Is Google a State Agent?

David Gray*

27 STAN. TECH. L. REV 206 (2024)

ABSTRACT

As Justice Samuel Alito has lamented, "today, some of the greatest threats to individual privacy may come from powerful private companies that collect and sometimes misuse vast quantities of data about the lives of ordinary Americans," but the Fourth Amendment offers no protection whatsoever because "it restricts the conduct of the Federal Government and the States, [but] does not apply to private actors." He is not alone in his frustration. Professor Shoshana Zuboff points out that we live in an age of "surveillance capitalism" where technology companies gather, aggregate, store, and analyze vast amounts of information, providing them with intimate pictures of our lives and the opportunity to manipulate our thoughts and actions, often to the detriment of our individual lives and democratic society. This all seems, well, "unreasonable." Yet, by virtue of the state agency requirement, the Fourth Amendment seems to be stuck on the sidelines. Or is it?

This Article challenges the unstated premise in Justice Alito's syllogistic dirge: that powerful technology companies who threaten "the right of the people to be secure . . . against unreasonable searches" are not state agents for purposes of the Fourth Amendment. As we shall see, many of these "private" [1] *companies are state agents under well-established Fourth Amendment doctrine. They routinely share the fruits of their surveillance activities with the government, which has come to expect to benefit from "private" searches. Whether willing or unwilling they are, as privacy advocate Chris Hoofnagle has described them, "Big Brother's little helpers." Separately, many of these*

---

* Jacob A. France Professor of Criminal Jurisprudence, University of Maryland, Francis King Carey School of Law. My thanks to those who offered comments during presentations at the Joel R. Reidenberg Northeast Privacy Scholars Workshop, the University of Basel, the Texas Tech Criminal Law Symposium, the University of Maryland, and the Constitutional Law Schmooze, including Chaz Arnett, Sara Sun Beale, Steve Bellovin, Kiel Brennan-Marquez, Madiha Choksi, Sherman Clark, Melodi Dincer, Sabine Gless, Mark Graber, Orin Kerr, Arnold Loewy, Michael Mannheimer, Scott Mulligan, Natalie Ram, Andrea Roth, Katherine Sandberg, Matiangai Sirleaf, Joseph Turow, Jeffrey Vagle, Ari Waldman, and Helena Whalen-Bridge. Cogan Rooney provided outstanding research support.

[1] leaks

"private" surveillants have assumed roles in society once the sole province of governments. During oral argument in Moody v. NetChoice*, Justice Ketanji Brown Jackson gave voice to rising sympathy for the view that, by virtue of the roles powerful social media companies play in contemporary society, they should not be insulated from First Amendment scrutiny based on the "public versus private distinction." This Article argues that they likewise should not evade Fourth Amendment regulation.*

Having argued that powerful "private" surveillants fall within the regulatory compass of the Fourth Amendment, the Article turns to practical consequences. In cases where the deployment and use of technology constitutes a search and there has not been user consent, the question is whether warrants are required. Because much of the surveillance conducted by powerful private companies is not for purposes of advancing normal criminal law enforcement goals, they are unlikely to be subjected to anything like a warrant requirement, at least in the first instance. Rather, what the Fourth Amendment demands are bespoke measures that strike a reasonable balance among legitimate corporate interests, the privacy interests of those surveilled, and public interests in safety and security. The Supreme Court provided one model in Carpenter v. United States*, but there are others. Much depends on the nature of the technology at issue and the privacy, corporate, and government interests at stake.*

TABLE OF CONTENTS

INTRODUCTION

In *Carpenter v. United States*, the Supreme Court held that, before accessing cell site location information gathered and stored by private telecommunication companies, law enforcement officers must secure a warrant.[2] That holding appears to set the stage for a revolution in Fourth Amendment law both by regulating access to a range of new and emerging surveillance technologies and by challenging doctrinal conventions, including the third-party doctrine,[3] the public observation doctrine,[4] and the assumption that Fourth Amendment rights are "personal" rather than collective.[5] The literature is awash with discussions of these potential impacts of *Carpenter*.[6] What has largely been left out of these conversations is the potential impact of *Carpenter* on another bit of received constitutional wisdom: the Fourth Amendment state agency requirement.

In a trenchant dissenting opinion filed in *Carpenter*, Justice Samuel Alito neatly summarizes the Fourth Amendment state agency requirement. "The Fourth Amendment," he writes, "restricts the conduct of the Federal Government and the States; [but] it does not apply to private actors."[7] As

---

[2] *See* 585 U.S. 296, 309–10, 319 (2018).

[3] *See id.* at 309–10, 313–16.

[4] *See id.* at 309–13.

[5] *See* David Gray, *Collective Rights and the Fourth Amendment After Carpenter*, 79 MD. L. REV. 66, 67–85 (2019). The Court's willingness to embrace the collective dimensions of Fourth Amendment rights are evident in both the majority opinion and dissenting opinions by Justices Anthony Kennedy and Clarence Thomas. *See Carpenter*, 585 U.S. at 300–06, 312; *id.* at 327–28 (Kennedy, J., dissenting); *id.* at 351–54 (Thomas, J., dissenting). Prior to *Carpenter*, the Court seemed committed to the view that Fourth Amendment rights are purely personal. *See, e.g.*, Rakas v. Illinois, 439 U.S. 128, 133–40 (1978) ("Fourth Amendment rights are personal in nature . . . ."); Katz v. United States, 389 U.S. 347, 350 (1967) (stating that the Fourth Amendment "protects individual privacy against certain kinds of governmental intrusion"). This is despite the fact that the text of the Amendment guarantees the "right of the people" rather than the "rights of persons." *See* DAVID GRAY, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE 146-56 (2017) [hereinafter GRAY, AGE OF SURVEILLANCE]; David Gray, *The Fourth Amendment Categorical Imperative*, 116 MICH. L. REV. ONLINE 14, 31–34 (2017) [hereinafter Gray, *Categorical Imperative*]; David Gray, *Fourth Amendment Remedies as Rights: The Warrant Requirement*, 96 B.U. L. REV. 425, 444–57 (2016); David Gray, *Dangerous Dicta*, 72 WASH. & LEE. L. REV. 1181 (2015). In addition to rules governing Fourth Amendment "standing," the assumption that Fourth Amendment rights are personal rather than collective underwrites a number of frequently criticized doctrines, including the third-party and public observation doctrines. *See, e.g.*, GRAY, AGE OF SURVEILLANCE, *supra*, at 78–92; David Gray, *Collective Standing Under the Fourth Amendment*, 55 AM. CRIM. L. REV. 77, 77–78, 86–97 (2018); Shima Baradaran, *Rebalancing the Fourth Amendment*, 102 GEO. L.J. 1, 4–8 (2013).

[6] *See supra* note 5.

[7] *Carpenter*, 585 U.S. at 386 (Alito, J., dissenting); *see also* Edmonson v. Leesville Concrete Co., Inc., 500 U.S. 614, 619 (1991) ("The Constitution's protections of individual liberty and equal protection apply in general only to action by the government.").

Justice Alito goes on to explain, this requirement dramatically limits the revolutionary potential of *Carpenter* and the scope of protections guaranteed by the Fourth Amendment itself. While the Fourth Amendment may well limit the ability of police officers to deploy and use surveillance technologies either directly or by "leverag[ing] the technology of a wireless carrier,"[8] "today, some of the greatest threats to individual privacy may come from powerful private companies that collect and sometimes misuse vast quantities of data about the lives of ordinary Americans." [9] Justice Alito's concerns echo widespread concerns that many of these corporations and their technologies play a more central role in our lives and pose more immediate threats to our privacy, autonomy, and democratic institutions than state agents like the police.[10] Despite these threats, Justice Alito reminds us, the Fourth Amendment offers no protections against these threats precisely because they come from "private" actors; and the Fourth Amendment only regulates state agents.[11]

Take, as an example, cellphone service providers' capacity to track their customers' locations through their cell tower networks—the technology at issue in *Carpenter*. Writing for the Court in *Carpenter*, Chief Justice John Roberts explains how cell site location tracking "provides an all-encompassing record of the holder's whereabouts," opening "an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" [12] Cellphone companies' ability to track us is not just in the moment, but also historical, allowing cellular service providers to document where we have been going for months back, and even years. [13] As the Chief Justice acknowledges, telecommunication companies gather and store this location information for

---

[8] *Carpenter*, 585 U.S. at 309–10.

[9] *Id.* at 386 (Alito, J., dissenting).

[10] *See generally* FRANK PASQUALE, THE BLACK BOX SOCIETY (2015) (discussing the effects of Big Data and algorithmic decision making on consumers); Jonathan Haidt, *Yes, Social Media Really Is Undermining Democracy*, ATLANTIC (July 28, 2022), https://perma.cc/UJC8-NSKV; Lauren Willis, *Deception by Design*, 34 HARV. J. L. & TECH. 115 (2020) (explaining the role of "dark patterns" in manipulating consumers); *see also* Brett Milano, *The Algorithm Has Primacy Over Media . . . over Each of Us, and It Controls What We Do,* HARV. L. TODAY (Nov. 18, 2001), https://perma.cc/V2CV-9SDJ (reporting on an academic panel exploring the effects of social media algorithms on democracy); Dean DeChiaro, *Social Media Algorithms Threaten Democracy, Experts Tell Senators*, ROLL CALL (Apr. 27, 2021), https://perma.cc/KCB7-2SHX (reporting on a Senate hearing exploring the effects of social media on democracy).

[11] *Carpenter*, 585 U.S. at 386 (Alito, J., dissenting).

[12] *Id.* at 311 (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

[13] *See id.*

their own "commercial purposes," but that "does not negate" the privacy interests at stake.[14] These detailed location histories still ''hold for many Americans the privacies of life;" and, because "location information is continually logged for all of the 400 million devices in the United States . . . this newfound tracking capacity runs against everyone."[15] Scary stuff; and all the more unsettling because, as Justice Alito warns, cellphone service providers and their business partners can and do misuse these troves of private information.[16]

After *Carpenter*, government agents will need to secure a warrant before they can gain access to historical cell site data. But, as Justice Alito rightly points out, *Carpenter* sets no limits at all on cellphone companies' ability to either track their customers or sell that information to corporate third parties, such as data brokers and marketers.[17] By virtue of the state agency requirement, these kinds of privately operated mass surveillance programs are completely immune from Fourth Amendment regulation.[18] Law enforcement may need a warrant to access cell site location records, but T-Mobile, Sprint, AT&T, and Verizon face no constitutional constraints when they decide to gather, aggregate, store, analyze, and exploit cell site location information.[19] They retain unfettered discretion to exploit our intimate relationships with our phones in order to track us all day, every day, and document in intimate detail our locations and movements as if each of us is wearing an "ankle monitor."[20]

The problem of constitutionally unregulated corporate surveillance is not limited to cellphone companies. For years, Google gathered and stored location information through applications like Google Maps.[21] So, too, do many social

---

[14] *Id.*

[15] *Id.* at 311–12; *see also* United States v. Chatrie, 590 F. Supp. 3d 901, 925 (E.D. Va. 2022) (noting that location searches using geofence technology implicate the same concerns raised in *Carpenter*)

[16] *See* Jennifer Valentino-DeVries, *How Your Phone Is* Used *to Track You*, N.Y. TIMES (Aug. 10, 2020), https://perma.cc/5F54-XBQ5; Lily Hay Newman, *Carriers Swore They'd Stop Selling Location Data. Will They Ever?*, WIRED (Jan. 9, 2019, 7:43 PM), https://perma.cc/AP23-K87Y; Jennifer Valentino-DeVries et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), https://perma.cc/RQ5D-L7DP; Sarah Krouse, *5 Ways Companies Use Your Cellphone Location Data*, WALL ST. J. (July 15, 2018, 9:00 AM ET), https://perma.cc/Q4RR-XTNY.

[17] *See Carpenter*, 585 U.S. at 385–86 (Alito, J., dissenting).

[18] *Cf. id.* at 386 (Alito, J., dissenting) (cautioning that if the Court's "decision encourages the public to think that this Court can protect them from this looming threat to their privacy, the decision will mislead as well as disrupt").

[19] *See id.* at 311–12, 315.

[20] *Id.* at 312.

[21] *See* Cullen Seltzer, *Google Knows Where* You've *Been. Should It Tell the Police?*, SLATE

media apps like Facebook, Instagram, X, and TikTok.[22] Internet service providers (ISPs) like Comcast along with web browsers like Chrome and Edge gather and store comprehensive details about where we go online, what we do, and what information we consume.[23] Social media platforms often have access to information about our online activities in addition to the intricate web of associations that form our personal and professional networks.[24] The records produced by these corporate surveillance programs reveal at least as much in terms of intimate details about our lives as do cell site location records.[25] In fact, information about our online activities may reveal even more about us and our private lives than where we go in the real world.[26] They may even pose challenges for our democracy.[27] But, by virtue of the state agency requirement,

---

(May 16, 2022, 11:04 AM), https://perma.cc/NL7F-UBPM; Valentino-DeVries, *supra* note 16; Daisuke Wakabayashi, *Google Sets Limit on How Long It Will Store Some Data*, N.Y. TIMES (June 24, 2020), https://perma.cc/CH47-229D. Google offers guidance for users who want to exercise some control over their location data. *See Manage Your Android Device's Location Settings*, GOOGLE, https://perma.cc/66SX-5SS9. In December 2023, Google announced that it would shift storage of location information from its servers to users' devices or encrypted cloud backup. *See* Rob Pegoraro, *Google Maps Location Data to Be Stored on Your Device, Not the Cloud*, PC MAG (Dec. 12, 2023), https://perma.cc/D7RH-6N9T.

[22] Max Mason, Amelia Adams, & Garry McNab, *Tik Tok Admits Collecting Location Data*, AUS. FIN. REV., Mar. 25, 2023, https://perma.cc/9297-AR7D ("An analysis of the code underpinning the TikTok app reveals that, contrary to the company's previous claims, it collects a full suite of location data . . . ."); *What Types of Apps Track Your Location?*, MCAFEE, https://perma.cc/6B45-B38F ("Many popular social media platforms such as Facebook, Instagram, and Snapchat use location tagging features. These features allow users to share their location with others or add a location tag to their posts. Furthermore, these platforms often have a 'Nearby Friends' or 'Find Friends' function, where users can find other users who are in close proximity.").

[23] *See* United States v. Chatrie, 590 F. Supp. 3d 901, 907–11 (E.D. Va. 2022); Natasha Singer & Jason Karaian, *Americans Flunked This Test on Online Privacy*, N.Y. TIMES, https://perma.cc/KW33-J9S8 (Feb. 15, 2023); Cecilia Kang, *Broadband Providers Will Need Permission to Collect Private Data*, N.Y. TIMES (Oct. 27, 2016), https://perma.cc/7NBD-BNFW (describing the limited scope of FCC rules).

