability inquiry).

[114] *Carpenter*, 138 S. Ct. at 2220.

[115] Kerr, *supra* note 15, at 21.

[116] *See* Donohue, *supra* note 63, at 381–83.

[117] For example, courts have suggested that bank cards, instant messaging apps, and internet service providers are optional rather than essential parts of modern life. *See* United States v. Hood, 920 F.3d 87, 92 (1st Cir. 2019) (holding that the use of a messaging app was optional and a user "could escape" it); United States v. Tolbert, No. CR 14-3761 JCH, 2019 WL 2006464, at *3 (D.N.M. May 7, 2019) (finding that, unlike cell phone data, subscriber information was generated voluntarily by a suspect when he chose to use

The inescapability standard would saddle judges with high decision costs. Elevated decision costs may be justified in some contexts, such as when a balancing test that captures essential normative considerations outperforms a simpler standard.[118] But inescapability is not this type of test. Indeed, as discussed below, it would create harmful incentives for consumers and do a poor job of protecting sensitive personal information.[119] Before *Carpenter*, inescapability might have been useful as a way to rebut the now-outmoded claim that any disclosure of data to a third party eliminates privacy rights in that data.[120] After *Carpenter*, and as the law continues to adapt to changing technological and social contexts, the numerous drawbacks of inescapability as a standard outweigh any remaining benefits.

3. Inescapability and Disadvantage

The inescapability inquiry appears to focus on the population as a whole, asking whether consumers in general can escape a given technology or surveillance practice.[121] This may help avoid further complicating an already difficult inquiry. But it does so at the expense of accurately measuring whether an individual can avoid disclosing their information.

---

an internet service provider); United States v. Frei, No. 3:17-CR-00032, 2019 WL 189826, at *3 (M.D. Tenn. Jan. 14, 2019) (stating that the use of bank cards was voluntary, unlike cell-phone use). The vague, abstract nature of the inescapability standard may yield especially high error rates, and courts may be tempted in difficult cases simply to defer to the government.

[118] Matthew Tokson, *Blank Slates*, 59 B.C. L. REV. 591, 613–18 (2018).

[119] *See infra* subparts II.B–C.

[120] This strong-form third-party doctrine concept is reflected in the much-criticized cases *Smith v. Maryland*, 442 U.S. 735, 745–46 (1979) and *United States v. Miller*, 425 U.S. 435, 442–43 (1976). The Supreme Court has not applied this concept since 1979 and repudiated it in *Carpenter*, 138 S. Ct. at 2220.

[121] *See Carpenter*, 138 S. Ct. at 2211 (recounting, in the first substantive sentence of the opinion, that there are more cell phones in use in the United States than there are people); *id.* at 2218 (describing the common practices of cell phone owners, including carrying their phones with them wherever they go); United States v. Kidd, 394 F. Supp. 3d 357, 367 (S.D.N.Y. 2019) (analyzing the societal ubiquity of a VOIP calling service); Kerr, *supra* note 15, at 21 (describing the inescapability inquiry as centered on modern society and modern life); *id.* at 48–49 (arguing that ride-sharing apps are not indispensable to modern life because people can generally choose alternative modes of travel).

People will vary widely in their reliance on various technologies and their ability to avoid surveillance. A privacy-threatening technology that most people can easily escape may be inescapable for others. For example, ride-sharing apps such as Uber create and store records of all the trips taken by their users. For most people, the use of such apps is optional.[122] They can simply walk, take a bus, or drive their own car. For proponents of an inescapability standard, ride-sharing apps are the paradigm example of an avoidable technology.

Yet for some individuals, ride-sharing apps may be as indispensable as cell phones or internet access. For disabled persons not living near public transportation, ride-sharing services may be the only viable means of transportation.[123] For individuals who cannot afford a car, ride-shares may be essential for getting to appointments, social functions, job interviews, and the like.[124] Studies have shown that majority-black neighborhoods often rely heavily on ride-sharing services, in part because those services may offer greater geographical coverage and less racial discrimination than traditional taxi services.[125] In many areas, non-ride-share taxis are unavailable or are

---

[122] Kerr, *supra* note 15, at 48–49.

[123] *See Rural Transportation Topic Guide Series Introduction*, NAT'L AGING AND DISABILITY TRANSP. CTR. 1–2 (2012), https://www.nadtc.org/wp-content/uploads/NADTC-Rural-Transportation-Topic-Guides-Introduction-PDF-version.pdf [https://perma.cc/VGV4-KSQW] (noting that eleven million rural residents are disabled, two-thirds of rural residents are "older adults," and "approximately 38 percent of rural residents live in areas with no public transportation"). Modern public transportation systems often take payments based on reusable cards purchased by credit card. Such payment systems make it possible to track the travel records of users. *See* Diana Budds, *A New Report Outlines Privacy Risks for the MTA's Contactless Payment System*, CURBED N.Y. (Oct. 3, 2019), https://ny.curbed.com/2019/10/3/20895736/mta-omny-privacy-surveillance-report [https://perma.cc/PW5Z-368Z].

[124] Carol Atkinson-Palombo, Lorenzo Varone & Norman W. Garrick, *Understanding the Surprising and Oversized Use of Ridesourcing Services in Poor Neighborhoods in New York City*, 2673 TRANSP. RES. REC.: J. TRANSP. RES. REC. 185, 189–90 (2019); Laura Bliss, *Lyft Is Reaching L.A. Neighborhoods Where Taxis Wouldn't*, CITYLAB (June 29, 2018), https://www.citylab.com/transportation/2018/06/lyft-is-reaching-la-neighborhoods-where-taxis-wouldnt/563810 [https://perma.cc/NTE5-VVLB].

[125] Bliss, *supra* note 124. Racial discrimination against black riders still persists on ride-sharing services, although comparisons suggest that it is less than that experienced by riders of traditional taxi services. *Id.*

themselves tracked by GPS systems.[126]

A similar point can be made about smart home devices, which often collect detailed records concerning activities inside the home.[127] Internet-connected devices that can unlock doors, raise windows, turn on lights, or operate appliances via voice command are a luxury for most consumers. But for disabled users, they can be essential for empowerment and independence.[128] Such devices have become a crucial part of many people's lives and relationships, dramatically expanding their economic, personal, and social possibilities.[129] As Todd Stabelfeldt, a quadriplegic man with no movement below his shoulders, put it, smart home devices have given him "a lot of opportunities to demonstrate that I'm a quality man and I'm a man of integrity . . . [y]ou can be who you want to be. This technology just allows you to be you in your story."[130]

Indeed, any technology may be indispensable to certain people even if it is unnecessary to most others. Dependence on various technologies will vary based on people's social, economic, and geographical contexts. For a twenty-two--year-old in Atlanta, a certain app may be essential to participating in the social life of her area, while a similar person in Houston may have no need to use the app at all.[131] Likewise, business managers may

---

[126] *See, e.g.*, Dareh Gregorian, *Appeals Court Rules City Can Monitor Taxis' Movements with GPS*, N.Y. DAILY NEWS (Aug. 26, 2016), https://www.nydailynews.com/new-york/appeals-court-rules-city-monitor-taxis-movements-gps-article-1.2767032 [https://perma.cc/JY9T-873Q] (describing New York's system for monitoring its taxis via GPS trackers and noting that it has operated since 2004).

[127] Tokson, *supra* note 11, at 52–55.

[128] Chiara A. Sottile, *How a Smart Home Empowers People with Disabilities,* NBCNEWS (May 9, 2017), https://www.nbcnews.com/tech/tech-news/how-smart-home-empowers-people-disabilities-n756731 [https://perma.cc/Y9T5-EE7Z] ("For some people, doing something like turning on your lights or opening a blind or changing your thermostat might be seen as a convenience, but for others, that represents empowerment, and independence, and dignity.").

[129] *Id.*[130] *Id.* (describing how smart home devices have enhanced Stabelfeldt's life and marriage, allowing him to operate independently and facilitating his job as an IT consultant).

[130] *Id.* (describing how smart home devices have enhanced Stabelfeldt's life and marriage, allowing him to operate independently and facilitating his job as an IT consultant).

[131] *See* Donohue, *supra* note 63, at 382–83.

find that a networking service is a professional necessity, while accountants find it useless. The potential for variance among differently situated people is enormous.

Existing concepts of inescapability do not appear to take personal differences into account, a potentially serious flaw in their theoretical framework.[132] Yet individualizing Fourth Amendment law is unlikely to be a viable solution either. A Fourth Amendment standard that varies among individuals based on their unique circumstances and the technological and social practices of their localities would create doctrinal inconsistency, a flood of litigation, and massive administrability problems for courts.[133] However as it is applied, inescapability would create substantial difficulties for courts and litigants.