[24] *See* Brian X. Chen & Daisuke Wakabayashi, *You're Still Being Tracked on the Internet, Just in a Different Way*, N.Y. TIMES (Apr. 6, 2022), https://perma.cc/5LX6-43PK (explaining how social media sites mine user information).

[25] *See* Kashmir Hill, *How Your Browsing History Is Like a Fingerprint*, FORBES (Aug. 1, 2012, 2:18 PM EDT), https://perma.cc/N3V3-QUDY

[26] *See generally* SETH STEPHENS-DAVIDOWITZ, EVERYBODY LIES: BIG DATA, NEW DATA, AND WHAT THE INTERNET CAN TELL US ABOUT WHO WE REALLY ARE (2017) (describing how online activities reveal intimate details about who we are, how we think, and what we do that we often hide from the real world); *cf.* Alex Marthews & Catherine Tucker, *The Impact of Online Surveillance on Behavior*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 437 (David Gray & Stephen Henderson eds., 2017) (documenting changes in search terms used by Google users after Snowden revelations suggesting concerns about revealing online behavior in the real world).

[27] *See* CATHY O'NEILL, WEAPONS OF MATH DESTRUCTION: HOW BIG DATA INCREASES INEQUALITY AND

the Fourth Amendment has nothing to say about how these programs gather, store, and exploit information.

And then, there is the fact that our homes are increasingly populated by corporate spies in the form of internet-connected devices that constitute the "internet of things" (IoT). For example, Amazon has developed an ecosystem of Alexa-enabled speakers, [28] lighting, [29] televisions, [30] alarm clocks, [31] thermostats,[32] smartphones,[33] dashboard cameras,[34] and earbuds.[35] Many of these devices are equipped with microphones that utilize voice recognition, allowing users to order granola, queue up music, turn on the television, compose emails, adjust the temperature, and even open their front doors.[36] The power is almost biblical—"And Fred said 'Let there be light!' and there was (Hue)light!"[37] But that power comes with a cost.[38] The price we pay is allowing Amazon and its corporate partners access to the private and intimate spheres comprising our homes and spaces around our homes.[39] That access implicates

---

THREATENS DEMOCRACY (2017) (describing how opaque, unregulated, and difficult to challenge algorithmic decisions undercut democratic society by reproducing and amplifying inequality); Mark Harris, *A Peek Inside the FBI's Unprecedented January 6 Geofence Dragnet*, WIRED (Nov. 28, 2022, 7:00 AM), https://perma.cc/E39C-ZK4H; Shoshana Zuboff, *The Coup We Are Not Talking About*, N.Y. TIMES (Jan. 29, 2021), https://perma.cc/2FP8-58GA (explaining the threats to democracy posed by ubiquitous public and private surveillance); Jon Swartz, *Justice Department Demand for Data on 1.3M Anti-Trump Protesters Sparks Debate*, USA TODAY, https://perma.cc/5KX6-2YLL (Aug. 16, 2017, 9:44 AM ET) (reporting on the Justice Department's efforts to get user information from disruptj20.org).

[28] *See* Kate Kozuch, *The Best Alexa Speakers in 2024*, TOM'S GUIDE, https://perma.cc/3XKV-QQWX (Mar. 26, 2024).

[29] *See Brilliant New Ways to See More*, RING, https://perma.cc/3SS6-K7EA.

[30] *See Smart TVs with Alexa Built-In*, BEST BUY, https://perma.cc/V4WT-4T6V.

[31] *See Echo Dot (4th Gen)*, AMAZON, https://perma.cc/3GUW-9AA5.

[32] *See Amazon Smart Thermostat*, AMAZON, https://perma.cc/7R4J-F2QS.

[33] *See Alexa Built-In Phones*, AMAZON, https://perma.cc/SR7H-BY2V.

[34] *See* Dan Seifert, *Ring Announces New Line of Security Cameras for Cars*, THE VERGE (Sept. 24, 2020, 10:27 AM PDT), https://perma.cc/H25M-AMGC.

[35] *See Echo Buds with Noise Cancellation*, AMAZON, https://perma.cc/4NYF-ZGFX.

[36] *See Schlage Encode Smart WiFi Deadbolt with Camelot Trim*, RING, https://perma.cc/7QNT-GL6Z.

[37] Hue is a line of Bluetooth enabled lightbulbs and fixtures that can be controlled with Alexa. *See Philips Hue and Amazon Alexa*, PHILLIPS HUE, https://perma.cc/5GEL-U98D.

[38] As Justice Alito put the point, "[n]ew technology may provide increased convenience or security at the expense of privacy." United States v. Jones, 565 U.S. 400, 427 (2012) (Alito, J., concurring).

[39] For example, in 2023, the Federal Trade Commission documented how Amazon was providing its employees and third party contractors with visual and auditory access to users' homes. *See* Lesley Fair, *Not Home Alone: FTC Says Ring's Lax Practices Led to Disturbing Violations of Users' Privacy and Security*, FED. TRADE COMM'N (May 31, 2023),

not just our privacy, but the privacy of those who visit or even walk by Amazon-infested spaces.[40] Exploitation of the information shared with Alexa and its ilk is inevitable—in fact, exploitation is inherent in their design.[41] But, as Justice Alito reminds us, they are immune to Fourth Amendment regulation because they are deployed and operated by private corporations.

All of this seems to leave us with a rather depressing set of options. We might urge legislative action,[42] but Congress and most state legislatures have failed to pass comprehensive privacy laws.[43] We might refuse to use these technologies, but it hardly seems right to expect anyone to choose between reasonable expectations of privacy and full participation in modern life.[44] We could just submit ourselves to the exploitation and control of our corporate overlords, but that seems like a wholly unacceptable sacrifice of autonomy and democratic citizenship. Surely there is a better way.

This Article argues that we already have a tool well suited to the task of forging reasonable compromises among the various interests at stake when citizens face the prospect of invasive surveillance: the Fourth Amendment. The problem, as Justice Alito reminds us, is the state agency requirement. I have

---

https://perma.cc/8GF6-MPUG. That same year, it charged Amazon with illegally recording, storing, and exploiting the voices of children in users' homes. *FTC and DOJ Charge Amazon with Violating Children's Privacy Law by Keeping Kids' Alexa Voice Recordings Forever and Undermining Parents' Deletion Requests*, FED. TRADE COMM'N (May 31. 2023), https://perma.cc/8LAP-VYSM. Other use of technology can similarly implicate privacy in intimate spheres of life; for example, many wearable devices monitor menstrual cycles. *See Track You Period with Cycle Tracking*, APPLE, https://perma.cc/RAA2-98YC.

[40] Consider Ring's monitoring of public spaces. *See* Dan Harwell, *Doorbell-Camera Firm Ring Has Partnered with 400 Police Forces, Extending Surveillance Concerns*, WASH. POST (Aug. 28, 2019, 6:53 PM EDT), https://perma.cc/BP64-BR3B; *see also* Christina Jelski, *Amazon's Alexa Can Be an Unwelcome Hotel Roommate*, TRAVEL WKLY. (Feb. 19, 2019), https://perma.cc/LLH6-DZK5 (reporting on how Alexa devices impact the privacy of hotel guests); Jay Stanley, *The Privacy Threat from Always-On Microphones Like the Amazon Echo*, ACLU NEWS (Jan. 13, 2017), https://perma.cc/3LHA-MBJG (describing how guests at a dinner party were affected by knowledge that the host's Alexa device was monitoring their conversation).

[41] *See* Niraj Dawar, *Marketing in the Age of Alexa*, HARV. BUS. REV. (May-June 2018), https://perma.cc/3RXK-4U3N ("A platform serves consumers by constantly anticipating their needs. To do that it must collect granular data on their purchasing patterns and product use and try to understand their goals . . . .").

[42] *See, e.g.*, Carpenter v. United States, 585 U.S. 296, 386 (2018) (Alito, J., dissenting) (contending that "[l]egislation is much preferable to the development of an entirely new body of Fourth Amendment caselaw").

[43] A notable exception is California, which has passed two important privacy laws in recent years, the California Consumer Privacy Act (2018), CAL. CIV. CODE §§ 1798.100-.199, and the California Privacy Rights Act, CAL. CIV. CODE §§ 1798.99.28-.40 (effective Jan. 1, 2023).

[44] *See Carpenter*, 585 U.S. at 298 ("[C]ell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society." (quoting Riley v. California, 573 U.S. 373, 385 (2014))).

argued elsewhere that there are good textual and historical reasons to be skeptical about the Fourth Amendment state agency requirement.[45] That work suggests that we abandon or dramatically alter our commitment to the state agency requirement itself.[46] This Article asks a different question: Are there good reasons under existing doctrine to believe that many of the most powerful "private" companies that engage in the kinds of broad, indiscriminate surveillance practices most likely to threaten the security of the people are, in fact, state agents? I think there are.

The argument proceeds in four parts. Part I sets the stage by providing a brief overview of the Fourth Amendment state agency requirement including the well-established doctrinal test used to determine whether otherwise private entities are state agents for purposes of the Fourth Amendment. Part II applies this doctrinal test to some of the "powerful private companies that collect and sometimes misuse vast quantities of data about the lives of ordinary Americans."[47] It concludes that many of these companies are acting as state agents when they surveil their customers, not to mention innocent members of the public. Sometimes they even recruit their customers to participate in the surveillance of others, effectively making customers state agents as well. Part III puts this conclusion in broader historical context by recalling prior occasions when the Court has required erstwhile private agents to submit to constitutional restraint. The conclusion that companies like Amazon, Meta, and Google are state agents when they engage in surveillance may seem revolutionary. Part IV explores the practical consequences. As we shall see, the sky will not fall if we bring the Fourth Amendment to bear on all state agents, whether .gov's or .com's. More important, however, is the imperative to preserve core protections afforded by the Fourth Amendment's imperative that "the right of the people to be secure in their persons, houses, papers, and effects *shall not* be violated."[48] That command is without exception, whether the threat comes from government agents directly or through more "circuitous and indirect methods."[49]

---

[45] *See* David Gray, *The Fourth Amendment State Agency Requirement: Some Doubts*, 109 IOWA L. REV. 1487 (2024).
[46] *Id.* at 1494, 1539.
[47] *Carpenter*, 585 U.S. at 386 (Alito, J., dissenting).
[48] U.S. CONST., AMEND. IV (emphasis added).
[49] Byars v. United States, 273 U.S. 28, 32 (1927).

I. THE FOURTH AMENDMENT STATE AGENCY REQUIREMENT

The state agency requirement holds that the Fourth Amendment only regulates government agents.[50] When most of us think about the Fourth Amendment, to the extent we do, we probably have in mind police officers and other law enforcement agents. Certainly, any fan of police procedurals has lost count of the times a police officer went to get a warrant. Relatedly, we have all learned in the last few years about the role of "no-knock" warrants and the dangers they pose to the public.[51] But the Fourth Amendment does not apply only to police officers and others who draw their paychecks from public coffers. It also governs the conduct of individuals whose engagements or associations with government agents make them "an agent or instrument of the Government."[52] Were it otherwise, the government could simply circumvent the Fourth Amendment by designating or incentivizing proxies to conduct searches and seizures;[53] and it is "axiomatic that a state may not induce, encourage[,] or promote private persons to accomplish what it is constitutionally forbidden to accomplish."[54] But how do we determine whether that threshold has been passed? The answer, as is common in the Fourth Amendment context,[55] depends on the facts,[56] and specifically "the degree of the Government's participation in the private party's activities."[57]

---

[50] *Carpenter*, 585 U.S. at 386 (Alito, J., dissenting); *see also* Edmonson v. Leesville Concrete Co., Inc., 500 U.S. 614, 619 (1991) ("The Constitution's protections of individual liberty and equal protection apply in general only to action by the government.").

[51] Breonna Taylor's death at the hands of police officers during a nighttime, no-knock raid on her home is among the most prominent of these cases. *See* Richard A. Oppel Jr., Derrick Bryson Taylor & Nicholas Bogel-Burroughs, *What to Know About Breonna Taylor's Death*, N.Y. TIMES (Dec. 13, 2023), https://perma.cc/5WWB-JXRW.

[52] Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 614 (1989) ("Although the Fourth Amendment does not apply to a search or seizure, even an arbitrary one, effected by a private party on his own initiative, the Amendment protects against such intrusions if the private party acted as an instrument or agent of the Government.").

[53] *Byars*, 273 U.S. at 33.

[54] Norwood v. Harrison, 413 U.S. 455, 465 (1973) (quoting Lee v. Macon Cnty. Bd. of Ed., 267 F. Supp. 458, 475–76 (M.D. Ala. 1967), *aff'd sub nom.* Wallace v. U S, 389 U.S. 215 (1967)).

[55] *See, e.g.*, Scott v. Harris, 550 U.S. 372, 383 (2007) ("Although respondent's attempt to craft an easy-to-apply legal test in the Fourth Amendment context is admirable, in the end we must still slosh our way through the factbound morass of 'reasonableness.'").

[56] *See Skinner*, 489 U.S. at 614 ("Whether a private party should be deemed an agent or instrument of the Government for Fourth Amendment purposes [is] a question that can only be resolved 'in light of all the circumstances.'" (citations omitted) (quoting Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971))); *cf.* Burton v. Wilmington Parking Auth., 365 U.S. 715, 722 (1961) ("Only by sifting facts and weighing circumstances can the nonobvious involvement of the State in private conduct be attributed its true significance.").

[57] *Skinner*, 489 U.S. at 614 (citations omitted).

The test courts apply when determining whether a private party is a state agent for purposes of the Fourth Amendment derives from well-established common law rules governing agency.[58] The question is whether, "in light of all the circumstances of the case," that party "must be regarded as having acted as an 'instrument' or agent of the state" when conducting a search or seizure;[59] but courts must be "vigilant to scrutinize the attendant facts with an eye to detect and a hand to prevent violations of the Constitution by circuitous and indirect methods."[60] Degradation of rights by proxy is degradation of rights nonetheless.

A private party acting spontaneously and "wholly on her own initiative" is likely not acting as an agent of the state.[61] However, the government does not need to order, direct, compel, request, or even be "the moving force of the search"[62] in order to bring the conduct of a "private" actor within the compass of Fourth Amendment regulation.[63] Likewise, the search does not need to be done for the sole or even primary purpose of advancing law enforcement or other government interests[64]—although either government direction or a "private" agent's explicit aim to assist law enforcement would certainly do.[65] All that is necessary is "clear indices of the Government's encouragement, endorsement, and participation."[66] Among the relevant factors to consider are whether the government "coerce[d]," "dominate[d]," or "direct[ed]" a search by explicit or "subtle" means;[67] and courts also look to whether the party acted under the authority of a statute,[68] and whether the government "removed . . .

[58] *See* United States v. Ackerman, 831 F.3d 1292, 1300–01 (10th Cir. 2016).
[59] *Coolidge*, 403 U.S. at 487.
[60] Byars v. United States, 273 U.S. 28, 32 (1927).
[61] *Coolidge*, 403 U.S. at 487, 490.
[62] Lustig v. United States, 338 U.S. 74, 78 (1949).
[63] *See* Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 615 (1989) ("The fact that the Government has not compelled a private party to perform a search does not, by itself, establish that the search is a private one.").
[64] *See Lustig*, 338 U.S. at 78.
[65] *See Byars*, 273 U.S. at 32–33 (noting that where parties to a search know there is a chance that "something would be disclosed of official interest to [a federal officer]," the "effect" is the same as if it was the federal officer's own "undertaking").
[66] *Skinner*, 489 U.S. at 615–16.
[67] Coolidge v. New Hampshire, 403 U.S. 443, 489 (1971).
[68] *See Skinner*, 489 U.S. at 615; Gambino v. United States, 275 U.S. 310, 316–17 (1927).

legal barriers" to a search,[69] "made plain" its interests in a search,[70] manifested a "desire to share the fruits" of a search,[71] or helped evaluate the evidentiary value of materials discovered during a search.[72]

What government agents know and when they know it also matters. If the government does not have advanced notice of a search conducted by a "private" actor, then that makes a finding of state agency less likely.[73] On the other hand, if a government employee knows or has reason to know that a private party is conducting a search, and the government hopes it will share in the proceeds of that search, then the Fourth Amendment is more likely to apply.[74] The intentions of a private party are also relevant.[75] A private party acting wholly on their own initiative without any purpose of promoting law enforcement or other government interests is less likely to be deemed a state agent[76] than those acting with the intention of securing evidence for a criminal investigation[77]—particularly where government agents have prior knowledge

---

[69] *Skinner*, 489 U.S. at 615. *But see* Jackson v. Metropolitan Edison, 419 U.S. 345, 350 (1974) ("The mere fact that a business is subject to state regulation does not by itself convert its action into that of the State for purposes of the Fourteenth Amendment.").

[70] *Skinner*, 489 U.S. at 615; *see also* Lustig v. United States, 338 U.S. 74, 77 (1949) (finding federal action where a Secret Service agent "remained at police headquarters" during a search conducted by local police because "he 'was curious to see what they would find'").

[71] *Skinner*, 489 U.S. at 615.

[72] *See Lustig*, 338 U.S. at 78.

[73] *See* Burdeau v. McDowell, 256 U.S. 465, 475 (1921) (finding no state agency where, among other factors, "no official of the federal government had . . . any knowledge [of the search] until several months after the property had been taken"); United States v. Pierce, 893 F.2d 669, 673 (5th Cir. 1990) (holding that for a search by a private person to trigger Fourth Amendment protection, the government must have known about the search in advance).

[74] *See Skinner*, 489 U.S. at 615–16; *Lustig*, 338 U.S. at 77; *see also Pierce*, 893 F.2d at 673 ("[T]he two critical factors in an 'instrument or agent' analysis are: (1) whether the government knew of and acquiesced in the intrusive conduct, and (2) whether the party performing the search intended to assist law enforcement efforts or to further his own ends.").

[75] *See* United States v. Miller, 688 F.2d 652, 657 (9th Cir. 1982) (citing as a "critical" factor in the "instrument or agent analysis . . . whether the party performing the search intended to assist law enforcement efforts or to further his own ends"); Kiel Brennan-Marquez, *The Constitutional Limits of Private Surveillance*, 66 KAN. L. REV. 485, 516 (2018) ("Either way, the upshot is the same: if private surveillance is guided by a desire to assist law enforcement, that should be germane to the Fourth Amendment analysis.").

[76] *See* United States v. Jacobsen, 466 U.S. 109, 110 (1984); Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971); *Pierce*, 893 F.2d at 674.

[77] *See* Gambino v. United States, 275 U.S. 310, 316–17 (1927); United States v. Souza, 223 F.3d 1197, 1201 (10th Cir. 2000) (holding that whether a private entity is acting as a state agent under the Fourth Amendment is a function of "1) whether the government knew of and acquiesced in the intrusive conduct, and 2) whether the party performing the search intended to assist law enforcement efforts or to further his own ends" (quoting Pleasant v.

of the search or the government effectively ratifies a search by exploiting the fruits.[78] So, too, one-off actors who provide information to law enforcement are less likely to be treated as state actors[79] than repeat players who frequently or routinely report to law enforcement.[80]

One of the Court's clearest statements of the rules governing state agency in the Fourth Amendment context appears in *Skinner v. Railway Labor Executives' Association*.[81] There, the Secretary of Transportation, acting pursuant to broad authority granted by the Federal Railroad Safety Act of 1970, promulgated regulations requiring private railroad carriers to test the blood and urine of employees involved in train accidents.[82] Those regulations also granted railroads discretionary authority to conduct breath and urine tests in other circumstances.[83] Writing for the Court, Justice Anthony Kennedy concluded that the railroads clearly acted as state agents when conducting federally mandated tests.[84] While admitting that discretionary testing licensed by federal regulations presented a closer question, the Court was "unwilling to conclude . . . that breath and urine tests required by private railroads in reliance

---

Lovell, 876 F.2d 787, 797 (10th Cir. 1989))); United States v. Walther, 652 F.2d 788, 791, 793 (9th Cir. 1981) (holding that an airline employee acted as government agent when he expected a DEA reward for his actions and the agency had encouraged him).

[78] *See Gambino*, 275 U.S. at 316–17; United States v. Silva , 554 F.3d 13, 18 (1st Cir. 2009) (focusing on "the extent of the government's role in instigating or participating in the search, its intent and the degree of control it exercises over the search and the private party, and the extent to which the private party aims primarily to help the government or to serve its own interests" (quoting United States v. Pervaz, 118 F.3d 1, 6 (1st Cir. 1997))); United States v. Bazan, 807 F.2d 1200 (5th Cir. 1986) (inquiring into "whether the government knew of and acquiesced in the intrusive conduct"); United States v. Miller, 688 F.2d 652, 657 (9th Cir. 1982) (citing as a "critical" factor in the "instrument or agent analysis . . . whether the government knew of and acquiesced in the intrusive conduct"); United States v. Walther, 652 F.2d 788, 792 (9th Cir. 1981); *cf.* Jackson v. Metro. Edison Co., 419 U.S. 345, 369 (1974) (Marshall, J., dissenting) ("[S]tate authorization and approval of 'private' conduct has been held to support a finding of state action.").

[79] *See Coolidge*, 403 U.S. at 489–90 (holding that there was no state agency where a wife conducted a search of the home for her husband's guns and clothes in the context of a single engagement with law enforcement and out of "spontaneous, good faith").

[80] *See* Brennan-Marquez, *supra* note 75, at 515 ; *cf.* United States v. Henry, 447 U.S. 264, 270–71 (1980) (finding that a jailhouse snitch who frequently provided information to law enforcement in exchange for consideration was working on a "contingent-fee basis" when, absent any specific instruction, he deliberately elicited incriminating statements from a fellow inmate in violation of the Sixth Amendment).

[81] 489 U.S. 602 (1989). Then-Judge Gorsuch has commented that *Skinner* is "the Supreme Court's leading Fourth Amendment agency case." United States v. Ackerman, 831 F.3d 1292, 1302 (10th Cir. 2016).

[82] *Skinner*, 489 U.S. at 606–12.

[83] *Id.*

[84] *Id.* at 614.

on [regulatory permission] will not implicate the Fourth Amendment."[85] Citing the fact that "[t]he Government has removed all legal barriers to the testing," and clear evidence that the government had "not only [a] strong preference for testing, but also [a] desire to share the fruits of such intrusions," the Court concluded that private train operators, when conducting discretionary testing, were acting as state agents for purposes of the Fourth Amendment.[86] The Court reached this holding despite the fact that the railroads were not instructed to conduct these tests and had strong independent business reasons for monitoring their employees' use of drugs and alcohol on the job.[87]

With this short primer in place, Part II turns to the question whether Google, Amazon, and other technology companies who gather, aggregate, store, and exploit vast amounts of information about their customers and other members of the public are state agents for purposes of the Fourth Amendment.

II. MODERN TECHNOLOGY COMPANIES AND THE FOURTH AMENDMENT STATE AGENCY DOCTRINE

This Part argues that there is good reason to think that many technology companies are state agents for purposes of the Fourth Amendment when they engage in the kinds of conduct most likely to threaten our security and privacy. In some cases, the conclusion is easy because the private companies are acting under a statutory mandate.[88] In others, there no mandate, but there are explicit—if sometimes secret—partnerships between the companies and government entities.[89] And then there are myriad examples where there is neither a mandate nor an explicit partnership, but private entities conduct surveillance or gather, aggregate, and store information while knowing that government agencies routinely seek to access and exploit the fruits of these efforts.[90] Before we turn to this discussion, however, a proviso is in order.

Whether an actor is a state agent is a threshold question in any Fourth Amendment analysis.[91] Importantly, however, it does not end the analysis.

---

[85] *Id.*
[86] *Id.* at 615–16.
[87] *Id.* at 614, 616.
[88] *See infra* notes 95–100 and accompanying text.
[89] *See infra* notes 103–124 and accompanying text.
[90] *See infra* notes 124–138 and accompanying text.
[91] *See, e.g.*, STEPHEN SALTZBURG, DANIEL CAPRA, & DAVID GRAY, AMERICAN CRIMINAL PROCEDURE 35 (2022). *But see* Gray, *supra note* 45 (arguing that there is no textual or historical basis for maintaining the Fourth Amendment state agency requirement).

Even if a technology company acts as a state agent when building and deploying the capacity to locate cellular phones, gathering, aggregating, and storing telephonic metadata, or monitoring the activities of people in their homes, the activities of the company would only be subject to Fourth Amendment regulation if they constitute "searches."[92] Further, even if the activities constituted "searches," we would still need to determine the form and extent of restraint required by the Fourth Amendment for these searches to be "reasonable."[93] We will have the opportunity to consider these critical downstream questions in Part IV. For now, we will focus our attention on the immediate question: whether some of the "powerful private companies" that pose "some of the greatest threats to individual privacy" are state agents for purposes of the Fourth Amendment when they "collect and sometimes misuse vast quantities of data about the lives of ordinary Americans."[94]

Some private surveillants are state agents by virtue of their statutory relationship to government agencies. For example, cellular service providers and other telecommunications companies operate under statutory obligations similar to those at stake in *Skinner*. The Wireless Communications and Public Safety Act of 1999 (911 Act), along with associated regulations issued by the FCC, require that cellular service providers be able to precisely identify the location of every phone in their networks.[95] In a similar vein, until its expiration in 2020, all telephone service providers operated under a revised version of the infamous Section 215 telephonic metadata program, which required that they gather and store telephonic metadata associated with calls made by and to their customers.[96] FCC regulations still require some telephone service providers to retain call metadata for at least eighteen months.[97] In each of these circumstances, private companies act under the "compulsion of

---

[92] *See* GRAY, AGE OF SURVEILLANCE, *supra* note 5, at 146–56.

[93] *See id.* at 165.

[94] Carpenter v. United States, 585 U.S. 296, 386 (2018) (Alito, J., dissenting).

[95] 47 C.F.R. §§ 9.1-9.3 (2019).

[96] Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline over Monitoring Act of 2015, Pub. L. No. 114–23, § 101, 129 Stat. 268, 269 et seq. (amending 50 U.S.C. § 1861 by requiring telephonic communication companies to preserve call records, produce call records upon receipt of a lawful order, providing compensation for companies, but prohibiting bulk collection of call records). *See also*, Christopher Slobogin, *"Volunteer" Searches*, 85 PITT. L. REV. 1, 10 (2023) (noting that "the USA FREEDOM Act . . . required that [telephonic metadata] be maintained by common carriers" in support of NSA surveillance programs).

[97] 47 C.F.R § 42.6 (2019).

sovereign authority," [98] the government is aware of their activities, and government agents expect to benefit from the fruits of the companies' data collection.[99] These companies are, therefore, acting as state agents when they monitor customer locations and gather call data, even if they may have independent business reasons for gathering that information.[100]

For other technology companies, the nature of their relationships with law enforcement and other government agencies provides compelling evidence that they are state agents for purposes of the Fourth Amendment when they monitor "ordinary Americans," including their customers. Recall from Part I that one factor courts consider when determining whether a private actor is a state agent for purposes of the Fourth Amendment is the nature and history of that actor's relationship with law enforcement. [101] Many of the companies and technologies that pose the greatest threats to privacy have close information-sharing relationships with law enforcement and other government agencies. Consider, as an example, Ring.

Ring is Amazon's Internet-connected surveillance camera and doorbell.[102] In August 2019, journalists revealed that Ring had inked partnerships with hundreds of law enforcement agencies across the country, facilitating police

---

[98] Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 614 (1989).

[99] *See supra* notes 66–80 and accompanying text; *see also* United States v. Canada, 527 F.2d 1374, 1376 (9th Cir. 1975) (holding that airline employees searching luggage pursuant to federal anti-hijacking program are state agents).

[100] *See* United States v. Ackerman, 831 F.3d 1292, 1303 (10th Cir. 2016) ("[T]he common law recognized that agents routinely intend to serve their principals with the further intention to make money for themselves. In *Skinner*, too, the fact that the private railroads had private (economic) reasons for seeking to curb drug abuse by railroad employees—and had sought to do so before the government promulgated its regulations—was no barrier to the Court's determination that the statutory scheme converted the railroads into governmental agents." (citations omitted)); United States v. Leffall, 82 F.3d 343, 347 (10th Cir. 1996) (holding that private entities need not be acting purely out of a subjective motivation to advance government interests to qualify as a state agent). One might argue that performance under these statutory mandates comprises a small component of these companies' business activities. But, even if true, that fact does not diminish the conclusion that they are state actors when performing under these statutory directives. *See* West v. Atkins, 487 U.S. 42, 48–57 (1988) (holding that a private physician working under limited contract with state prison is a state actor while treating prisoners). *Compare* United States v. Canada, 527 F.2d 1374, 1376 (9th Cir. 1975) (holding that airline employees searching luggage pursuant to federal anti-hijacking program are state agents), *with* United States v. Ogden, 485 F.2d 536, 539 (9th Cir. 1973) (holding that an airline employee searching luggage outside the scope of federal anti-hijacking program is not a state agent). *But see* United States v. Pierce, 893 F.2d 669, 674 (5th Cir. 1990) (declining to apply the Fourth Amendment where "airline employees opened [a suspicious] package to further the airline's own ends, not solely to assist law enforcement officers").