B. Harmful Incentives and Deadweight Loss

One of the most serious drawbacks of inescapability is the incentives it creates for consumers. When a technology is escapable, consumers are incentivized to avoid it in order to preserve their privacy rights. But these technologies, while perhaps not essential to modern life, tend to be beneficial. Incentivizing people to avoid modern technology in order to prevent government monitoring creates "deadweight loss"—it causes people to reduce their use of beneficial technologies.[134] The Fourth Amendment regime that *Carpenter* seems to endorse is a profoundly inefficient one.

There are numerous technologies that are arguably optional but nonetheless greatly enhance users' lives. Google Maps, Waze, and other

---

[132] *See supra* note 121 and accompanying text.

[133] In other contexts, the Court has taken pains to avoid "mak[ing] a crazy quilt of the Fourth Amendment" by allowing it to vary across different localities or based on the differing practices of telephone service providers. Smith v. Maryland, 442 U.S. 735, 745 (1979).

[134] A deadweight loss is a permanent loss to society that occurs when the equilibrium for a good or service is not Pareto optimal, i.e., when there are other potential allocations under which one actor in the system would be better off, and no one would be worse off. *See, e.g.*, R. PRESTON MCAFEE, INTRODUCTION TO ECONOMIC ANALYSIS 112–113, 182–83, 198 (2006) ("The deadweight loss is important because it represents a loss to society much the same as if resources were simply thrown away or lost.").

navigation apps are an important part of modern life,[135] but are probably not inescapable in any meaningful sense.[136] Alternative navigation methods like paper maps or asking directions are viable and widely available. Navigation service providers generally collect and store data on users' locations, creating a detailed history of their movements and activities.[137] Government requests for such data have sharply increased in recent years.[138] If users want to ensure that this sensitive information is not available to the government without a warrant, they would have to forego the use of navigation apps and use more privacy-protective alternatives. But navigation apps greatly improve users' ability to navigate, avoid traffic, and prevent getting lost. Giving consumers incentives to stop using these apps would result in substantial societal harm, even if only a small percentage of navigation app users changed their

---

[135] RJ Reinhart, *Most Americans Already Using Artificial Intelligence Products*, GALLUP NEWS: ECONOMY (Mar. 6, 2018), https://news.gallup.com/poll/228497/americans-already-using-artificial-intelligence-products.aspx [https://perma.cc/5CYT-7TNR] (roughly 84% of Americans use navigation apps).

[136] It is difficult to say for certain, given the vagueness of the inescapability standard. *See supra* subpart II.A.

[137] *See, e.g.*, Andrew Couts, *Terms & Conditions: Waze Is a Privacy Accident Waiting to Happen*, DIGITAL TRENDS: MOBILE (Mar. 3, 2013), https://www.digitaltrends.com/mobile/terms-conditions-waze-privacy-accident [https://perma.cc/4ZL6-WJSA]; *Delete Maps History on Your iPhone, iPad, or iPod Touch*, APPLE, https://support.apple.com/en-us/HT208651 [https://perma.cc/87D8-D64N] (last visited July 31, 2020); *Delete Navigation History*, WAZE HELP, https://support.google.com/waze/answer/6262570?hl=en&ref_topic=6262561[https://perma.cc/PVC6-KLPV] (last visited Jan. 27, 2020);; Jillian D'Onfro, *Turning Off Location History Doesn't Stop Google from Storing Where You've Been—Here's How to Limit the Info It Logs*, CNBC: TECH (Aug. 13, 2018), https://www.cnbc.com/2018/08/13/how-to-stop-google-from-storing-your-location-history.html [https://perma.cc/8QXG-A8PW]; *Manage Your Location History*, GOOGLE ACCOUNT HELP, https://support.google.com/accounts/answer/3118687?hl=en [https://perma.cc/ESP6-RPVS] (last visited July 31, 2020). However, effectively preventing the storage of one's location information by Google Apps is difficult, and the time and effort required to manually delete one's searches on the other apps is likely prohibitive. *See* D'Onfro, *supra* note 137. Location search histories are also useful, creating an accessible database of previously visited addresses and making navigation easier. Speed and ease of use is particularly important for users navigating while driving.

[138] Zack Whittaker, *Uber Reports a Sharp Rise in Government Demands for User Data*, TECH CRUNCH (Nov. 20, 2019, 11:00 AM), https://techcrunch.com/2019/11/20/uber-transparency-government-data [https://perma.cc/3MHF-MY63].

behavior.[139]

Roughly 6% of Americans are currently using a dating app and 21% have done so in the past.[140] These apps are popular but would probably not be considered inescapable, even for single people.[141] The majority of couples still meet through other means, generally through friends, in bars or restaurants, through coworkers, in school, or through family.[142] Dating apps gather a vast quantity of user information, some of it quite intimate.[143] For example, Tinder collects information on all of one's matches, including their age and race; the location and timing of every online conversation between matches; which words one uses the most; how much time users spend looking at others' pictures before swiping; data from Facebook on users' "likes" and friend networks; and more.[144]

In order to protect this information from government exposure, individuals would have to choose one of the alternative, offline methods for meeting potential dates. But many individuals would incur substantial costs

---

[139] *See* Reinhart, *supra* note 135 (roughly 84% of Americans use navigation apps).

[140] J. Clement, *Percentage of Online Users in the United States Who Have Used a Dating Website or App as of January 2019*, STATISTA (April 29, 2020), https://www.statista.com/statistics/310256/us-online-dating-app-site-usage/ [https://perma.cc/3MHF-MY63]. I use "app" to refer to both smartphone applications and web-based applications on websites.

[141] Again, it is difficult to say for certain given the conceptual confusion of the inescapability principle. *See supra* subpart II.A. It could be argued that dating apps are essentially inescapable for young, single people without extensive friend groups or social networks, who have recently relocated to a new city, or who are recently divorced. Again, an accurate assessment of escapability would require a granular, fact-based inquiry that would vary from person to person. *See supra* section II.A.3.

[142] *See* Michael J. Rosenfeld et al., *Disintermediating Your Friends: How Online Dating in the United States Displaces Other Ways of Meeting*, 116 PNAS 17753, 17755 (2019).

[143] Thomas Germain, *How Private Is Your Online Dating Data?*, CONSUMER REPS. (Sept. 21, 2019), https://www.consumerreports.org/privacy/how-private-is-your-online-dating-data [https://perma.cc/X926-B8UV] (reporting that dating apps may collect data on one's location, contacts, photos, network connections, time spent on profiles, and type of person preferred by a user). Some dating apps generate revenue by using personal data to target ads or by selling it to third parties. *Id.*

[144] Judith Duportail, *I Asked Tinder for My Data. It Sent Me 800 Pages of My Deepest, Darkest Secrets*, THE GUARDIAN (Sept. 26, 2017), https://www.theguardian.com/technology/2017/sep/26/tinder-personal-data-dating-app-messages-hacked-sold [https://perma.cc/MRS3-QLDE].

in doing so. Their dating prospects may be significantly reduced, especially for LGBT+ persons or other individuals whose offline dating pool may be limited.[145] The time and effort they spend seeking a dating partner might increase substantially. Some may fail to meet their "soulmate"—millions of marriages have had their start with online dating.[146] Even if the effects of foregoing dating apps are not typically so severe, a legal regime that discourages a popular and effective way for people to meet risks substantial societal loss.[147]

A similar analysis could be done for those users who can avoid using ride-sharing apps and smart home devices.[148] These technologies are not mandatory for many people, but they can nonetheless substantially enhance people's lives.[149] Ride-sharing apps may even save lives—most studies find that their use is correlated with a significant reduction in drunk driving

---

[145] *See* Anna Brown, *Couples Who Meet Online Are More Diverse than Those Who Meet in Other Ways, Largely Because They Are Younger*, PEW RES. CTR. (June 24, 2019), https://www.pewresearch.org/fact-tank/2019/06/24/couples-who-meet-online-are-more-diverse-than-those-who-meet-in-other-ways-largely-because-theyre-younger [https://perma.cc/SDL2-7722].

[146] *Cf.* Erin Duffin, *Number of Marriages in the United States from 1990 to 2018*, STATISTA (Jan. 17, 2020), https://www.statista.com/statistics/195931/number-of-marriages-in-the-united-states-since-1990 [https://perma.cc/V5KW-LL4A] (showing that over two million marriages occur per year in the United States); Rosenfeld et al., *supra* note 142, at 1 n.1, fig.1 (The rate of marriage for couples who meet online is very similar to that of couples meeting offline, and 40% of couples now meet online);.

[147] For a discussion of dating app information collection and the potential for deterrence, see Danielle Citron, *The Data Death Penalty and Other Reforms for Protecting Intimate Information*, 62 WM. & MARY L. REV. (forthcoming 2021).

[148] *See supra* section II.A.3.

[149] Ride-sharing apps can make transportation far easier for travelers or persons who do not own a car, reduce traffic, and may have unique social benefits for riders and drivers. *See* Javier Alonso-Mora et al., *On-demand High-capacity Ride-sharing via Dynamic Trip Vehicle Assignment*, 114 PNAS 462, 467 (2017); *Why Ridesharing Reaps Unexpected Benefits*, KNOWLEDGE@WHARTON (Nov. 14, 2019), https://knowledge.wharton.upenn.edu/article/ridesharing-culture-benefits [https://perma.cc/L6LS-QZC2]. Smart homes have several benefits for consumers, including energy efficiency, convenience, improving security, entertainment, detecting faulty appliances, increasing property value, and improving health and quality of life. *See* Charlie Wilson et al., *Benefits and Risks of Smart Home Technologies*, 103 ENERGY POL'Y 72, 76–77 (2017).

fatalities.[150] Courts should be reluctant to establish a legal regime that disincentivizes the use of potentially life-saving technologies among people concerned with fundamental rights to privacy.

It might be objected that few people exist who are sufficiently concerned with privacy from government observation to forego the useful technologies described above. But this is hardly reassuring. Rather, it demonstrates that the inescapability standard is behaviorally unrealistic and inconsistent with meaningful Fourth Amendment protection in the digital age. It is not reasonable to ask people to forego profoundly beneficial technologies in order to preserve their rights. The likely upshot of such a standard is that many consumers will continue to use these technologies and face comprehensive government surveillance without constitutional safeguards.

C. The Normative Implications of Inescapability

A central goal of the reasonable expectation of privacy test is to protect whatever society considers private.[151] Thus the Court has typically safeguarded intimate places and information while declining to protect less sensitive things.[152] Yet inescapability does an especially poor job of protecting sensitive data. An inescapability standard would often expose private data to government scrutiny while shielding data that is relatively non-sensitive.[153]

Optional technologies frequently capture the most intimate forms of

---

[150] Jacey Fortin, *Does Uber Really Prevent Drunken Driving? It Depends on the Study*, N.Y. TIMES (Apr. 7, 2017), https://www.nytimes.com/2017/04/07/business/uber-drunk-driving-prevention.html [https://perma.cc/Z6C4-8JRZ] (noting that studies predominantly show a correlation between Uber services and lower rates of alcohol-related accidents).

[151] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("My understanding of the rule that has emerged from prior decisions is that there is 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.'"); *id.* at 351–52 (holding that telephone conversations are protected by the Fourth Amendment in light of the "vital role that the public telephone has come to play in private communication").

[152] Tokson, *supra* note 11, at 13–16.

[153] For a detailed discussion of the concept of sensitive data, see Paul Ohm, *Sensitive Information*, 88 S. CAL. L. REV. 1125, 1128–1132 (2015).

data. Smart speakers record sounds inside the home and transmit those recordings to third party service providers.[154] Internet-connected beds, appliances, and personal items can record and transmit extremely intimate details about people's lives.[155] Health apps and "femtech" services collect extensive, personal data about users' bodies, prescriptions, habits, and preferences.[156] Smart door locks such as Amazon Ring record all comings and goings to a home and videotape all of a resident's activities on their porch or front yard.[157] DNA analysis services can obtain detailed information about an individual's genetic makeup, paternity, future health prospects, and more.[158] These technologies are escapable for most consumers, yet exposing the sensitive data they collect to government observation subverts fundamental Fourth Amendment values.[159]

---

[154] Raphael Davidian, *Alexa and Third Parties' Reasonable Expectation of Privacy*, 54 AM. CRIM. L. REV. ONLINE 58, 59–60 (2017) (describing how smart speakers record and process requests and other speech from their users); Austin Carr et al., *Silicon Valley Is Listening to Your Most Intimate Moments*, BLOOMBERG BUSINESSWEEK (Dec. 11, 2019), https://www.bloomberg.com/news/features/2019-12-11/silicon-valley-got-millions-to-let-siri-and-alexa-listen-in [https://perma.cc/K93B-Y5WJ] (discussing the "recordings of intimate moments inside people's homes" and other personal data captured by Amazon's Alexa and listened to by its employees).

[155] *See, e.g.*, Tim Bajarin, *The Next Big Thing for Tech: The Internet of Everything*, TIME (Jan. 13, 2014), http://time.com/539/the-next-big-thing-for-tech-the-internet-of-everything/ [https://perma.cc/8R96-PJH5]; Bree Fowler, *Gifts that Snoop? The Internet of Things Is Wrapped in Privacy Concerns*, CONSUMER REPORTS (Dec. 13, 2017), https://www.consumerreports.org/internet-of-things/gifts-that-snoop-internet-of-things-privacy-concerns/ [https://perma.cc/QD6H-5PCJ]; Melia Robinson, *This Sex Wearable that's Being Falsely Marketed as a 'Smart Condom' Is Kind of Ridiculous*, BUS. INSIDER (Mar. 3, 2017), https://www.businessinsider.com/smart-condom-icon-sex-wearable-2017-3 [https://perma.cc/VF4Q-VVET].

[156] *See* Citron, *supra* note 147(manuscript at 5).

[157] Rani Molla, *How Amazon's Ring Is Creating a Surveillance Network with Video Doorbells*, VOX (Jan. 28, 2020, 12:08 PM), https://www.vox.com/2019/9/5/20849846/amazon-ring-explainer-video-doorbell [https://perma.cc/NV9J-XG9X].

[158] Andelka M. Phillips, *Only a Click Away—DTC Genetics for Ancestry, Health, Love … and More: A View of the Business and Regulatory Landscape*, 8 APPLIED & TRANSLATIONAL GENOMICS 16, 16–20 (2016).

[159] For a discussion of those values, see Tokson, *supra* note 118, at 635 & n.279 (discussing historical sources on the broader purposes of the Fourth Amendment, including the protection of privacy, property, and liberty). See also *supra* notes 127–129 and accompanying text for a discussion of how smart home technologies may be essential to

At the same time, many difficult-to-escape technologies may produce less sensitive information or information that is especially useful in detecting crime. Online banking or electronic wire transfers may be an inescapable part of modern financial life, but the information they produce is rarely intimate and is often essential to detecting white-collar crimes.[160] Utility bills that record the electricity or water usage of a home are largely unavoidable but typically reveal only very general and nonsensitive information.[161] Similarly, giving one's subscriber information to online service providers is likely inescapable because it is usually necessary for internet access.[162] Yet subscriber information is not itself especially sensitive, mostly consisting of data such as one's name, address, and telephone number.[163] Inescapability

---

some disabled persons.

[160] *See* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 509–10 (2011) (explaining that the Supreme Court eliminated the warrant requirement for financial records following the rise of difficult-to-detect white-collar crimes).

[161] Smart meters and smart utilities may record more granular data about energy usage, but traditional utility metering reveals only the overall energy consumption of a household. *See* Deirdre K. Mulligan et al., *Privacy in the Smart Grid: An Information Flow Analysis*, CAL. INST. ENERGY & ENV'T 1, 5–6 (2011), https://ssrn.com/abstract=1815605 [https://perma.cc/EQ5U-569T] (comparing the household information revealed by smart meters versus traditional metering systems).

[162] *See, e.g.*, *Comcast Customer Privacy Notice*, COMCAST, https://cdn.comcast.com/-/media/Images/www_xfinity_com/Corporate/PrivacyPolicyUniLegalStndENG.pdf?rev=19ecf433-a422-4978-ac4a-b7e17ffe8801&la=en [https://perma.cc/G53K-BYUM] (last updated Jan. 1, 2018) (explaining that a customer's name, address, email address, and phone number are collected upon an account's creation).

[163] *See* Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2122 (2009). To be sure, this data can implicate privacy when it is used to de-anonymize internet users. In any event, this data generally receives minimal statutory protections compared to communications content, location information, and other forms of digital data, and courts have virtually always declared it outside of the Fourth Amendment's scope, both before and after *Carpenter*. *See* 18 U.S.C. § 2703(c)(2) (2018); United States v. Morel, 922 F.3d 1, 9 (1st Cir. 2019); United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008); United States v. Hambrick, No. 99-4793, 2000 WL 1062039, at *3 (4th Cir. Aug. 3, 2000) (per curiam); United States v. Maclin, 393 F. Supp. 3d 701, 708 (N.D. Ohio 2019); United States v. Tolbert, No. CR 14-3761 JCH, 2019 WL 2006464, at *3 (D.N.M. May 7, 2019); United States v. Sherr, 400 F. Supp. 2d 843, 848 (D. Md. 2005). *See also* Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2018) (providing little protection for subscriber information, which can be obtained via subpoena). This data is frequently obtained by the government in cases involving child

would privilege these less sensitive forms of information over the intimate data generated by more escapable technologies.[164] In many cases, an inescapability standard would produce normatively undesirable outcomes and fail to adequately protect privacy.