[101] *See supra* notes 66–80 and accompanying text.

[102] *See New Battery Doorbell Pro*, AMAZON, https://perma.cc/5ZLD-HZ5P.

access to video and still images taken from millions of doorbell cameras.[103] That kind of explicit agreement almost certainly makes Ring a state agent when it is performing on these agreements—which is to say, all the time. So, too, are Ring customers who grant ongoing access to the Ring-law enforcement partnership. Again, this does not end the Fourth Amendment inquiry. Even if Ring and many of its customers are state agents when deploying and using Ring devices, they very well may not be engaged in conduct that qualifies as a "search" for purposes of the Fourth Amendment. And, even if they were, we would still need to ask questions about what would be required to render those searches "reasonable."

Ring is not alone in establishing ongoing information-sharing relationships with law enforcement. Many other private entities that own or operate video surveillance cameras are also state agents for purposes of the Fourth Amendment when they utilize those cameras to capture, gather, and store images. The conclusion is strongest when it comes to organizations that grant ongoing access to law enforcement agencies. This is an increasingly frequent practice, particularly in municipalities like New York City that operate data integration centers where officers and analysts have access to large networks of surveillance cameras, some of which are owned and operated by private entities. [104] These private entities are crucial partners, allowing law enforcement agencies to expand their surveillance capacities by leveraging "private" security cameras. Some localities even offer financial incentives to private property owners who install security cameras and make them accessible to law enforcement.[105] By virtue of these kinds of close relationships, there can be little doubt that corporations, businesses, and individuals are acting as state agents when they link their surveillance cameras to government networks, although, again, the question whether their surveillance activities constitute "searches" remains open.[106]

---

[103] *See* Dan Harwell, *supra* note 40.

[104] *See* POLICE DEP'T, CITY OF NEW YORK, DOMAIN AWARENESS SYSTEM: IMPACT AND USE POLICY 7 (2021), https://perma.cc/3GY3-S5S6 (referring to "External stakeholders providing NYPD with access to their public-space facing cameras"); POLICE DEP'T, CITY OF NEW YORK, CLOSED CIRCUIT TELEVISION SYSTEMS: IMPACT AND USE POLICY 4 (2021), https://perma.cc/5KBJ-NS7H ("The NYPD does engage in cooperative agreements with external entities that have installed their own CCTV cameras in order to share such footage with the NYPD.").

[105] *See, e.g.*, *Police-Private Security Camera Incentive Program*, MONTGOMERY COUNTY DEP'T OF POLICE, https://perma.cc/GX25-7YYX.

[106] Although it has long been assumed that visual surveillance of movements in public places does not constitute a "search" for purposes of the Fourth Amendment, the Court's holding

Beyond the world of visual surveillance, there are also scores of companies that have ongoing working relationships that facilitate data surveillance by law enforcement and other government agencies.[107] Reportage in the wake of information leaked by Edward Snowden in 2013 documented some of the "handshake agreements" under which telephone service providers like Verizon and AT&T supported the National Security Agency's Section 215 telephonic metadata surveillance program.[108] Information leaked by Snowden also exposed efforts by major technology companies to "stockpile emails, messages, and browser records" in support of government surveillance programs.[109] Apart from the war on terror, *The New York Times* reported in 2013 that AT&T was secretly feeding billions of call records to the government as part of "Hemisphere," a surveillance program aimed at interdicting illegal drugs.[110] Then there are data aggregators, which privacy scholar Chris Hoofnagle has dubbed "Big Brother's little helpers."[111] These companies gather, aggregate, store, analyze, and package data for law enforcement and other government agencies.[112] One of these companies, Geofeedia, scrapes user data from social media sites like Twitter, Facebook, and Instagram, which it then sells to

in *Carpenter* has caused some reconsideration. As an example, in *Beautiful Struggle v. Baltimore Police Department*, the Fourth Circuit applied the Court's reasoning in *Carpenter* to hold that the deployment of planes equipped with high-powered digital cameras to conduct broad, indiscriminate surveillance constitutes a "search" for purposes of the Fourth Amendment. 2 F.4th 330, 342–47 (4th Cir. 2021). Although not at issue in that case, systems of networked surveillance cameras offer law enforcement similar capacities.

[107] *See* Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 112–16 (2018) (documenting the role of "surveillance intermediaries" in amassing data for law enforcement); Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CAL. L. REV. 901, 904, 927–28, 937–38 (2008) (documenting the role of private corporations in conducting surveillance in assistance of the war on terror).

[108] Rozenshtein, *supra* note 107, at 104, 113; *see also* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005), https://perma.cc/A4Z8-76N8.

[109] Rozenshtein, *supra* note 107, at 104–05, 115–16. These kinds of data sharing programs are not new. As Rozenshtein reports, "Project SHAMROCK, which lasted from the end of World War II to its exposure in the mid-1970s, Western Union and other telegraph companies voluntarily provided the NSA with daily copies of most international telegraphs entering or exiting the United States." *Id.* at 113.

[110] Scott Shane & Colin Moynihan, *Drug Agents Use Vast Phone Trove Eclipsing N.S.A.'s*, N.Y. TIMES (Sept. 1, 2013), https://perma.cc/PW57-AW7V; *see also* Adam Schwartz, *AT&T Requires Police to Hide Hemisphere Phone Spying*, ELEC. FRONTIER FOUND. (Oct. 27, 2016), https://perma.cc/P8PJ-AWGS.

[111] Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. 595 (2004).

[112] *See id.* at 596–70.

government agencies interested in tracking political protestors.[113] As Professor Kiel Brennan-Marquez has observed, these kinds of programs are likely to increase in their number and reach "as data analysis subsumes an ever-greater share of traditional police work."[114]

Given their explicit information sharing and contract relationships with law enforcement and other government agencies, there is no doubt that these "private" entities are government agents. True, the government is not compelling them to act, but that is not necessary to establish state action.[115] Certainly, the technology and telecommunication companies that fed data to the National Security Agency and other government agencies under the auspices of these programs were not acting "wholly on their own initiative."[116] But it is enough for purposes of establishing agency that the government is "the moving force" [117] behind Hemisphere and the various national security surveillance programs uncovered in the wake of the Snowden leaks.[118]

The case for agency is stronger still when there are explicit agreements in place. Ring and other private entities that routinely share surveillance video with law enforcement agencies operate under written agreements. So, too, do data aggregators and their government clients. Even in the absence of explicit agreements, there is still good reason to believe that many of the "private" entities that routinely share data, surveillance feeds, and other information with law enforcement are state agents for purposes of the Fourth Amendment. After all, government agents know in advance that these private surveillants are watching, gathering, and storing data and are willing to share what they know with the government;[119] the government has "made plain" its interests in that information[120] and manifested its "desire to share in the fruits" of these

---

[113] See Matt Cagle, *Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color*, ACLU N. CAL. BLOG (Oct. 11, 2016), https://perma.cc/X4GM-ED7E.

[114] Brennan-Marquez, *supra* note 75, at 487.

[115] *See* Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 615 (1989) ("The fact that the Government has not compelled a private party to perform a search does not, by itself, establish that the search is a private one.").

[116] Coolidge v. New Hampshire, 403 U.S. 443, 490 (1971).

[117] Lustig v. United States, 338 U.S. 74, 78 (1949).

[118] *See* Slobogin, *supra* note 96, at 7-8 (arguing that private corporations that supported "Stellarwind" and other NSA surveillance programs revealed by Edward Snowden are state agents for purposes of the Fourth Amendment).

[119] *See Skinner*, 489 U.S. at 615–16; *Lustig*, 338 U.S. at 77; United States v. Pierce, 893 F.2d 669, 669 (5th Cir. 1990).

[120] *Skinner*, 489 U.S. at 615; *see also Lustig*, 338 U.S. at 77.

surveillance efforts.[121] By virtue of the ongoing relationships between the government and the private surveillants, there can be no doubt that the government endorses and ratifies the surveillance and data gathering performed by these "private" parties.[122]

The case is less certain, but still compelling, for private entities who share the fruits of their surveillance or data gathering with the government on a contingent or infrequent rather than ongoing basis.[123] Consider banks. Banks and other financial institutions operate video surveillance systems at least in part to gather evidence for law enforcement in the event of a robbery or other crime on their premises.[124] Law enforcement, in turn, knows that banks operate these systems and fully expects to benefit from the evidence they produce.[125] The same is also true of other private entities that install surveillance systems with an eye toward providing evidence for law enforcement. Obvious examples include cash-intensive businesses such as check-cashing companies, off-track betting locations, and casinos, but might also include convenience stores, corner bodegas, grocery stores, cannabis dispensaries, and any other business that uses surveillance systems as a risk-management tool with an eye toward providing evidence for law enforcement should a crime occur.[126] Most of these businesses will only share surveillance video with law enforcement infrequently, such as when they are victims of crime or their cameras happen to capture information valuable to law enforcement. Nevertheless, motive matters and a primary motive for their deployment and use of surveillance systems is to assist law enforcement should their assistance be needed.

---

[121] *Skinner*, 489 U.S. at 615.

[122] Gambino v. United States, 275 U.S. 310, 316–17 (1927); United States v. Silva, 554 F.3d 13, 18 (1st Cir. 2009); United States v. Bazan, 807 F.2d 1200, 1202–07 (5th Cir. 1986); United States v. Miller, 688 F.2d 652, 657 (9th Cir. 1982); United States v. Walther, 652 F.2d 788, 792 (9th Cir. 1981); Brennan-Marquez, *supra* note 75, at 515.

[123] *See* Brennan-Marquez, *supra* note 75, at 515–16 (noting that "repeated interaction with the police is not strictly necessary" to establish state agency where the private party is acting out of "law enforcement motives" when it transfers information to government agents).

[124] *See Responses to the Problem of Bank Robbery*, ARIZ. STATE UNIV. CTR. FOR PROBLEM-ORIENTED POLICING, https://perma.cc/2ULP-S6YV ("Surveillance images are valuable for police in identifying and apprehending suspects and can aid in prosecution as well. The use of good quality photographs during news broadcasts and on reward programs has contributed to the apprehension of a number of offenders.").

[125] *See id.*; *see also Caught on Camera*, FED. BUREAU OF INVESTIGATION, https://perma.cc/4TJG-2M5G (demonstrating how law enforcement can benefit from security cameras installed by businesses).

[126] *See Private Surveillance Cameras Catching More Criminals*, ABC NEWS (Jan. 25, 2013, 10:01 AM), https://perma.cc/FT9W-BBFS.

There is also a persuasive case to be made that technology companies like Microsoft and Google and Internet service providers like Verizon and Comcast act as state agents for purposes of the Fourth Amendment when they gather and store customer information, including location information and data documenting where customers go and what they do online. Although these companies may not operate under explicit agreements with the government for the expressed purpose of advancing law enforcement interests, by dint of experience they know that law enforcement and other government agents are interested in, and frequently access and exploit, the fruits of their data collection. Government agents likewise know that these companies gather and store copious amounts of customer data and eagerly leverage that data for law enforcement, national security, and other purposes. As examples, Microsoft received almost 25,000 government requests for user information in the last six months of 2020 implicating over 45,000 user accounts;[127] Google fielded over 200,000 government requests for user information relating to over 400,000 accounts during the first half of 2023;[128] and Verizon responded to over 250,000 demands for customer information from domestic law enforcement agencies in 2023.[129]

In addition to frequent requests for user information, Google has also become a go-to source when law enforcement officers want to identify persons in proximity to locations connected to an investigation.[130] In 2020 alone, Google responded to over 10,000 "geofence" requests.[131] Similarly, cellphone providers receive thousands of requests every year for tower-dumps, which document user proximity to specific cell towers.[132] To be sure, these companies

---

[127] *See Law Enforcement Requests Report*, MICROSOFT, https://perma.cc/UM6H-V7GH.

[128] *See Global Requests for User Information*, GOOGLE, https://perma.cc/9GCW-6B8S.

[129] *See Verizon Transparency Reports*, VERIZON, https://perma.cc/ZPH9-EPMD.

[130] *See, e.g.*, United States v. Chatrie, 590 F. Supp. 3d 901, 914 (E.D. Va. 2022) ("Geofence warrants represent 'a novel but rapidly growing [investigatory] technique.'" (alteration in original) (citation omitted)).

[131] *See Supplemental Information on Geofence Warrants in the United States*, GOOGLE, https://perma.cc/9L2S-VL2R.

[132] *See* Emma Lux, *Privacy in the Dumps: Analyzing Cell Tower Dumps Under the Fourth Amendment*, 57 AM. CRIM. L. REV. 109, 109 (2020) ("[G]overnmental collection of cell tower dump location information is becoming ubiquitous, in part because the Supreme Court in *Carpenter v. United States* declined to address whether it triggers Fourth Amendment protection."); Kate Haas, *Cell Tower Dumps: Another Surveillance Technique, Another Set of Unanswered Questions*, ACLU (Mar. 27, 2014), https://perma.cc/V4UA-9XMH ("Cell tower dumps aren't rare. A congressional inquiry found that companies received at least 9,000 tower dump requests in 2012, and in 2013 Verizon alone reported receiving 3,200 such requests.").

do not necessarily *want* to be acting as state agents,[133] but, given the frequency and regularity of government requests for information, law enforcement's obvious awareness and interest in accessing and exploiting the information, and the fact that the companies know that the government will come calling, they seem to qualify as state agents under existing doctrine whether they like it or not.[134]

This analysis adds another dimension to the conclusion that telephone companies like Verizon, Sprint, and AT&T act as state agents when they gather,

---

[133] This fact is amply demonstrated by lawsuits pursued by Apple, Microsoft, and Google resisting government requests, seeking reform of gag orders keeping government requests secret from targets, and seeking to publish statistics regarding government requests for user information. *See, e.g.*, Steve Lohr, *Microsoft Sues Justice Department to Protest Electronic Gag Order Statute*, N.Y. TIMES (Apr. 14, 2016), https://perma.cc/Q6AS-747E.

[134] *See* David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 136–37 (2013) (making this case); *cf*. United States v. Walther, 652 F.2d 788, 792 (9th Cir. 1981) (holding that airline employee who opens luggage in order to determine whether it contains illegal drugs with intent to report his findings to the DEA is a state agent for purposes of the Fourth Amendment). This conclusion runs up against a line of cases holding that technology companies who screen customer files and communications for hashes associated with known images of child pornography are not state agents for purposes of the Fourth Amendment. *See, e.g.*, United States v. Stevenson, 727 F.3d 826, 831 (8th Cir. 2013) (holding that "AOL's voluntary efforts to" thwart child pornography did not make it a state agent solely because "it shares [that goal] with law enforcement"); United States v. Cameron, 699 F.3d 621, 637–38 (1st Cir. 2012) (holding that Yahoo!, Inc., is not acting as a state agent when it searches e-mails for images of child pornography and sends reports to the National Center for Missing and Exploited Children); United States v. DiTomasso, 81 F. Supp. 3d 304, 305 (S.D.N.Y. 2015) (holding chat service provider Omegle is not a government agent when searching customer files for images of child pornography); United States v. Richardson, 607 F.3d 357, 366 (4th Cir. 2010) (holding that AOL is not a state agent when scanning email communications for child pornography because no law enforcement officer or agency asked the provider to search or scan emails); United States v. Keith, 980 F. Supp. 2d 33, 40 (D. Mass. 2013) (same); United States v. Miller, No. 8:15CR172, WL 5824024, at *4 (D. Neb. Oct. 6, 2015) (holding that Google is a "private, for profit entity" and did not become a state agent solely by complying with statutory obligations to report images of child pornography); United States v. Drivdahl, No. CR 13-18-H-DLC, 2014 WL 896734, at *3–4 (D. Mont. Mar. 6, 2014) (holding that Google is not a government agent when scanning for images of child pornography). Bluntly, these cases were wrongly decided. Or, at least, their discussions of state agency are both strained and unnecessary. In keeping with its holding in *Ex parte Jackson*, 96 U.S. 727 (1878), the Supreme Court has long distinguished between the contents of "houses, papers, and effects" and their interiors. Although the analogy is not perfect, the unique hash values used to identify known images of child pornography are akin to the address and markings on the outside of an envelope, which means that deploying technology that reads these hash values is not a "search" for purposes of the Fourth Amendment in that it neither physically intrudes into a constitutionally protected area nor violates reasonable expectations of privacy. In addition, because hash values are unique, and the screening technologies used to monitor for child pornography can only detect the presence of these illegal images, the deployment and use of these technologies is no more a "search" than allowing a reliable drug-dog to sniff the outside of a suitcase to determine whether it contains illegal narcotics. *See* United States v. Place, 462 U.S. 696 (1983).

aggregate, and store customer information, including cell site location information.[135] As the Supreme Court recently acknowledged, investigators regularly access cell site location information in the context of criminal investigations.[136] This routine activity demonstrates that law enforcement knows that cellular service providers gather location information on their customers, that law enforcement expects to benefit from that surveillance, and that cellular service providers are aware of these law enforcement expectations when the companies gather, aggregate, and store cell site location information. This relationship is so close and familiar that telecommunications companies have maintained law enforcement portals to receive and respond to official inquiries, sometimes for a fee.[137] That checks a bunch of the state agency factors. One might argue that cellular service providers would gather and store this information regardless of government expectations,[138] but, as the Supreme Court has explained, that in no way settles the state agency question.[139]

Although the Supreme Court has not squarely addressed the question whether and to what degree technology companies might be state agents under existing Fourth Amendment doctrine, it signaled some sympathy for the possibility with its decision in *Carpenter v. United States*. The question presented there was "how to apply the Fourth Amendment to a new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals."[140] The Court ultimately held that government agents must secure a warrant in order to access these records,[141] but had a very

---

[135] *See supra* notes 95–133 and accompanying text. This theory was at the heart of numerous lawsuits against telecommunications companies filed in the wake of the Snowden revelations. *See, e.g.*, *In re* Nat'l Sec. Agency Telecomm. Recs. Litig., 671 F.3d 881 (9th Cir. 2011). Those cases ultimately were dismissed after the companies were granted immunity under the FISA Amendments Act. *Id.* at 904 (upholding district court's dismissal of claims against telecommunications companies after the Attorney General certified the companies for immunity under Section 802).

[136] *See* Carpenter v. United States, 585 U.S. 296, 301–03 (2018).

[137] *See* Theodoric Meyer, *No Warrant, No Problem: How the Government Can Get Your Digital Data*, PROPUBLICA (June 27, 2014, 10:29 AM EDT), https://perma.cc/QTC5-R9ZL; *see also, e.g.*, *Verizon Security Assistance Team*, VERIZON, https://perma.cc/YCM6-94SF; *Law Enforcement Online Requests*, FACEBOOK, https://perma.cc/4EQM-QB8P; *How Google Handles Government Requests for User Information*, GOOGLE, https://perma.cc/H6ZU-J8VY.

[138] *See, e.g.*, Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971) (noting that if a private party "wholly on her own initiative," conducts a search or seizure, then those "articles would later [be] admissible in evidence").

[139] *See* Skinner v. Ry. Lab. Execs.' Ass'n, 489 U.S. 602, 614, 616 (1989).

[140] *Carpenter*, 585 U.S. at 309.

[141] *See id.* at 316.

difficult time describing the nature of the "new phenomenon"[142] within the bounds of existing doctrine, including the state agency requirement. At times, the Court seemed to assume that government investigators conducted the search when they obtained the data, which made the Fourth Amendment issue one of "access[ing] historical cell phone records that provide a comprehensive chronicle of the user's past movements."[143] In keeping with that view, the Court at one point described itself as holding that "a warrant is required in the rare case where the suspect has a legitimate privacy interest in records held by a third party."[144] At another point, however, the Court implied that it was the cellular service providers who were conducting the search, which made the question presented whether it is a "search" if "the Government . . . leverages the technology of a wireless carrier" to document a user's "physical movements."[145] In answer to that question, the Court held that "[t]he location information obtained from Carpenter's wireless carriers was the product of a search."[146]

Justice Alito's concerns aside, the Court's equivocation on these core issues reflects the fact that many technology and communications companies are so intertwined with law enforcement and national security agencies that they are government actors for purposes of the Fourth Amendment. Perhaps more importantly for present purposes, the Court's efforts in *Carpenter* self-consciously reflect its longstanding commitment to guard against "violations of the Constitution by circuitous and indirect methods." [147] Specifically, the *Carpenter* Court paints a vivid picture of the extent and reach of cell site location as a technology, describing how granting unfettered access to historical cell site location information would expose intimate details of almost everyone's lives.[148] "Only the few without cell phones," the Court writes, "could

---

[142] *Id.* at 309.

[143] *Id.* at 300; *see also id.* at 310 n.3 ("It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search."); *id.* at 320 ("In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection. The Government's acquisition of the cell-site records here was a search under that Amendment.").

[144] *Id.* at 298.

[145] *Id.* at 309–10.

[146] *Id.* at 310.

[147] Byars v. United States, 273 U.S. 28, 32 (1927).

[148] *See Carpenter*, 585 U.S. at 300–01, 308–14.

escape this tireless and absolute surveillance."[149] The *Carpenter* Court simply cannot, and will not, abide that result given the basic purpose of the Fourth Amendment "to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials."[150] Although the question was not directly before the Court in *Carpenter*, there is no reason to believe that the Court would, or that we should, accept life in a surveillance state simply because it is effected by proxy.

It may be tempting to shrink from this conclusion, both because it cuts against conventional wisdom and because it suggests radical, perhaps devastating, consequences for technology companies and their government partners. Part III addresses the first concern by situating the argument advanced in this Part in a broader doctrinal context. As we shall see, rather than challenging conventional wisdom, the foregoing analysis squarely addresses a question that just has not been asked. If it challenges anything, it is untested assumptions. Part IV addresses the second concern by elaborating on the potential consequences of treating technology companies like Google, Verizon, Meta, and X as state agents for purposes of the Fourth Amendment. But far more important than these accessions to pragmatism is the commitment to preserve the fundamental rights afforded to each and all of us by the Fourth Amendment against threats posed by "new phenomen[a]."[151]

Notably, some of the technology companies that pose the greatest threats to privacy also resist as best they can efforts by governments to co-opt their surveillance capacities or exploit their customers' data. Microsoft and Google have long been at the vanguard of disclosing data relating to law enforcement requests for customer data.[152] Microsoft forced the Department of Justice into a consent decree setting limits on gag orders in particular cases.[153] Apple, Google, and Meta all boast their use of encryption.[154] Moreover, there is a lot

---

[149] *Id.* at 312.

[150] *Id.* at 303 (quoting Camara v. Mun. Ct. of S.F., 387 U.S. 523, 528 (1967)).

[151] *Id.* at 309.

[152] *See* Brendan Sasso, *Microsoft Claims Right to Publish Surveillance Data*, HILL (June 27, 2013, 2:00 PM ET), https://perma.cc/65N4-QVD6; Andy Greenberg, *Google Hands over User Data for 94% Of U.S. Law Enforcement Requests*, FORBES (June 27, 2011, 12:55 PM EDT), https://perma.cc/S437-25ZF.

[153] *See* Nick Wingfield, *U.S. to Limit Use of Secrecy Orders that Microsoft Challenged*, N.Y. TIMES (Oct. 24, 2017), https://perma.cc/MD8K-NZHL.

[154] *See, e.g.*, Pegoraro, *supra* note 21 (describing how Google will encrypt location data stored on its servers); Loredana Crisan, *Launching Default End-to-End Encryption on Messenger*, META (Dec. 6, 2023), https://perma.cc/GD7Z-FHUT; Jack Nicas & Katie Benner, *F.B.I. Asks*

of dynamism here, with companies and governments developing new technologies, new ways to gather and exploit data, and new means of conducting surveillance. What remains constant, however, is the persistence of government efforts to exploit private companies. Unwilling though they may be at times, technology companies will always be drawn into relationships with government cooperative enough to satisfy the requirements of state agency, though we should not forget that they may not always be so unwilling.[155]

III. THERE ARE GOOD DOCTRINAL PRECEDENTS FOR TAKING A MORE EXPANSIVE VIEW OF FOURTH AMENDMENT STATE AGENCY

The Court's willingness in *Carpenter* to take a more expansive view of the state agency requirement is not without precedent. The Court has a long tradition of treating private actors as state agents in order to protect constitutional rights against the "stealthy encroachments"[156] of "private" entities collaborating with governments or, in some cases, acting as governments. This Part surveys those cases. As a starting point, consider *Byars v. United States*, decided in 1927.[157]

In *Byars*, a federal prohibition agent named Adams tagged along with local law enforcement officers while they conducted a warranted search of premises controlled by A.J. Byars.[158] During that search, officers discovered counterfeit stamps and other evidence implicating Byars in violations of the Volstead Act, which they passed along to Adams. Byars was convicted in federal court based, in part, on the counterfeit stamps. He appealed, arguing that the stamps were fruits of an illegal search.[159] Writing for the Court, Justice George Sutherland noted that the warrant application endorsed by the state judge did not allege sufficient facts to establish probable cause.[160] That did not necessarily mean the search itself violated the Fourth Amendment, however, because, at that

---

Apple to Help Unlock Two iPhones, N.Y. TIMES (Jan. 7, 2020), https://perma.cc/AT9N-8WB6 (reporting that Apple has built encryption into iPhones since 2014 that can only be unlocked by users' passwords).

[155] *See, e.g.*, Jennifer Martinez, *Snowden Claims Web Companies Gave NSA "direct access" to Systems in New Video Clip*, HILL (July 18, 2013, 9:17 PM ET), https://perma.cc/G4DA-AG56 (reporting on claims by Edward Snowden that technology companies gave government agencies "direct access" to their servers to facilitate bulk surveillance programs).

[156] Byars v. United States, 273 U.S. 28, 33–34 (1927).

[157] *Id.*

[158] *Id.* at 29–30.

[159] *Id.* at 29.

[160] *Id.*

time, the Fourth Amendment had not yet been incorporated to the states, which meant that local officers could not, as a matter of constitutional law, violate the Fourth Amendment.[161] In addition, the "silver platter doctrine" allowed federal courts to admit evidence seized by state agents during searches that would violate the Fourth Amendment if conducted by federal agents.[162] Relying on these two rules, federal prosecutors argued that the primary agents in the search were local law enforcement officers, not Adams, rendering the search immune from Fourth Amendment scrutiny and the counterfeit stamps admissible in federal court.

On behalf of the Court, Justice Sutherland rejected the federal government's efforts to exploit the fruits of the illegal search.[163] Citing the history of the Fourth Amendment as a means of combating the "long misuse of power in the matter of searches and seizures both in England and the colonies," Justice Sutherland maintained that "[c]onstitutional provisions for the security of person and property are to be liberally construed, and 'it is the duty of courts to be watchful for the constitutional rights of the citizen, and against any stealthy encroachments thereon.'"[164] Among the "stealthy encroachments," Justice Sutherland identified were "equivocal methods, which, regarded superficially, may seem to escape the challenge of illegality but which, in reality, strike at the substance of the constitutional right."[165] Where these attempts are made, he intoned, "the court must be vigilant to scrutinize the attendant facts with an eye to detect and a hand to prevent violations of the Constitution by circuitous and indirect methods."[166] Because Adams was present during the search, expected to benefit from the search, and took possession of evidence at the scene that was uniquely useful to federal prosecutors, Justice Sutherland concluded that the search was "a joint operation of the local and federal officers."[167] As a consequence, the search was subject to Fourth Amendment

---

[161] *See* Wolf v. Colorado, 338 U.S. 25 (1949) (incorporating the Fourth Amendment through the Due Process Clause of the Fourteenth Amendment).

[162] *Byars*, 273 U.S. at 33. *See also* Elkins v. United States, 364 U.S. 206 (1960) (overturning the silver platter doctrine); Lustig v. United States, 338 U.S. 74 (1949) (upholding the silver platter doctrine).

[163] *Byars*, 273 U.S. at 33–34.

[164] *Id.* at 32, 33 (quoting Boyd v. United States, 116 U.S. 616, 635 (1886)).

[165] *Id.* at 33–34.

[166] *Id.* at 32.

[167] *Id.* at 32–33.

review and any evidence seized in violation of the Fourth Amendment was inadmissible in federal court.[168]

Almost a century later, the *Carpenter* Court took heed of Justice Sutherland's call to put fundamental rights ahead of pedantic technicality when determining the scope of Fourth Amendment protections. The *Carpenter* Court could have cited the third party doctrine or the public observation doctrine to hold that cell site location tracking by "private" companies is not a "search"—indeed, at least three Justices favored that result.[169] Instead, Chief Justice Roberts, following Justice Sutherland's lead, focused on the history of the Fourth Amendment and "the plain spirit and purpose of the constitutional prohibitions intended to secure the people against unauthorized official action."[170] Rather than indulging the willful blindness of constitutional technicality, the *Carpenter* Court decided to give full effect to the sacred promise made by the Fourth Amendment, adapting existing doctrine to meet challenges to the absolute right of the people to live free from threats of unreasonable search posed by the "new phenomenon" of cell site location tracking.[171]

The holdings in *Byars* and *Carpenter* are of a piece with scores of cases where the Court has met emerging threats to citizens' rights by imposing constitutional constraints on "private" actors.[172] Many of the most significant of these cases arise in the context of the Fourteenth Amendment.[173] For

---

[168] *Id.* at 33–34.