D. Inescapability and Precedent

Aside from its conceptual problems, the inescapability standard threatens to make a mess of Fourth Amendment jurisprudence. It is directly contradicted by several Supreme Court precedents still in force.[165] Indeed, the *Carpenter* opinion reaffirms two of these precedents at the same time it purportedly establishes the importance of inescapability.[166]

In *Smith v. Maryland*, the Supreme Court held that people have no reasonable expectation of privacy in the phone numbers that they dial.[167] In *United States v. Miller*, it ruled that they have no privacy in their bank records.[168] In neither case was the disclosure of information to a third party any more escapable than the disclosures in *Carpenter*.[169] Telephones were certainly a vital part of modern life by the time *Smith* was decided—the Court

---

pornography and online harassment. *See, e.g.*, Sherr, 400 F. Supp. at 846; Freedman v. Am. Online, Inc., 412 F. Supp. 2d 174, 179–183 (D. Conn. 2005).

[164] *See supra* text accompanying notes 154–158. Note that, under Professor Kerr's preferred application of *Carpenter*, subscriber information would not be protected despite meeting the requirement of inescapability because it would fail under a separate requirement that protected, third-party records be uniquely digital. *See* Kerr, *supra* note 15, at 16, 47.

[165] *See* California v. Greenwood, 486 U.S. 35, 40 (1988) (holding that people had no reasonable expectation of privacy in their household trash placed in bags and left for pickup, despite the potentially inescapable nature of trash disposal in areas where individuals cannot lawfully bring their own trash to a landfill); Smith v. Maryland, 442 U.S. 735, 745–46 (1979) (holding that the Fourth Amendment does not protect dialed phone numbers); United States v. Miller, 425 U.S. 435, 442–43 (1976) (holding that the Fourth Amendment does not apply to bank records).

[166] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) ("We do not disturb the application of *Smith* and *Miller* . . . .").

[167] *Smith*, 442 U.S. at 745–46.

[168] *Miller*, 425 U.S. at 442–43.

[169] *See Carpenter*, 138 S. Ct. at 2220.

itself had said so in a prior case.[170] And the use of a bank is a necessary part of most people's lives.[171] These cases have been widely criticized,[172] yet the Court did not critique them or invoke stare decisis in upholding them.[173]

There are a few possible explanations for the Court's refusal to overturn or criticize these cases. One is that the Court does not consider inescapability an important factor, let alone a decisive one.[174] The *Carpenter* opinion devotes substantially more discussion to the deeply revealing and extensive nature of cell phone tracking than it does to inescapability.[175] It distinguishes

---

[170] Katz v. United States, 389 U.S. 347, 352 (1967) (noting "the vital role that the public telephone has come to play in private communication").

[171] Moreover, bank customers are unable to prevent banks from making and retaining records of their financial transactions. The Bank Secrecy Act requires banks to, among other things, make "a microfilm or other reproduction of each check, draft, or similar instrument" presented for payment or deposit and retain these and other records for a period of up to six years. 12 U.S.C. § 1829b(d)–(g) (2018). The Court expressly ruled in *Miller* that this compulsory record keeping did not give rise to any Fourth Amendment right for bank customers, who could not lawfully avoid scrutiny of their records. *Miller*, 425 U.S. at 441–42.

[172] *See, e.g.*, Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211, 242–44 (2006); Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 113–14 (2008); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1136–38 (2002).

[173] *Carpenter*, 138 S. Ct. at 2220. Neither did the Court question the rule of *Stoner v. California*, where the Court held that hotel guests have a Fourth Amendment right in their rooms despite giving permission to the cleaning staff to enter the room in the performance of their duties. *See* Stoner v. California, 376 U.S. 483, 489 (1964). Observation of a hotel room by cleaning staff is easily avoidable in most situations; the guest need only place a "Do Not Disturb" sign on the door to prevent it. Yet hotel rooms are universally protected, no matter what steps the guest takes or fails to take to prevent observation by third parties. Finsel v. Hartshorn, 200 F. Supp. 2d 960, 967 (C.D. Ill. 2002) (noting that "[i]t is beyond question . . . that an unconsented police entry into a residential unit, be it a house or an apartment or a hotel or motel room, constitutes a search within the meaning of *Katz v. United States*" (alteration in original) (quoting 1 WAYNE R. LAFAVE, SEARCH & SEIZURE § 2.3(b) at 474–75 (3d ed. 1996)), *aff'd sub nom*. Finsel v. Cruppenink, 326 F.3d 903 (7th Cir. 2003); People v. Superior Court, 49 Cal. Rptr. 3d 831, 848 (Cal. Ct. App. 2006) (drawing on *Stoner* to find a Fourth Amendment right against police inspections of dorm rooms).

[174] *Cf. supra* subpart I.C. (discussing interpretations of *Carpenter* that consider inescapability either an important factor or a requirement for Fourth Amendment protections).

[175] *Carpenter*, 138 S. Ct. at 2216–19. The Court's relative lack of discussion of

Smith and *Miller* by noting that those cases emphasized the nonrevealing nature of the information obtained.[176] It may be that the intimacy, extent, and low cost of cell phone location tracking are what mattered to the Court,

---

inescapability is notable in light of the fact that Carpenter's attorneys devoted several pages to the topic. Brief for Petitioner at 39–44, Carpenter v. United States, 138 S. Ct 2206 (2018) (No. 16-402) . They argued that Carpenter had little choice but to use a cell phone and to disclose its location to his service provider. *Id.* at 39–40. They pointed out that nearly all American adults own a cell phone and that cell phones automatically transmit location data to cell phone companies. *Id.* at 39–44. They note that alternative means of vocal communication are disappearing, as a "majority of American homes now do not have a landline telephone, as residents rely exclusively on cell phones." *Id.* at 40. Payphones have likewise shrunk to near irrelevance over the past two decades. *See id.* They note that cell phones are often the exclusive means through which people contact first responders in a medical emergency, report a crime, or to seek roadside assistance. *Id.* at 41. Roughly seventy percent of 911 calls are placed from cell phones. *Id.* Cell phones generate and transmit location data as long as they are switched on. *Id.* at 42. Location privacy settings on a smartphone have no impact on the transmission of cell signals that permit tower-based location tracking. *Id.* "There is no way to avoid the aggregation and retention of this location information short of turning off or disabling the phone." *Id.* Several amicus briefs raised similar arguments about inescapability. *See, e.g.*, Brief for Electronic Frontier Foundation et al. as Amici Curiae Supporting Petitioner at 22, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402) (contending that "owning and carrying a phone is hardly a choice at all" and "cell-phone users have no choice but to reveal certain information to their cellular provider"); Brief for Scholars of the History and Original Meaning of the Fourth Amendment as Amici Curiae Supporting Petitioner at 12, 26, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402) (arguing that cell phones are "essential tool[s] of modern life" and that people have no choice over whether CSLI is collected); Brief for Michael Varco as Amicus Curiae Supporting Respondent at 17, 20, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402) (arguing that petitioner could have avoided having CSLI data collected by using internet-based apps or leaving his cellular phone at home); Brief for National District Attorneys Association as Amicus Curiae Supporting Respondent at 17, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402) (arguing that petitioner could have restricted the conveyance of CSLI by using apps to complete calls, putting his phone in airplane mode, or turning it off).

[176] *Carpenter*, 138 S. Ct. at 2219–20 (describing *Smith* and *Miller*); *see* Smith v. Maryland, 442 U.S. 735, 741 (1979) (noting that "pen registers do not acquire the contents of communications. . . . Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed." (emphasis omitted)); *Miller*, 425 U.S. at 440–42 ("On their face, the documents subpoenaed here are not respondent's 'private papers[]' . . . The checks are not confidential communications but negotiable instruments to be used in commercial transactions.")

while inescapability did little or no work in resolving the case.[177]

Another possibility is that the Court failed to recognize the conflict between its precedents, creating a jurisprudence of confusion and unpredictability. Lower courts looking for guidance on how to apply an inescapability standard have only the brief discussion in *Carpenter* and several contradictory precedents to consult. This doctrinal confusion adds to the profound conceptual confusion surrounding inescapability, making it even more difficult for lower courts to apply consistently.[178]

Neither of these possibilities supports the use of an inescapability standard going forward. Indeed, the conceptual, normative, and doctrinal flaws of inescapability suggest that courts should look elsewhere for a Fourth Amendment standard. The next Part explores ways that courts can minimize the use of inescapability and examines alternative methods of applying the Fourth Amendment to new technologies.