[169] Carpenter v. United States, 585 U.S. 2212–13 (2018) (Kennedy, J. dissenting).

[170] *Byars*, 273 U.S. at 33. *See also Carpenter,* 585 U.S. at 2213–14 ("As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to 'assure[ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'") (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).

[171] *Carpenter*, 585 U.S. at 216.

[172] *See, e.g.*, Dep't of Transp. v. Ass'n of Am. R.R., 575 U.S. 43 (2015) (holding that Amtrak is a state entity in light of its ownership and corporate structure, the political branches' supervision over its priorities and operations, its statutory goals; government supervision of its day-to-day management; and federal financial support); Williams v. United States, 341 U.S. 97 (1951) (holding that a private detective was a state actor when "by force and violence" he obtained a confession where he had a special license issued by the municipality and was conducting an investigation in conjunction with local law enforcement).

[173] It is worth noting here that, in contrast to the Fourth Amendment, the Fourteenth Amendment actually specifies its application to "the State." U.S. CONST. amend. IX ("All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the state wherein they reside. No state shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any state deprive any person of life, liberty, or property, without due process

example, the Court has held unconstitutional the discriminatory use of peremptory challenges by private attorneys in both civil[174] and criminal trials.[175] It has also condemned private actors when they discriminate against customers based on race.[176] These efforts reinforce the fact that the state agency requirement is somewhat elastic and certainly capable of reaching those contemporary surveillance practices that are most likely to threaten the right of the people to be secure against unreasonable searches.[177]

---

of law; nor deny to any person within its jurisdiction the equal protection of the laws."). *See also* Griffin v. Maryland, 378 U.S. 130, 136 (1964) ("When a State undertakes to enforce a private policy of racial segregation it violates the Equal Protection Clause of the Fourteenth Amendment." (citing Pennsylvania v. Board of Trusts, 353 U.S. 230 (1957)). For an expanded discussion of the absence of how the absence of the word "state" in the Fourth Amendment suggests the absence of any textual foundation for the Fourth Amendment state agency requirement, *see* Gray, *supra* note 45.

[174] *See* J.E.B. v. Alabama, 511 U.S. 127 (1994) (prohibiting the discriminatory use of peremptory challenges based on sex in civil cases); Edmonson v. Leesville Concrete Co., Inc., 500 U.S. 614 (1991) (prohibiting the discriminatory use of peremptory challenges based on race in civil cases).

[175] *See* Georgia v. McCollum, 505 U.S. 42 (1992) (prohibiting the discriminatory use of peremptory challenges based on race by private defense counsel in criminal cases).

[176] *See* Adickes v. Kress & Co., 398 U.S. 144 (1970) (holding that exclusion of customers from restaurant on the basis of race is state action for purposes of 18 U.S.C. § 1983 and the 14th Amendment to the extent the owner acted in accordance with "a state-enforced custom requiring racial segregation"); Griffin v. Maryland, 378 U.S. 130 (1964) (holding that a deputy sheriff providing security for an amusement park through a contract with a private security firm was a state actor when he enforced the park's policy of racial exclusion); Lombard v. Louisiana, 373 U.S. 267 (1963) (dismissing trespass charges brought against participants in a civil rights sit-in who refused to leave a "refreshment counter" after being ordered to do so by a manager enforcing the store's racial segregation policy, which conformed to local ordinance); Burton v. Wilmington Parking Auth., 365 U.S. 715, 722–24 (1961) (holding that a restaurant that discriminated against customers based on race was state actor subject to the Fourteenth Amendment because it was a tenant in a building owned by the state); Shelley v. Kraemer, 334 U.S. 1 (1948) (effectively banning racially discriminatory land covenants by prohibiting judicial enforcement under the Fourteenth Amendment).

[177] Slobogin, *supra* note 96, at 18. That elasticity surely has its limits. *See, e.g.*, Jackson v. Metro. Edison Co., 419 U.S. 345 (1974) (applying narrow "state action" test to hold that a public utility was not a state actor when terminating services for a customer due to non-payment despite background conditions including close state regulations because the specific action was not dictated by state regulation); Flagg Bros. v. Brooks, 436 U.S. 149 (1978) (private entity availing itself of right afforded under state law to liquidate property in order to cover a debt was not a state actor for purposes of due process); Am. Mfrs. Mut. Ins. Co. v. Sullivan, 526 U.S. 40 (1999) (withholding medical insurance payments pending review was not state action despite state authorizing statute); Blum v. Yaretsky, 457 U.S. 991 (1982) (holding that a nursing home was not state actor despite significant regulatory regime when evicting patient). Judge Friendly described this more limited view of state action in *Powe v. Miles*, 407 F.2d 73, 81 (2d Cir. 1968), writing that the "essential point" is "that the state must be involved not simply with some activity of the institution alleged to have inflicted injury upon a plaintiff but with the activity that caused the injury. Putting the point another way, the state action, not the private action, must be the subject of the complaint." Even under this more restricted

Perhaps most salient for present purposes is the line of cases enforcing the Fourteenth Amendment against private parties when they play important roles in the political process[178] or assume responsibilities usually borne by the government.[179] For example, in *Terry v. Adams*, the Court held that a private political group was bound by the Fourteenth Amendment because its endorsement of candidates played an outsized role in determining the results in primary and general elections.[180] A decade earlier, the Court held in *Marsh v. Alabama* that a corporation violated the First Amendment by prohibiting pamphleteering on the streets of a company town because that space was presented as a public square. Writing for the Court in *Marsh*, Justice Hugo Black advanced the principle that "[t]he more an owner, for his advantage, opens up his property for use by the public in general, the more do his rights become circumscribed by the statutory and constitutional rights of those who use it."[181] Just as "the owners of privately held bridges, ferries, turnpikes and railroads may not operate them as freely as a farmer does his farm," so, too, those who manage and operate spaces for "the public benefit."[182]

Many of the technology companies that concern privacy advocates self-consciously maintain virtual spaces that are open to the public, occupy a critical role in public life—including politics—and explicitly present themselves as

---

approach, much of the activity described in this section would qualify for state action, including conduct such as location tracking that is the subject of statutory mandate and frequently exploited by law enforcement and national security agencies.

[178] *See, e.g.*, Terry v. Adams, 345 U.S. 461 (1953) (holding that a local organization exercising de facto authority to choose party candidates violated Fifteenth Amendment by discriminating against African American candidates); Smith v. Allwright, 321 U.S. 649 (1944) (holding that a political party is subject to constitutional suit when it excludes voters based on race); United States v. Classic, 313 U.S. 299 (1941) (holding that party officials who altered ballots to affect the outcome of a primary election were state actors where "misuse of power, possessed by virtue of state law and made possible only because the wrongdoer is clothed with the authority of state law, is action taken 'under color of' state law.").

[179] *See, e.g.*, Amalgamated Food Emps. Union v. Logan Valley Plaza, 391 U.S. 308 (1968) (holding that a shopping center is governed by the First and Fourteenth Amendments "because the shopping center serves as the community business block and 'is freely accessible and open to the people in the area and those passing through' (quoting Marsh v. Alabama, 326 U.S. 501 (1946)); Marsh v. Alabama, 326 U.S. 501 (1946) (holding that a company town that assumed public functions acted like a state, and therefore was bound by the First and Fourteenth Amendments).

[180] *Adams*, 345 U.S. at 469–71.

[181] *Marsh*, 326 U.S. at 506.

[182] *Id. See also Amalgamated Food Emps.*, 391 U.S. 308 (1968) (holding that labor advocates protesting in public areas outside a shopping center may claim First Amendment protections against private owners). *Amalgamated Food Emps.* was limited in *Lloyd Corp. v. Tanner*, 407 U.S. 551 (1972), and *Hudgens v. NLRB*, 424 U.S. 507 (1976).

being "operated primarily to benefit the public."[183] Consider, as examples, Equifax's "purpose . . . to help people live their financial best [by striving] to create economically healthy individuals and communities everywhere we do business,"[184] Meta's "mission . . . to give people the power to build community and bring the world closer together,"[185] X's commitment "to give everyone the power to create and share ideas and information, and to express their opinions and beliefs without barriers" because "[f]ree expression is a human right" and "[o]ur role is to serve the public conversation,"[186] and YouTube's "mission . . . to give everyone a voice and show them the world."[187]

Although the roles, statuses, and responsibilities of these and other technology companies are subjects of considerable controversy, there is good reason to conclude that they should be subject to constitutional restraint under the Court's reasoning in *Marsh*, at least to the extent they play roles in public life more familiar to states, municipalities, and their direct agents, including those affecting economic opportunities and access to the political process.[188] Equifax and its kin gather, aggregate, store, and analyze a wide variety of consumer and personal data in order to issue credit scores that determine access and opportunity in almost every sector of economic and social endeavor, including access to credit, education, employment, housing, and even romance.[189] As Justice Ketanji Brown Jackson recently reminded us, social

---

[183] *Marsh*, 326 U.S. at 506; s*ee also* Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598 (2018) (arguing that, by virtue of their role in society, social media platforms should be governed by free speech norms). The idea that social media platforms may be state agents by virtue of their responsibilities for maintaining the "public square" is before the Court in *NetChoice v. Paxton* and *Moody v. NetChoice*. Amy Howe, *Social Media Content Moderation Laws Come Before Supreme Court*, SCOTUSBLOG (Feb. 23, 2024), https://perma.cc/FLT4-XWPV.

[184] *Who We Are*, EQUIFAX, https://perma.cc/F8ZD-QFJL.

[185] *FAQs: Meta Investor Relations*, META, https://perma.cc/HZ4U-UTRD.

[186] *X's Policy on Hateful Conduct*, X (Apr. 2023), https://perma.cc/N8UM-L2UT. That public mission was also central to Twitter's identity. *See* SEC, Form S-1 Registration Statement under the Securities Act of 1933 (Oct. 3, 2013), https://perma.cc/2VAT-VC25 (declaring Twitter's commitment "to give everyone the power to create and share ideas and information instantly without barriers" and solemn promise that "[o]ur business and revenue will always follow that mission in ways that improve—and do not detract from—a free and global conversation").

[187] *About YouTube*, YOUTUBE, https://perma.cc/54EJ-5D9F.

[188] *See infra* note 189.

[189] *See* Jessica Silver-Greenberg, *Perfect 10? Never Mind That. Ask Her for Her Credit Score*, N.Y. TIMES (Dec. 25, 2012), https://perma.cc/EJ3U-FFTZ ("The credit score, once a little-known metric derived from a complex formula that incorporates outstanding debt and payment histories, has become an increasingly important number used to bestow credit, determine

media companies are the modern public square, providing critical forums for public expression and debate, and therefore should not escape First Amendment prohibitions on censorship.[190] Cellphone companies and others capable of erecting "geofences" track participation in public protests.[191] It is hard to imagine a set of activities more appropriate for constitutional regulation under the test elaborated in *Marsh* and its progeny.

These appeals to First and Fourteenth Amendment cases are by way of analogy, of course. But the thread of analogy is important. The fundamental purpose of the Bill of Rights, inclusive of the First and Fourth Amendments, is to constrain government power, preserving to "the people" fundamental freedoms of thought, expression, and privacy while the Fourteenth Amendment guarantees equality in their enjoyment. Just as *Byars* and *Carpenter* counsel against expansions of government power by proxy, so too do parallel lines of precedent running through the First and Fourteenth Amendments. The consistent lesson is that the government cannot accomplish through proxies what it is constitutionally forbidden to do directly.[192] It can no

housing and even distinguish between job candidates. It's so widely used that it has also become a bigger factor in dating decisions, sometimes eclipsing more traditional priorities like a good job, shared interests and physical chemistry.").

[190] Transcript of Oral Argument at 109, Moody v. NetChoice, No. 22-277 (Feb. 26, 2024)*; see also* Packingham v. North Carolina, 582 U.S. 98, 104, 107 (2017) ("A fundamental principle of the First Amendment is that all persons have access to places where they can speak and listen, and then, after reflection, speak and listen once more . . . a street or a park is a quintessential forum for the exercise of First Amendment rights . . . Even in the modern era, these places are still essential venues for public gatherings to celebrate some views, to protest others, or simply to learn and inquire . . . Social media allows users to gain access to information and communicate with one another about it on any subject that might come to mind. By prohibiting sex offenders from using those websites, North Carolina with one broad stroke bars access to what for many are the principal sources for knowing current events, checking ads for employment, speaking and listening in the modern public square, and otherwise exploring the vast realms of human thought and knowledge. These websites can provide perhaps the most powerful mechanisms available to a private citizen to make his or her voice heard."); Knight First Amendment Inst. v. Trump, 928 F.3d 226 (2d Cir. 2019) (holding that President Donald J. Trump violated the First Amendment by "blocking" some users from his Twitter feed because it is a public forum), *vacated as moot* 141 S. Ct. 1220 (2021). *See also* Biden v. Knight First Amendment Inst., 141 S. Ct. 1220, 1222 (2021) (Thomas, J., concurring) ("If part of the problem is private, concentrated control over online content and platforms available to the public, then part of the solution may be found in doctrines that limit the right of a private company to exclude."); Howe, *supra* note 183 (reporting claim at issue in *NetChoice v. Paxton* and *Moody v. NetChoice* that "states describe social media platforms as the new "digital public square," with enormous control over news that members of the public see and communicate.").

[191] Note, *Geofence Warrants and the Fourth Amendment*, 134 HARV. L. REV. 2508, 2519–20 (2021).

[192] Norwood v. Harrison, 413 U.S. 455, 465 (1973).

more force us to the cloisters by delegation than direct oppression. Neither, *Marsh* teaches, can a "private" entity exercise unrestricted authority to censor, search, or seize if it has assumed the role of the state. As Justice Alito points out, these are precisely the threats posed by many contemporary technology companies. As Parts II and III have argued, the Court's state agency doctrine provides ample grounds for courts to bring constitutional rights to bear. Part IV takes up the question of how.

IV. WHAT IT WOULD MEAN TO TREAT GOOGLE AS A STATE AGENT

Assume, for the moment, that the foregoing analysis is correct and that many of the corporations whose surveillance activities most concern privacy advocates are state agents, at least when conducting the kinds of surveillance activities that pose the "greatest threats to individual privacy."[193] Does this mean companies like Verizon must secure warrants before gathering cell site location information or that banks must have warrants to install surveillance cameras on their premises? As we shall see in this Part, the answer depends on whether the surveillance conducted by a "private" entity qualifies as a "search" or "seizure" for purposes of the Fourth Amendment, whether those subject to surveillance have consented to that search, and whether imposing a warrant requirement strikes the right balance among the competing interests at stake.[194] Let us begin with the question whether corporate surveillance constitutes a "search" for purposes of the Fourth Amendment.

A. Do Corporations Like Google Engage in Searches or Seizures?

After establishing government action, the threshold question in any Fourth Amendment analysis is whether the conduct at issue constitutes a "search" or a "seizure" for purposes of the Fourth Amendment.[195] In its seminal 1928 decision in *Olmstead v. United States*, the Court held that government action constitutes a "search" if it entails a physical intrusion into a constitutionally protected person, house, paper, or effect for purposes of gathering

---

[193] Carpenter v. United States, 585 U.S. 296, 385 (2018) (Alito, J., dissenting).
[194] *See* GRAY, AGE OF SURVEILLANCE, *supra* note 5, at 170–71, 255–56, 266–74; Gray & Citron, *supra* note 134, at 116.
[195] SALTZBURG ET AL., *supra* note 91, at 40.

information.[196] In 1967, largely in response to the inability of this physical intrusion test to reach new technologies capable of "subtler and more far-reaching means of invading privacy,"[197] the Court expanded the definition of "search" in *Katz v. United States* to include government actions that intrude upon subjectively manifested expectations of privacy that society is prepared to recognize as reasonable.[198]

When determining whether government actions constitute "searches," facts matter.[199] Nevertheless, the Court has established some doctrinal rules that can help us decide whether conduct by "private" actors operating as state agents falls within the scope of Fourth Amendment regulation. One is the public observation doctrine, which holds that visual surveillance conducted from a vantage outside constitutionally protected "persons, houses, papers, and effects" does not constitute either a "search" or "seizure," even if it reveals activities inside a constitutionally protected area.[200] Citing this doctrine, the Court has declined to apply the Fourth Amendment in cases where law enforcement officers peered into homes through open windows from a public

---

[196] Olmstead v. United States, 277 U.S. 438, 464–66 (1928)*; see also* Florida v. Jardines, 569 U.S. 1, 6 (2013) ("When 'the Government obtains information by physically intruding' on persons, houses, papers, or effects, 'a "search" within the original meaning of the Fourth Amendment has "undoubtedly occurred."'" (quoting United States v. Jones, 565 U.S. 400, 404–05 (2012)).).

[197] On Lee v. United States, 343 U.S. 747, 763 (1952) (Douglas, J., dissenting) (quoting Olmstead v. United States, 277 U.S. 438, 473 (1928) (Brandeis, J., dissenting))*; see also* Silverman v. United States, 365 U.S. 505, 508–09 (1961) (noting concerns that the physical intrusion test was inadequate in light of "recent and projected developments in the science of electronics"); Goldman v. United States, 316 U.S. 129, 139 (1942) (Murphy, J., dissenting) (noting that "the search of one's home or office no longer requires physical entry, for science has brought forth far more effective devices for the invasion of a person's privacy").

[198] Katz v. United States, 389 U.S. 347, 353 (1967)*; see also id.* at 361 (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.'"). The Court subsequently made clear that the *Katz* test is additive, and did not replace the *Olmstead* test. United States v. Jones, 565 U.S. 400, 404–05 (2012).

[199] *See* Scott v. Harris, 550 U.S. 372, 383 (2007) ("[W]e must still slosh our way through the factbound morass of "reasonableness."); United States v. Curry, 965 F.3d 313, 316 (4th Cir. 2020) ("Any Fourth Amendment analysis . . . must be grounded on an accurate understanding of the facts.").

[200] Carpenter v. United States, 585 U.S. 296, 306 (2018).

vantage point,[201] looked down into homes from public airspace,[202] and monitored a person's movement through public spaces.[203]

In another important line of cases, the Court has held that, if we share information with third parties, then we assume the risk that those third parties may share that information with others.[204] Applying this rule, the Court has held that the Fourth Amendment does not apply when confidants share the contents of privately recorded conversations,[205] telephone companies share the metadata associated with customers' telephone calls,[206] or banks share information relating to customers' financial transactions.[207]

A third important doctrine is the requirement to show "standing," which means that anyone seeking Fourth Amendment protection must establish interference with *their* person or property or violation of *their* personal expectations of privacy.[208] As Justice Clarence Thomas has put the point, "individuals do not have Fourth Amendment rights in *someone else's* property."[209]

Under these well-established rules, much of the surveillance performed by "private" actors does not qualify as a search or seizure for purposes of the Fourth Amendment because it is discrete and limited. For example, individual cameras that surveil public spaces, like those deployed at many commercial institutions, likely do not raise Fourth Amendment concerns.[210] Customers and others who enter or pass by these facilities cannot claim either property interests or reasonable expectations of privacy in the places where these cameras are deployed. As a consequence, they cannot object on Fourth Amendment grounds if these cameras are used to monitor their activities,

---

[201] Florida v. Riley, 488 U.S. 445, 449–50 (1989).
[202] Dow Chem. Co. v. United States, 476 U.S. 227, 251 (1986); California v. Ciraolo, 476 U.S. 207 (1986).
[203] United States v. Knotts, 460 U.S. 276, 281–82 (1983).
[204] *Carpenter*, 585 U.S. at 307.
[205] United States v. White, 401 U.S. 745 (1971).
[206] Smith v. Maryland, 442 U.S. 735, 742 (1979).
[207] United States v. Miller, 425 U.S. 435 (1976); California Bankers Ass'n v. Shultz, 416 U.S. 21 (1974). As Part IV discusses, Congress passed legislation to protect the privacy of some of those activities because the Fourth Amendment did not.
[208] Rakas v. Illinois, 439 U.S. 128 (1978). For an extended critique of the doctrine of Fourth Amendment standing, *see* David Gray, *Collective Standing Under the Fourth Amendment*, 55 AM. CRIM. L. REV. 77 (2018).
[209] *Carpenter*, 585 U.S. at 353 (Thomas, J., dissenting).
[210] *See, e.g.*, United States v. May-Shaw, 955 F.3d 563 (6th Cir. 2020) (holding that twenty-three-day surveillance of apartment complex parking lot and carport was not a search).

whether in a public place or in private locations visible from a public location.[211] Neither, it seems, can customers complain about corporations gathering information in the course of providing commercial services. Under established doctrine, none of this voluntary information sharing would constitute a Fourth Amendment "search."[212] This may not be too discomfiting, however, precisely because these kinds of surveillance activities are relatively limited and discrete. They only involve a particular location or relatively limited information. Far more worrisome is what Professor Christopher Slobogin calls "panvasive surveillance"[213]—surveillance programs that, by virtue of their range and scope, reveal "a wealth of detail about [our] familial, political, professional, religious, and sexual associations."[214] Fortunately, "different constitutional principles" probably apply when it comes to these kinds of programs because they can facilitate "twenty-four hour surveillance of any citizen of this country."[215]

The Supreme Court drew a distinction between discrete surveillance and programmatic surveillance in *Carpenter v. United States*, a cellphone tracking case decided in 2018. Prior to *Carpenter*, the Court had applied the public observation doctrine in location tracking cases, holding that the use of visual surveillance and radio beeper tracking devices does not implicate the Fourth Amendment because we do not have a reasonable expectation of privacy in our public movements.[216] However, as the *Carpenter* Court pointed out, these

---

[211] *See, e.g.*, United States v. Tuggle, 4 F.4th 505 (7th Cir. 2021), *cert. denied*, Tuggle v. United States, 142 S. Ct. 1107 (2022) (holding that use of pole camera installed on public property to surveil target's home was not a search, irrespective of duration); United States v. May-Shaw, 955 F.3d 563 (6th Cir. 2020) (holding that twenty-three-day surveillance of apartment complex parking lot and carport was not a search); *see also* United States v. Moore-Bush, 36 F.4th 320 (1st Cir. 2022) (en banc court preserving lower court determination that pole cameras deployed in public space to surveil a home for eight months did not constitute a search); *but see* United States v. Cuevas-Sanchez, 821 F.2d 248 (5th Cir. 1987) (holding that use of pole camera to record activities in a target's backyard was a "search" for purposes of the Fourth Amendment); Commonwealth v. Mora, 150 N.E.3d 297 (Mass. 2020) (holding that use of pole cameras to conduct continuous, long-term, targeted surveillance of a person's home constitutes a "search" under Article 14 of the Massachusetts Declaration of Rights).

[212] *See* Smith v. Maryland, 442 U.S. 735, 742 (1979) (telephonic metadata); United States v. White, 401 U.S. 745 (1971) (financial information).

[213] Christopher Slobogin, *Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine*, 102 GEO. L.J. 1721 (2014).

[214] United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring); *see also Carpenter*, 585 U.S. at 309–11 (describing how CSLI threatens individual and collective privacy interests); Riley v. California, 573 U.S. 373, 393–94 (2014) (distinguishing between searches of wallets and cellular phones in reference to the quantity and quality of information stored on cellular phones); Gray & Citron, *supra* note 134, at 110 (describing the collective threats posed by broad, indiscriminate surveillance).

[215] *Carpenter*, 585 U.S. at 306 (quoting United States v. Knotts, 460 U.S. 276, 283 (1983)).

[216] *Knotts*, 460 U.S. at 281–82.

cases all involved "rudimentary" technologies used in specific investigations to monitor "discrete" journeys.[217] The analysis is different, the *Carpenter* Court held, when it comes to technologies that, by virtue of their capabilities and scalability, can facilitate programmatic surveillance.[218] That is because these technologies can achieve "near perfect surveillance,"[219] "revealing not only [our] particular movements, but through them [our] 'familial, political, professional, religious, and sexual associations,'"[220] which "hold for many Americans the 'privacies of life.'"[221] Moreover, granting unfettered authority to deploy and use these technologies threatens not just targeted individuals, but all of us.[222] For example, cellular phones are ubiquitous.[223] The location data they "convey[] to the wireless carrier [provides] a detailed and comprehensive record of the person's movements,"[224] and the "intimate window into a person's life."[225] Because those records are "cheap," "continually logged for all of the 400 million devices in the United States," retained for many years, and "effortlessly compiled," the threat to privacy "runs against everyone."[226]

Under the Court's analysis in *Carpenter*, the deployment and use of any technology capable of compiling detailed location records on a programmatic scale—panvasive surveillance—likely constitutes a "search" for purposes of the Fourth Amendment. *Carpenter* dealt with historical cell site location information, but there are other technologies equally capable of compiling similarly detailed location records, including aerial surveillance,[227] networked surveillance cameras,[228] and many cellphone apps.[229]

---

[217] *Carpenter*, 585 U.S. at 306.

[218] *Id.* at 310–13. *See also* Gray & Citron, *supra* note 134, at 101–25 (explaining how the Fourth Amendment recommends different regulatory approaches based on the technology at issue).

[219] *Carpenter*, 585 U.S. at 312.

[220] *Id.* at 311 (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

[221] *Id.* (quoting Riley v. California, 573 U.S. 373, 403 (2014)).

[222] *Id.* at 311–12.

[223] *Id.* at 300 ("There are 396 million cell phone service accounts in the United States—for a Nation of 326 million people.").

[224] *Id.* at 309.

[225] *Id.*

[226] *Id.* at 312. *See also* Gray & Citron, *supra* note 134, at 101–02 (describing how these features of technologies factor in determining the Fourth Amendment status of new and emerging surveillance technologies).

[227] GRAY, AGE OF SURVEILLANCE, *supra* note 5, at 257–60; Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330 (4th Cir. 2021) [hereinafter *Baltimore Air*] (en banc).

[228] Gray & Citron, *supra* note 134, at 65–67.

[229] *See supra* notes 21–23 and accompanying text.

Particularly with the advent of drones, aerial surveillance represents an emerging threat to the location privacy of many Americans.[230] Applying the framework elaborated by the Supreme Court in *Carpenter*, the Fourth Circuit Court of Appeals held in *Leaders of a Beautiful Struggle v. Baltimore Police Department* that aerial surveillance conducted on a programmatic scale constitutes a "search" because it has the capacity to both track individuals in real time and aggregate detailed location histories.[231] In that case, a private corporation called Persistent Surveillance Systems (PSS) contracted with the Baltimore Police Department to deploy a piloted aircraft outfitted with several high-resolution digital cameras. During daylight hours, the plane circled over Baltimore, recording indiscriminately the movements of hundreds of thousands of residents and visitors. Those recordings were stored on servers controlled by PSS.[232] Police investigators would then ask PSS to compile image data to assist in their investigations of specific incidents—by tracking suspects and witnesses from the scene of a crime—their investigations of individuals—by monitoring their movements—and their investigations of locations—by documenting comings and goings.[233]

Writing for his *en banc* court, Chief Judge Roger Gregory held that the surveillance technology deployed by PSS and the Baltimore Police Department constituted a "search" for purposes of the Fourth Amendment.[234] Key to that holding was the programmatic nature of the surveillance activity. In contrast with discrete instances where officers might surveil a particular person for a limited time, Judge Gregory regarded PSS's surveillance as more "like the CSLI in *Carpenter*," in that the aerial surveillance conducted by PSS "tracks every movement of every person outside in Baltimore," creates "a detailed, encyclopedic, record of where everyone came and went within the city during daylight hours over the prior month-and-a-half," and "enables police to retrace a person's whereabouts, granting access to otherwise unknowable information." [235] On that basis, the Fourth Circuit concluded that the

---

[230] GRAY, AGE OF SURVEILLANCE, *supra* note 5, at 257–63.

[231] 2 F.4th 330 (4th Cir. 2021).

[232] *Baltimore Air*, 2 F.4th at 335–40.

[233] *Id.*

[234] *Id.*

[235] *Id.* at 341–42. State agency was not litigated in *Baltimore Air* because the named defendants were Baltimore City and the Baltimore Police Department. There can be no doubt, however, that Persistent Surveillance Systems was a state agent insofar as the entire program it operated in Baltimore was in cooperation with the Baltimore Police Department.

programmatic use of aerial surveillance constitutes a "search" for purposes of the Fourth Amendment.[236]

The Fourth Circuit's analysis in *Baltimore Air* suggests that programmatic surveillance conducted at a more terrestrial level using land-based surveillance cameras also constitutes a "search" for purposes of the Fourth Amendment.[237] To be sure, every federal court to address the constitutional status of fixed surveillance cameras after *Carpenter* has held that they do not implicate the Fourth Amendment.[238] However, all of these cases involved the use of a small number of cameras to conduct discrete surveillance of a targeted location. None involved the programmatic use of networked surveillance cameras. That matters from a Fourth Amendment perspective.