III. ESCAPING INESCAPABILITY

In light of the issues described above, this Part explores several alternative approaches that avoid the use of inescapability. Lower courts can plausibly focus on other factors and minimize inescapability when applying *Carpenter*, as part of the interpretative process that inevitably follows a major new Supreme Court decision. More broadly, scholars have proposed alternative regimes that would transform Fourth Amendment law and replace the current "reasonable expectation of privacy" framework. Most of these approaches would offer more protection and clarity than an inescapability standard. This Part discusses the advantages and disadvantages of these alternatives and examines how they would address issues of third-party disclosure and digital surveillance.

---

[177] *See* Tokson, *supra* note 97, at 11–12 (describing the importance of intimacy, amount, and cost in virtually all of the Court's reasonable expectation of privacy cases, including *Carpenter*).

[178] *See supra* subparts II.A–B.

It is worth noting that, under most of these approaches, concepts like the widespread disclosure or publication of one's information may still be relevant to Fourth Amendment privacy. If a person posts their data to Facebook or publishes it in a newspaper, that is likely to impact how revealing,[179] or intimate,[180] or protected by law[181] that information will be. When disclosure is limited to a single counterparty, however, its relevance is likely to be limited.[182] Moreover, none of the alternative approaches turns on whether a person had the ability to avoid the relevant transaction or disclosure.[183] That assessment carries with it the substantial drawbacks and decision costs described above.

A. Refining the *Carpenter* Framework

Supreme Court precedents, especially important ones, require interpretation.[184] They do not resolve every possible issue or ambiguity but leave it to future courts and other legal actors to fully articulate their meaning.[185] In many cases, the Supreme Court expressly relies on lower court interpretations of its prior decisions.[186] The Court also regularly consults scholars' interpretations and critiques of its prior cases.[187]

---

[179] *See infra* subpart III.A.
[180] *See infra* subsection III.B.4(b).
[181] *See infra* section III.B.2.
[182] *See infra* subpart III.B. For a theoretical discussion of the relevance of the extent of dissemination, see Lior Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 973–975 (2005) (arguing that limited disclosures of information do not eliminate privacy and detailing how social network analysis can aid courts in assessing the extent of public disclosure in cases involving wider dissemination).
[183] *See infra* subpart III.B.
[184] Thus Supreme Court opinions interpret and apply past opinions while providing material for future courts to interpret in an ongoing process of precedential interpretation.
[185] Richard M. Re, *Narrowing Supreme Court Precedent from Below*, 104 GEO. L.J. 921, 925–26 (2016).
[186] *See infra* notes 204–206 and accompanying text.
[187] *See infra* note 208. Legal scholarship appears to be especially influential in difficult cases and those in which the Court alters precedent. Lee Petherbridge & David L. Schwartz, *An Empirical Assessment of the Supreme Court's Use of Legal Scholarship*, 106 NW. U. L. REV. 995, 998–99 (2012) (noting that the Supreme Court is more likely to cite scholarship in cases with indicia of difficulty and where decisions alter precedent).

This "precedential dialogue" allows the Supreme Court to assess the various interpretations of its rulings and observe their practical consequences.[188] It also presents an opportunity for courts and scholars to influence the law's development.[189] Broad Supreme Court opinions can be viewed as a kind of delegation to lower courts, providing them with space for interpretive flexibility.[190]

The *Carpenter* opinion is notably cryptic regarding how courts should address digital surveillance in the future.[191] It overtly declined to address any form of information beyond historical cell phone location data.[192] The Court instead chose to proceed incrementally so as not to "embarrass the future" with a sweeping but erroneous decision.[193] Nonetheless, the impact of the Court's ruling that people can retain a Fourth Amendment right in information owned by third parties is potentially massive.[194] The considerations identified by the Court—the revealing, extensive, inescapable nature of cell phone tracking—are broadly applicable to digital surveillance generally.[195] This is the archetypal example of a case that calls for further development and interpretation.[196]

An important part of that development will be the minimization or abandonment of inescapability in cases applying *Carpenter*. Inescapability

---

[188] Re, *supra* note 185, at 927.
[189] *See infra* notes 204–206, 208 and accompanying text.
[190] Re, *supra* note 185, at 926.
[191] Strahilevitz & Tokson, *supra* note 63.
[192] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) ("We do not express a view on matters not before us: real-time CSLI or 'tower dumps' . . . . We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information.").
[193] *Id.* (quoting Nw. Airlines, Inc. v. Minnesota, 322 U.S. 292, 300 (1944)).
[194] Ohm, *supra* note 8, at 385.
[195] *Carpenter*, 138 S. Ct. at 2223.
[196] Caminker, *supra* note 16, at 460 (stating that *Carpenter*'s "amorphous nature . . . now gives judges license, if not permission, to deviate, to innovate, and even to anticipate technological change"); Re, *supra* note 185, at 947 ("[T]he existence of ambiguity in a higher court precedent can itself be regarded as a meaningful message to lower courts . . . . disuniformity can sometimes be helpful in fostering 'percolation'—that is, experimentation and reflection on what might otherwise be stale legal rules.").

should be minimized for the reasons described above: it is difficult to administer, conceptually confused, oblivious to disability and difference, inefficient and socially harmful, and normatively undesirable.[197] Moreover, minimizing inescapability reflects a plausible reading of *Carpenter* itself. As noted above, the Court's discussion of inescapability is relatively brief, while the bulk of its opinion is concerned with the intimate, voluminous nature of cell phone tracking.[198] The Court describes in detail the serious threats to privacy that cell phone tracking poses.[199] Given this emphasis, it is unlikely that the Court would permit the government to collect revealing or extensive data at low cost regardless of how escapable it was.[200] Nor is inescapability compatible with the Court's other Fourth Amendment precedents.[201]

Lower courts applying *Carpenter* can plausibly assess surveillance based on its revealing and extensive nature while ignoring inescapability or mentioning it only in passing.[202] Indeed, some courts have already ignored inescapability when applying *Carpenter*.[203] Moreover, lower courts have successfully narrowed or modified constitutional doctrines in several similar contexts.[204] For example, the "reasonable expectation of privacy" test is

---

[197] *See supra* Part II.

[198] *See supra* notes 175–177 and accompanying text.

[199] *See* Tokson, *supra* note 97, at 10 n.78.

[200] *Carpenter*, 138 S. Ct. at 2217–19 (describing at length the privacy harms that may result from cell phone tracking); *id.* (noting the ubiquity of cell phone use); Tokson, *supra* note 97, at 10 n.78, 13 (noting the ubiquity of cell phone use).

[201] *See supra* subpart II.D.

[202] *See* Re, *supra* note 185, at 942 (discussing the plausibility of a lower court's narrowing interpretation of a search incident to arrest precedent).

[203] *Compare* United States v. Howard, No. 1:19-CR-54-WKW, 2019 WL 6048885, at *6 (M.D. Ala. Nov. 15, 2019) (assessing GPS tracking without addressing inescapability), *and* People v. Tafoya, 2019 COA 176, ¶¶ 42–48 (holding that video surveillance of a suspect's curtilage was a Fourth Amendment search on the basis of factors other than inescapability), *with* United States v. Hood, 920 F.3d 87, 92 (1st Cir. 2019) (holding that the government could warrantlessly collect IP address data associated with a messaging app because the app was optional and escapable), *and* State v. Martinez, 570 S.W.3d 278, 288 (Tex. Crim. App. 2019) (holding that a blood draw of an accident victim was a search because the patient could not have escaped it).

[204] After *Boumediene v. Bush* held that prisoners held in Guantanamo Bay could file writs of habeas corpus and secure "meaningful" review of their detentions, the D.C. Circuit repeatedly construed detainees' rights of review narrowly. Boumediene v. Bush, 553 U.S.

nominally a two-prong test, but its first prong, asking whether a person had a subjective expectation of privacy, is largely ignored by lower courts.[205] Most courts do not mention it, and most that do mention it do not apply it. Courts could similarly excise inescapability from any application of *Carpenter* to digital information.[206]

Lower courts[207] and scholars[208] should recognize the flaws of the

---

723, 779 (2008); Re, *supra* note 185, at 963–64; Stephen I. Vladeck, *The D.C. Circuit After* Boumediene, 41 SETON HALL L. REV. 1451 (2011). Lower court decisions interpreted Supreme Court precedents to require only a preponderance of the evidence standard for detention, to permit the use of hearsay evidence, and to limit remedies for unlawfully held detainees. Al-Bihani v. Obama, 590 F.3d 866, 878 (D.C. Cir. 2010), *cert. denied*, 131 S. Ct. 1814 (2011); Al-Adahi v. Obama, 613 F.3d 1102, 1104 (D.C. Cir. 2010) (suggesting that the burden for continued detention might be even less than a preponderance of the evidence), *cert. denied*, 131 S. Ct. 1001 (2011); Vladeck, *supra* note 204, at 1476–88 (describing the relevant remedies cases). The Supreme Court has largely accepted these modifications. *See* Vladeck, *supra*, at 1475; Lyle Denniston, *Ex-judge:* Boumediene *Is Being "Gutted"*, SCOTUSBLOG (July 17, 2012, 3:54 PM), https://www.scotusblog.com/2012/07/ex-judge-boumediene-is-being-gutted [https://perma.cc/3KCS-55HS].

In *Saucier v. Katz*, the Supreme Court commanded lower courts to resolve qualified immunity cases by first assessing whether a constitutional right was violated and only then assessing qualified immunity. Saucier v. Katz, 533 U.S. 194, 200 (2001). Many lower courts declined to enforce this rule, while others criticized the rule aggressively. Matthew Tokson, *Judicial Resistance and Legal Change*, 82 U. CHI. L. REV. 901, 955 (2015). Eight years later, the Supreme Court reversed its prior decision, citing lower court confusion and criticism. Pearson v. Callahan, 555 U.S. 223, 234–35 (2009).

[205] Orin S. Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113, 114 (2015).

[206] Alternatively, courts might minimize, narrow, and/or critique inescapability even if they consider it binding law. For examples of courts minimizing or successfully critiquing aspects of Supreme Court law, see *supra* note 204 and accompanying text.

[207] *See supra* notes 202–206 and accompanying text.

[208] Scholars likewise play a substantial role in interpreting and critiquing ambiguous Supreme Court standards. In areas ranging from the Establishment Clause to contempt of court, the Court has acknowledged and often ruled in accordance with academic criticism of its prior decisions. Am. Legion v. Am. Humanist Ass'n, 139 S. Ct. 2067, 2081 (2019) (noting that the *Lemon* test has been "questioned by a diverse roster of scholars" and declining to apply the test to evaluate longstanding monuments using religious imagery); Int'l Union, United Mine Workers of Am. v. Bagwell, 512 U.S. 821, 827 n.3 (1994) ("Numerous scholars have criticized as unworkable the traditional distinction between civil and criminal contempt."). It often rules in line with the scholarly consensus in these cases. Am. Legion, 139 S. Ct. at 2081, 2089 (ruling in favor of a longstanding monument,

inescapability standard. In light of these flaws, *Carpenter* is best read to create a standard that focuses on the revealing and detailed nature of digital surveillance. Surveillance that reveals "the privacies of life" and "provides an all-encompassing record" of a user's activities should be governed by the Fourth Amendment, regardless of escapability.[209]

B. Alternative Models of Fourth Amendment Protection

Although *Carpenter* forges a new path for Fourth Amendment law in the digital era, it does so by refining the "reasonable expectation of privacy" test that courts have used since the late 1960s.[210] That test has been criticized as tautological, confusing, and underprotective, in addition to its difficulties with data held by third parties.[211] In recent years, scholars have proposed various alternative regimes for determining the Fourth Amendment's scope. These approaches have their own advantages and disadvantages, but each of them would avoid using inescapability to determine Fourth Amendment rights. This section explores these alternatives and assesses how each would apply to government surveillance of digital information held by third parties.

1. The Normative Approach

Rather than attempting to assess people's expectations of privacy, courts

---

contrary to what the *Lemon* test might direct); Carpenter v. United States, 138 S. Ct. 2206, 2262 (2018) (Gorsuch, J., dissenting) (noting that the Court's limitation of the third-party doctrine was bolstered by vigorous scholarly criticism of the doctrine)*; see* Moore v. Texas, 137 S. Ct. 1039, 1052 n.10 (2017) (noting scholarly criticism of a Texas standard and overruling that standard).

[209] *Carpenter*, 138 S. Ct. at 2217.

[210] Terry v. Ohio, 392 U.S. 1, 9 (1968) ("We have recently held that . . . wherever an individual may harbor a reasonable 'expectation of privacy,' he is entitled to be free from unreasonable government intrusion." (quoting Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring))).

[211] Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring); William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1824–25 (2016); 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, 132–39 (2002); Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1511 (2010).

might take a more directly normative approach, asking what protections the Fourth Amendment should provide to people regardless of societal expectations.[212] For example, courts could apply a balancing test analogous to those used throughout First Amendment law, weighing the benefits of a type of government surveillance against its harms.[213] In prior work, I have offered an account of the core normative considerations involved: the benefits of crime detection and prevention, and the harms of deterring lawful activities, impairing relationships, and inflicting direct psychological injury.[214] The Supreme Court has itself engaged in normative balancing in prior Fourth Amendment cases, albeit in a rudimentary manner.[215] Likewise, some lower courts applying *Carpenter* have taken a normative approach, focusing directly on the privacy harms and chilling effects of government surveillance in novel Fourth Amendment contexts.[216]

A normative balancing approach would have several advantages,

---

[212] Aya Gruber, *Garbage Pails and Puppy Dog Tails: Is That What* Katz *Is Made of?*, 41 U.C. DAVIS L. REV. 781, 795 (2008) ("At some level the constitutional inquiry must concern not just what society actually believes is private, but what we ought to be able to regard as private . . . ."); Joel R. Reidenberg, *Privacy in Public*, 69 U. MIAMI L. REV. 141, 155–57 (2014) (proposing a normative regime based on whether surveilled behavior is of private or public concern); Olivier Sylvain, *Failing Expectations: Fourth Amendment Doctrine in the Era of Total Surveillance*, 49 WAKE FOREST L. REV. 485, 522 (2014) (arguing that courts should reject expectation-based tests and adopt a more normative approach); Matthew Tokson, *The Normative Fourth Amendment*, 104 MINN. L. REV. 741, 743 (2019) (proposing a normative balancing test for Fourth Amendment Searches).

[213] Tokson, *supra* note 212.

[214] *Id.* My proposed test would also consider whether the same law enforcement goals could be achieved via a less invasive practice. *Id.* at 768; *see also* Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3 (discussing factors that make government observation especially worthy of regulation); Henderson, *supra* note 43, at 985–1014 (listing considerations that lower courts have found relevant to privacy).

[215] *See* Hudson v. Palmer, 468 U.S. 517, 527 (1984) (balancing a prisoner's privacy interests against the government's interests in prison administration).

[216] *See* United States v. Chavez, No. 3:18-CR-00311-MOC-DCK-3, 2019 WL 5849895, at *6 (W.D.N.C. Nov. 7, 2019) (evaluating the vital role that social media plays as a conduit for intimate or political speech and finding that the Fourth Amendment protects nonpublic Facebook communications from government surveillance); United States v. Moore-Bush, 381 F. Supp. 3d 139, 148–49 (D. Mass. 2019), *as amended* (June 4, 2019) (discussing at length surveillance's chilling effects on religious, intimate, and social activities in evaluating pole camera surveillance of a suspect).

including its adaptability to new surveillance technologies and social contexts, consideration of discrimination-based harms, and ability to address programmatic surveillance.[217] Its drawbacks include the relative difficulty of administering a balancing test and the potential for unpredictability when addressing novel issues.[218]

In contrast to an inescapability standard, this approach would likely protect most forms of personal digital information held by third parties.[219] When government observation of such information would cause serious privacy harms—as with emails, smart home devices, websurfing data, IP addresses, and more—a normative approach would generally require the government to secure a warrant.[220] In areas where data is less sensitive and especially important to crime detection, such as noncredit-card banking information, the Fourth Amendment would likely not apply.[221]

2. The Positive Law Regime

Courts could rely on other sources of law to determine the Fourth Amendment's scope. Under a positive law approach, the Amendment would apply whenever an official commits an act that would be unlawful or tortious if done by a private citizen.[222] The Supreme Court has looked to positive law

---

[217] Tokson, *supra* note 212, at 778–86.

[218] *Id.* at 786–95. Note that the current reasonable expectation of privacy standard suffers from the same flaws, and a normative replacement would likely be no harder to administer or more unpredictable than the current test, which is famously confusing and unpredictable in its application. *See* Ronald J. Allen & Ross M. Rosenberg, *The Fourth Amendment and the Limits of Theory: Local Versus General Theoretical Knowledge*, 72 ST. JOHNS L. REV. 1149, 1153–58, 1166 (1998); Alan Z. Rozenshtein, *Fourth Amendment Reasonableness After* Carpenter, 128 YALE L.J.F. 943, 958–60 (2019); *see also* George M. Dery III, *Failing to Keep "Easy Cases Easy":* Florida v. Jardines *Refuses to Reconcile Inconsistencies in Fourth Amendment Privacy Law by Instead Focusing on Physical Trespass*, 47 LOY. L.A. L. REV. 451, 471–79 (2014) (discussing the flaws and inconsistencies of the Court's current property-based subtest).

[219] Tokson, *supra* note 212, at 801–08.

[220] *See id.*

[221] *Id.* at 804–05.

[222] *See* Baude & Stern, *supra* note 211, at 1831–32; Michael J. Zydney Mannheimer, *Decentralizing Fourth Amendment Search Doctrine*, 107 KY. L.J. 169, 210–11 (2019).

in a handful of prior Fourth Amendment cases.[223]

Such an approach would be predictable where existing law is clear and would benefit from legislators' informational advantages and ability to regulate comprehensively.[224] On the other hand, a positive law regime would often base the Fourth Amendment on considerations that are irrelevant to privacy, would remove limits to the political branches' ability to compromise citizens' rights, and might underprotect privacy due to the high enactment costs of legislation.[225]

A positive law approach would likely protect digital information held by third parties in many situations, though it is difficult to say for certain due to the ambiguous application of positive law in this context. The leading positive law proposal would apply the Fourth Amendment not only to violations of law but also when an official uses the government's unique legal authority to obtain information.[226] This would presumably prohibit grand jury and administrative subpoenas, although civil subpoenas available to any citizen would likely be allowed.[227] Informal government requests for data or documents are more difficult to assess.[228] While requests from a government

---

[223] The Court typically invokes positive law when finding no constitutional violation in situations when police behavior was otherwise lawful or did not affect the defendant's property. *See* Florida v. Riley, 488 U.S. 445, 451 (1989) (plurality opinion) (noting that the government flew a helicopter at a lawful height above a defendant's house); Rakas v. Illinois, 439 U.S. 128, 129 (1978) (finding that Petitioner could assert no property right or possessory interest in the items searched). The Court does not appear to have ever found a Fourth Amendment right on the basis that the police violated applicable positive law. *Cf.* California v. Greenwood, 486 U.S. 35, 40 (1988) (holding that people have no reasonable expectation of privacy in their trash left on the curb and rejecting the idea that state law could dictate the scope of the Fourth Amendment).

[224] Baude & Stern, *supra* note 211, at 1851–53; Tokson, *supra* note 50, at 192–93. Many Fourth Amendment cases will present issues that are unresolved in existing statutes or precedents. *See* Tokson, *supra* note 212, at 795–96. Government surveillance practices like drug-sniffing dogs or satellite-based observation do not arise in litigation between private parties, and the privacy tort cases that do arise typically rest on an open-ended reasonableness standard that is not well developed. *Id.* at 796.

[225] Richard M. Re, *The Positive Law Floor*, 129 HARV. L. REV. F. 313, 330–31 (2016); Tokson, *supra* note 212, at 796–98.

[226] Baude & Stern, *supra* note 211, at 1831–32.

[227] *See* FED. R. CIV. P. 45.

[228] Tokson, *supra* note 212, at 798 n.331.

official would likely be far more influential than those from a private party, it is unclear whether a positive law approach would take such nonlegal factors into account.[229]

3. The Historical Approach

Courts could interpret the Fourth Amendment as Justice Thomas proposed in his dissent in *Carpenter*, limiting it to certain types of tangible property owned by an individual.[230] Under this approach, the Amendment would apply only to one's person, houses, papers, and effects.[231] Intangible things, other types of property, and records and data owned by other parties would not be covered.[232]

This approach would be conceptually clear and would comport well with historical Fourth Amendment practices.[233] It would mean, however, that nearly all information disclosed to a third party would be unprotected, along with one's conversations and nonresidential real property.[234] This approach would be easier to administer than an inescapability standard but would offer

---

[229] Re, *supra* note 225, at 324. Re criticizes Baude and Stern's positive law model for directing judges to imagine a police officer stripped of official authority, without accounting for the social authority that officers also possess. *Id.* Baude and Stern posit that the positive law model might be loosened to incorporate some effects of official authority, but appear to limit this to "hidden legal privilege." Baude & Stern, *supra* note 211, at 1865–66.

[230] *See* Carpenter v. United States, 138 S. Ct. 2206, 2238–39 (2018) (Thomas, J., dissenting); Jeffrey Bellin, *Fourth Amendment Textualism*, 118 MICH. L. REV. 233, 260–62 (2019).

[231] *See* U.S. CONST. amend. IV (establishing a right in "persons, houses, papers, and effects").

[232] *Carpenter*, 138 S. Ct. at 2238 (Thomas, J., dissenting).

[233] The idea that people can only assert their own property rights in Fourth Amendment is often framed as textualist, but the text of the Fourth Amendment uses plural terms such as "the people" and "their" persons, houses, papers, and effects. While historical practice is consistent with a Fourth Amendment limited to trespasses on an individual claimant's property, the text itself is consistent with a broader, collective right. *See generally* David Gray, *Collective Standing Under the Fourth Amendment*, 55 AM. CRIM. L. REV. 77 (2018) (arguing for a more expansive interpretation of Fourth Amendment privacy interests).

[234] *See* Tokson, *supra* note 212, at 800.

little protection for most forms of digital information.[235]

Such a rule would expose a vast swath of personal data to government observation, at least until legislatures acted to fill in the gaps.[236] It would also enact a substantial institutional shift, largely transferring responsibility for privacy protection against government officials from courts to legislatures, and from the Constitution to statutory law. The effects of such a transition are difficult to predict but would likely result in diminished protection against government surveillance.[237]

4. Alternative Interpretations of Existing Law

a) Empirically Measuring Expectations

Instead of replacing the reasonable expectation of privacy test, courts might reinterpret it to make its application more coherent and predictable.

---

[235] The contents of emails and text messages probably would be protected under a historical approach. *See* Bellin, *supra* note 230, at 279–80. Although service providers often have access to such documents, they are generally stored on behalf of the user and are likely to be considered "their . . . papers." *Id.* at 280. However, the government could subpoena a person's emails from their recipients without violating the person's Fourth Amendment rights under this approach. *See id.*

Some theories grounded in text and history would go in another direction, requiring a warrant for nearly every type of information recorded on paper. Laura Donohue has proposed that courts could find that an individual has a property right and thus a Fourth Amendment right in records that exist due to the individual's actions. Donohue, *supra* note 63, at 353. The idea of owning another person's records on the basis that those records reflect information about one's life would allow for sweeping Fourth Amendment protection but would likely require a substantial restructuring of current property doctrines. *Cf. id.* at 400 (suggesting that granting individuals ownership in information generated about them may not comport with current or historical bailment law).

[236] Bellin, *supra* note 230, at 243.

[237] Legislatures may struggle to do so quickly or effectively, given the various institutional barriers to comprehensive privacy legislation. *See, e.g.*, FRANK R. BAUMGARTNER ET AL., LOBBYING AND POLICY CHANGE 24–26, 45 (2009). They might also simply not be interested in erecting new barriers to government surveillance. Historically, legislatures have been largely ineffective in regulating government surveillance of electronic information. *See* Tokson, *supra* note 50, at 193–94. Further, in the decades before the Supreme Court held that wiretapping was unconstitutional, Congress was ineffective in preventing widespread wiretapping and egregious government misuses of the recorded conversations. *See* Tokson, *supra* note 212, at 798, 799 n.340.

Several scholars have argued that surveys assessing people's expectations of privacy should play an important role in determining the scope of the Fourth Amendment.[238] These scholars would interpret the reasonable expectation of privacy standard more literally than the Supreme Court has to date.[239] Under this interpretation, empirical evidence indicating that Americans expect privacy in a given form of information against government surveillance would weigh heavily in favor of Fourth Amendment protection.[240]

A survey-based approach to the Fourth Amendment's scope would be conceptually straightforward and, based on existing surveys, would produce fairly clear answers.[241] There are now several high-quality surveys of privacy expectations available.[242] That said, an approach that turns on people's literal

---

[238] *See, e.g.*, Bernard Chao et al., *Why Courts Fail to Protect Privacy: Race, Age, Bias, and Technology*, 106 CALIF. L. REV. 263, 276–77 (2018); Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 6 SUP. CT. REV. 205, 226–28 (2015); Christine S. Scott-Hayward et al., *Does Privacy Require Secrecy? Societal Expectations of Privacy in the Digital Age*, 43 AM. J. CRIM. L. 19, 46 (2015). These scholars do not propose wholly substituting empirical evidence for the existing reasonable expectation of privacy test, but rather that such evidence would play a pivotal role in cases where the Court determines that probabilistic expectations should determine the Fourth Amendment's scope. *E.g.*, Kugler & Strahilevitz, *supra*, at 222–23 (integrating survey evidence into existing theories of the reasonable expectation of privacy test). Still, most of these scholars appear to contemplate a robust, even determinative role for survey evidence in Fourth Amendment search law. *See id.* at 228 (contending that a public-opinion-focused Fourth Amendment test is normatively desirable); Chao et al., *supra*, at 276 (arguing that "the most natural reading of the *Katz* reasonable expectations of privacy test" is one that consults surveys of Americans); Scott-Hayward et al., *supra*, at 46 ("[W]hat constitutes a reasonable expectation of privacy by societal standards poses an empirical question." (emphasis omittd)).

[239] *See* Tokson, *supra* note 11, at 49 (discussing *Hudson v. Palmer* and the Court's overt rejection of a literal reasonable expectation of privacy inquiry); *cf. supra* note 238 and accompanying text (arguing for a literal, empirical definition of expectations of privacy).

[240] Chao et al., *supra* note 238, at 276; Kugler & Strahilevitz, *supra* note 238, at 228.

[241] *See* Chao et al., *supra* note 238, at 300–01 tbl.2 (reporting that overwhelming majorities of respondents found a violation of reasonable expectations of privacy for scenarios including GPS tracking, cloud document searches, drone surveillance, and email metadata). Both Kugler and Strahilevitz, *supra* note 238, at 246, 260 tbl.9, and Chao et al., *supra* note 238, at 298 fig.1, show that a majority of respondents considered location tracking to violate a reasonable expectation of privacy.

[242] *See, e.g.*, Chao et al., *supra* note 238, at 298–302; Kugler & Strahilevitz, *supra* note 238,

expectations of privacy is vulnerable to government manipulation and subject to change over time.[243] In addition, surveys of expectations about novel or largely unknown forms of surveillance may not produce meaningful results.

Evidence from existing surveys generally supports protecting electronic data disclosed to third parties. Respondents have indicated that they expect privacy in their cell phone location data,[244] emails,[245] websurfing data,[246] cloud documents,[247] Google maps data,[248] and more.[249] However, particular results may vary based on question phrasing and the details of the surveillance scenarios that pollsters create.[250] Respondents were less likely to report expectations of privacy when hypothetical surveillance conduct was directed at another person rather than themselves.[251] And they were much less likely to report expectations of privacy when the hypothetical surveillance yielded useful evidence.[252] Even with these caveats, existing survey evidence suggests that people expect privacy in electronic data exposed to third parties in many scenarios.[253]

b) Intimacy, Amount, and Cost

Finally, the Supreme Court could interpret the reasonable expectation of privacy test to depend on three factors discussed in *Carpenter* and other cases—the intimacy of the thing searched, the amount of information

---

at 246–60; Scott-Hayward et al., *supra* note 238, at 52–58; Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 335 (2008); Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society"*, 42 DUKE L.J. 727, 732 (1993).

[243] Solove, *supra* note 211, at 1522–24.

[244] Kugler & Strahilevitz, *supra* note 238, at 246.

[245] *Id.* at 260 tbl.9.

[246] Chao et al., *supra* note 238, at 298 fig.1.

[247] *Id.*

[248] *Id.*

[249] *Id.*; Kugler & Strahilevitz, *supra* note 238, at 260.

[250] *E.g.*, Chao et al., *supra* note 238, at 298–299 (discussing biases observed in the study's survey results).

[251] *Id.* at 298–299; Slobogin & Schumacher, *supra* note 242, at 759–61.

[252] Chao et al., *supra* note 238, at 298–299.

[253] *Id.* at 298 fig.1.

obtained, and the cost of the surveillance practice.[254] This doctrinal shift finds support in the Court's Fourth Amendment precedents, which are nearly always decided in accord with the intimacy, amount, and cost of the surveillance at issue.[255] The Court has overtly addressed these factors in many cases and appears to implicitly rely on them in others.[256] By contrast, other factors such as disclosure to third parties or inescapability have had little to no influence on the outcomes of the Court's cases.[257]

The Court could expressly adopt this approach, holding that the intimacy, amount, and cost of surveillance will dictate whether it violates a reasonable expectation of privacy.[258] This framework is relatively easy to

---

[254] Tokson, *supra* note 11 (manuscript at 2–3). In general, the more intimate the place or thing targeted by surveillance, the more likely it is to violate reasonable expectations of privacy. The greater the amount of information sought, the more likely it is to violate reasonable expectations of privacy. Conversely, the more costly the investigation, the less likely it is to violate reasonable expectations of privacy. *Id.*

[255] *Id.*

[256] *See, e.g.*, United States v. Jones, 565 U.S. 400, 429–30 (2012) (Alito, J., concurring in the judgment) (discussing the large amount of data gathered and low cost of long-duration GPS surveillance of a car); *id.* at 415–16 (Sotomayor, J., concurring) (discussing the intimacy, amount, and cost associated with GPS surveillance of a car); Kyllo v. United States, 533 U.S. 27, 37 (2001) ("In the home, our cases show, all details are intimate details, because the entire area is held safe from prying government eyes." (emphasis omitted)); Florida v. Riley, 488 U.S. 445, 446 (1989) ("[T]here is no evidence . . . that intimate details connected with the use of the home or curtilage were observed . . . ."); United States v. Dunn, 480 U.S. 294, 302 (1987) (concluding that police could visually inspect a barn because they "possessed objective data indicating that the barn was not being used for intimate activities of the home"); Dow Chem. Co. v. United States, 476 U.S. 227, 238 (1986) (holding that the surveillance of commercial property via airplane-mounted camera was not a Fourth Amendment search because the "photographs here are not so revealing of intimate details as to raise constitutional concerns"); Oliver v. United States, 466 U.S. 170, 179 (1984) ("[O]pen fields do not provide the setting for those intimate activities that the Amendment is intended to shelter from government interference or surveillance. There is no societal interest in protecting the privacy of those activities, such as the cultivation of crops, that occur in open fields."); United States v. Place, 462 U.S. 696, 707 (1983) (noting the limited amount of information disclosed by a drug dog sniff); United States v. Knotts, 460 U.S. 276, 283 (1983) (discussing the possibility of "twenty-four hour surveillance of any citizen").

[257] *See* Tokson, *supra* note 97.

[258] It might apply this on a case-by-case basis, in accordance with its existing precedents. Tokson, *supra* note 11, at 43. Or it may focus on the potential for new surveillance technologies to gather large volumes of data at low cost, rather than analyzing the

apply and fairly effective at capturing the harms of pervasive surveillance.[259] As for drawbacks, this approach is largely intuitive and non-specific, and may be vulnerable to changes in surveillance practices over time.[260]

Its application to digital records held by third parties may vary depending on the facts of the case, but in general it would offer strong protection for digital information. Government requests for data stored in third-party databases generally involve obtaining large amounts of personal data at low cost.[261] In many contexts, such as smart homes and devices, websurfing, search terms, television and streaming data, ride-sharing services, dating apps, and more, an approach focused on intimacy, amount, and cost would require the government to obtain a warrant before collecting people's information.[262]

Inescapability is not inevitable as a Fourth Amendment standard. There are several viable alternatives for applying the Fourth Amendment in the digital age. While these alternatives have their own drawbacks, most of them offer more protection for personal data, and a more coherent standard, than inescapability.

CONCLUSION

This Article has analyzed the concept of inescapable surveillance and challenged the prevailing wisdom that it should be a determinant of Fourth Amendment protection. Inescapabilty is difficult to apply, inequitable in its treatment of disadvantaged groups, ineffective in its protection of sensitive data, and poorly designed to incentivize beneficial behavior by consumers.

---

circumstances of the particular case. David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 71–72 (2013). This approach would broadly protect virtually all forms of digital information and would be relatively easy to apply, though it risks restraining event-driven or minimal police investigations of non-intimate data.

[259] Tokson, *supra* note 11, at 43.

[260] *Id.* at 43–44.

[261] Gray & Citron, *supra* note 258, at 114.

[262] *See* Tokson, *supra* note 11, at 47 (discussing several of these technologies and assessing the likely intimacy, amount, and cost associated with associated surveillance practices).

In light of inescapability's conceptual, practical, and normative flaws, lower courts should avoid its use in future Fourth Amendment cases. Courts should focus instead on the revealing and extensive nature of the government surveillance at issue. These were the factors that drove the result in *Carpenter*, and they should set the path of Fourth Amendment law in the near term.

Going forward, the Supreme Court should consider whether the time has come to adopt a new paradigm for Fourth Amendment law in the digital age. There are several alternatives that avoid relying on inescapability and that may be more effective than the current test. Even if it retains the existing framework, the Court should reject inescapability as a measure of constitutional protection. An inescapability standard threatens to eliminate privacy rights in a wide variety of personal data. There is still time to choose a better path for Fourth Amendment law.