Although discrete surveillance cameras cannot facilitate the kind of broad, pervasive, and indiscriminate surveillance at issue in *Carpenter* and *Baltimore Air*, networked systems of surveillance cameras can . . . and do.[239] Following the lead of New York's Data Awareness System (DAS),[240] American cities are increasingly innervated by surveillance cameras that send the data they collect to central repositories.[241] Using that data, surveillants can trace in detail the movements of individuals going back days, weeks, months, or years.[242] Already daunting, the capacities of these technologies to compile detailed location histories have been dramatically enhanced by the emergence of facial recognition technologies.[243] Given these capacities, there is no doubt that these systems violate reasonable expectations of privacy, and therefore constitute

---

As Part II shows, the result would not change if PSS or another "private" company set up shop as an independent surveillant and then sold their services to law enforcement agencies. *See supra* notes 107–122 and accompanying text.

[236] *Baltimore Air*, 2 F.4th at 345.

[237] *See* Gray & Citron, *supra* note 134, at 105–12 (describing how aerial surveillance programs constitute "searches").

[238] *See supra* note 211.

[239] *Cf. Baltimore Air*, 2 F.4th at 345 (discussing the differences between discrete, fixed pole cameras and technologies capable of pervasive surveillance and "the creation of a retrospective database of everyone's movements across the city").

[240] Gray & Citron, *supra* note 134, at 65–67.

[241] For example, in July 2023 San Diego advanced plans to expand its network of surveillance cameras. Press Release, City of San Diego Police Dep't, Council Committee Advances SDPD's Smart Streetlight, License Plate Recognition Technology Proposal (July 19, 2023), https://perma.cc/RT26-NJYH.

[242] GRAY, AGE OF SURVEILLANCE, *supra* note 5, at 40–42, 264–65; Gray & Citron, *supra* note 134, at 112–24.

[243] David Gray, *Bertillonage in an Age of Surveillance: Fourth Amendment Regulation of Facial Recognition Technologies*, 24 SMU SCI. & TECH. L. REV. 3, 3–10 (2021) [hereinafter Gray, *Bertillonage*].

"searches" for purposes of the Fourth Amendment.[244] Because these systems are operated by, or for the principal benefit of, government agencies, including law enforcement, "private" participants in these programs are state agents for purposes of the Fourth Amendment, whether they are the technology companies that create and operate the systems, commercial enterprises that provide access to their surveillance systems, or homeowners who allow law enforcement access to home security cameras.[245]

In addition to cell site location information and networked surveillance cameras, there are other location tracking technologies that likely conduct "searches" for purposes of the Fourth Amendment. Among these are scores of cellphone applications that gather and aggregate location data. For example, Google apps and devices create detailed histories of users' movements.[246] Some of these applications track users even if they have disabled "Location History."[247] Google is not alone. Social media apps like Facebook, X, and Instagram also gather location information.[248] In fact, gathering, storing, and analyzing location data is critical to the economic models that underwrite these apps.[249] As with the cell cite location information at issue in *Carpenter*, the detailed, historical location data gathered by these apps reveals a comprehensive, intimate history of user's lives.

Based on the foregoing analysis, Google and its ilk seem to be conducting "searches" when they leverage devices and applications to gather, aggregate, and store location information. In many cases they do so as state agents. That is because government agencies, including law enforcement, are well aware that Google and other device and application providers engage in location tracking and those agencies routinely seek to exploit that tracking information to advance a range of government goals, including criminal investigations[250]

---

[244] *Baltimore Air*, 2 F.4th at 345; Gray, *Bertillonage*, *supra* note 243, at 26–32.

[245] *See supra* notes 107–122.

[246] Marriam Zhou & Richard Nieva, *Google Is Probably Tracking Your Location, Even If You Turn It Off, Says Report*, CNET (Aug. 13, 2018), https://perma.cc/EJB5-HGEH.

[247] Ryan Nakashima, *Google Tracks Your Movements, Like It or Not*, ASSOCIATED PRESS (Aug. 13, 2018), https://perma.cc/9X8V-DXN4.

[248] *See supra* notes 246–247.

[249] Jon Keegan & Alfred Ng, *There's a Multibillion-Dollar Market for Your Phone's Location Data*, THE MARKUP (Sept. 30, 2021), https://perma.cc/ZGQ5-8XGY.

[250] *See, e.g.*, Madison Hall, *The DOJ Is Creating Maps from Subpoenaed Cell Phone Data to Identify Rioters Involved with the Capitol Insurrection*, BUS. INSIDER (Mar. 24, 2021), https://perma.cc/V8VD-LCK7 (reporting on law enforcement's use of cellphone location data to identify suspects in the January 6, 2021, insurrection); Charlies Arzel & Stuard Thompson,

and monitoring political activities.[251] There is, therefore, a strong case to be made that, under existing doctrine, these "private" entities conduct "searches" as state agents when they gather and store their customers' location data.

For similar reasons, large-scale data surveillance programs, sometimes referred to as "Big Data," qualify as "searches" for purposes of the Fourth Amendment. Perhaps the most notorious operators of these programs are the data aggregation companies discussed earlier in this chapter[252] that Chris Hoofnagle vividly describes as "Big Brother's little helpers."[253] These companies gather, aggregate, store, analyze, and sell a wide variety of information ranging from professional histories to financial data. They are not alone. There is a variety of more specialized data surveillance companies that gather, aggregate, and store copious amounts of personal and consumer data for particular purposes. Prominent examples include credit rating companies like Equifax and Transunion.[254] But simply by virtue of the fact that we live in a data economy, almost every corner of our financial, social, and political lives is surveilled by one or another corporation.[255] These companies actively collect and analyze vast amounts of data including personally identifying information (like social security numbers and addresses), "merely" personal information (such as internet protocol data, internet device identifiers, and browser cookies), web and consumer engagement data (from websites, social media, mobile apps, emails), and behavioral and attitudinal data (from online advertisements, financial transactions, and product purchases).[256] They collect this data in a

They Stormed the Capitol. Their Apps Tracked Them, N.Y. TIMES (Feb. 5, 2021), https://perma.cc/T8S8-KM9R (reporting on how location data from cellphone apps was used to identify suspects in the insurrection of January 6, 2021); Tyler Dukes, *To Find Suspects, Raleigh Police Quietly Turn to Google*, WRAL NEWS (July 13, 2018), https://perma.cc/TFW6-7SJT (documenting how police used Google location data to identify criminal suspects).

[251] *See* Mark Harris, *A Peek Inside the FBI's Unprecedented January 6 Geofence Dragnet*, WIRED (Nov. 28, 2022), https://perma.cc/E39C-ZK4H; Shoshana Zuboff, *The Coup We Are Not Talking About*, N.Y. TIMES (Jan. 29, 2021), https://perma.cc/77V2-ME7E (explaining threats to democracy posed by ubiquitous public and private surveillance); Jon Swartz, *Justice Department Demand for Data on 1.3M anti-Trump Protesters Sparks Debate*, USA TODAY (Aug. 16, 2017), https://perma.cc/5DG2-3SPX (reporting on Justice Department's efforts to get user information from disruptj20.org).

[252] *See supra* notes 111–114 and accompanying text.

[253] Hoofnagle, *supra* note 111, at 595.

[254] O'NEILL, *supra* note 27.

[255] *See generally* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019) (documenting the use of surveillance and exploitation of personal information in the data economy).

[256] Danielle Citron & Barry Friedman, *Indiscriminate Surveillance*, 110 VA. L. REV. (forthcoming

variety of ways, including web tracking, monitoring social media activity, buying data, or just asking consumers for the information in exchange for "free" services.[257]

Much of this data surveillance might appear to fall within the compass of the third-party doctrine. Information about financial transactions certainly does.[258] Most of the other information of interest to Big Data is, or was at one point, shared with one entity or another.[259] But so too is the location data at issue in *Carpenter* that cellphone users voluntarily share with their service providers.[260] Nevertheless, the *Carpenter* Court held that, because aggregated cell site location information reveals the intimate details of consumers' lives, programmatic cell site tracking violates reasonable expectations of privacy.[261] The same is true when it comes to the information gathered by Big Data, some of which is revealing in discrete doses, but all of which is revealing in the aggregate. The Court expressed sympathy with this conclusion in *California v. Riley*.[262]

Riley asked whether law enforcement officers may search data stored on cellphones without a warrant incident to lawful arrest.[263] In the normal course of an arrest, officers may search suspects along with the property on their persons or within their reach and control without first securing a warrant.[264] Authority to conduct searches incident to arrest encompasses items like wallets, purses, briefcases, notebooks, and journals that may contain a range of private information.[265] In *Riley*, officers accessed data on arrestees' phones, including call records, contact lists, text messages, and photographs.[266] The officers argued that these searches of personal effects were reasonable—and did not require a warrant—because they were conducted secondary to lawful

---

2024); Thorin Klosowski, *Big Companies Harvest Our Data. This is Who They Think I Am*, N.Y. TIMES (May 28, 2020), https://perma.cc/6NYQ-4DFB; Andriy Slynchuk, *Big Brother Brands Report: Which Companies Access Our Personal Data the Most?*, CLARIO BLOG (Nov. 29, 2022), https://perma.cc/6JUX-7P3Y.

[257] William Goddard, *How Do Big Companies Collect Consumer Data*, IT CHRONICLES (Jan. 14, 2019), https://perma.cc/X94X-CJL8.

[258] United States v. Miller, 425 U.S. 435 (1976); Cal. Banker's Ass'n v. Shultz, 416 U.S. 21 (1974).

[259] *See* Goddard, *supra* note 257 (describing how we share information with data aggregators).

[260] Carpenter v. United States, 585 U.S. 296, 308 (2018).

[261] *Id.* at 310.

[262] 573 U.S. 373 (2014).

[263] *Id.* at 378.

[264] United States v. Robinson, 414 U.S. 218 (1973); Chimel v. California, 395 U.S. 752 (1969).

[265] *Riley*, 573 U.S. at 386, 392–93.

[266] *Id.* at 378–81.

arrests. [267] Writing for the Court, Chief Justice Roberts conceded that warrantless searches incident to arrest are reasonable as a general matter, but concluded that cellular phones require more robust protection due to both the intimate and revealing nature of the information users store on these devices and their "immense storage capacity."[268] For the same reason, most Big Data surveillance programs qualify as "searches" for purposes of the Fourth Amendment. Many of these programs gather information that is private by any reasonable measure, including social security numbers, birth dates, and other personally identifying information. [269] Others gather more quotidian information in staggering amounts that, in the aggregate, paint vivid and revealing pictures of our lives. That, in fact, is the whole point of these technologies. Judged by standards established by the Court in *Riley* and *Carpenter*, the deployment and use of Big Data constitute "searches."

Separate from conduct constituting "searches," "private" agents also assist the government in conducting "seizures" from time to time. Whether an action qualifies as a "seizure" for purposes of the Fourth Amendment depends on what, or whom, is seized. When it comes to "houses, papers, and effects," seizures occur when there is a material interference with property interests, including possession, access, and privacy.[270] Seizures of "persons" occur either when a person submits to a show of official authority that would cause a

---

[267] *Id.* at 380–81.

[268] *Id.* at 386, 393–97; *see also Carpenter*, 585 U.S. at 305 ("[I]n *Riley*, the Court recognized the 'immense storage capacity' of modern cell phones in holding that police officers must generally obtain a warrant before searching the contents of a phone. We explained that while the general rule allowing warrantless searches incident to arrest 'strikes the appropriate balance in the context of physical objects, neither of its rationales has much force with respect to' the vast store of sensitive information on a cell phone." (internal citations omitted)).

[269] This fact has been at the fore when these firms suffer data breaches, leading to the theft of personally identifying information belonging to millions of individuals. *See, e.g.*, *Equifax Data Breach Settlement*, FED. TRADE COMM'N (Dec. 2022), https://perma.cc/X5EK-USKD (reporting on PII lost in breach of Equifax).

[270] United States v. Jacobsen, 466 U.S. 109, 113 (1984); *see, e.g.*, Illinois v. McArthur, 531 U.S. 326 (2001) (preventing access to home constitutes a "seizure"); United States v. Place, 462 U.S. 696 (1983) (holding luggage in order to allow a drug detection dog to arrive on the scene was a "seizure"); Olmstead v. United States, 277 U.S. 438, 466 (1928) (noting that seizures of homes may be accomplished by "an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure."); Segura v. United States, 468 U.S. 796, 822 (1984) (Brennan, J., dissenting) ("A 'seizure' occurs when there is some meaningful interference with an individual's possessory interests."); United States v. Ramirez, 342 U.S. F.3d 1210 (officers "seized" an effect when delaying delivery of package for twenty-eight hours); Morgan Cloud, *Property Is Privacy: Locke and Brandeis in the Twenty-First Century*, 55 AM. CRIM. L. REV. 37, 42 (2018) (discussing foundational interests in privacy underlying Fourth Amendment's protection of "papers").

reasonable person to believe they are not free to leave or when a state agent physically touches a person with the objective purpose of effecting a seizure.[271] One ready example of corporate-government partnerships to seize property is the increasing use of spyware. Government agencies like the Drug Enforcement Agency have long acquired, deployed, and used spyware and other malicious software produced by private firms.[272] That includes recent efforts to acquire tools developed by the NSO Group, including Pegasus (which can be used to eavesdrop on encrypted cellphone communications[273]) and a covert cellphone tracking tool[274] (with the apparent aim of using these technologies to conduct operations in the United States[275]).

Inserting spyware on a cellular phone or other device likely constitutes a "seizure" for purposes of the Fourth Amendment. These are, after all, physical devices. Like all software, malware occupies physical space on electronic devices and takes at least partial control over its operations. That appropriation of memory and operation sometimes interferes materially with the way a device functions, either by making the device slow or clunky, or sometimes by locking it down entirely. But even where spyware does not noticeably affect the operation of a device, it still materially affects property interests by turning those devices against their owners. The possibility is particularly disconcerting when you consider the number of "smart" devices in our homes and the potential that hackers, government or otherwise, might use them to spy on us.[276] The consequences are not trivial. NSO's tools and other spyware have been used by foreign governments to target journalists and political dissidents.[277] In recognition of the dangers posed by governments' deployment and use of spyware, President Joseph Biden issued an executive order in March 2023 prohibiting the use of privately produced spyware by the federal

---

[271] Torres v. Madrid, 592 U.S. 306 (2021).

[272] Mark Mazzetti et al., *How the Global Spyware Industry Spiraled Out of Control*, N.Y. TIMES (Jan. 28, 2023), https://perma.cc/X5MN-B98Q.

[273] Ronen Bergman & Mark Mazzetti, *The Battle for the World's Most Powerful Cyberweapon*, N.Y. TIMES MAG. (Jan. 28, 2022), https://perma.cc/G6VJ-5SBV.

[274] Mark Mazzetti & Ronen Bergman, *A Front Company and a Fake Identity: How the U.S. Came to Use Spyware It Was Trying to Kill*, N.Y. TIMES (Apr. 2, 2023), https://perma.cc/FY2L-ZCJV; Mark Mazzetti & Ronen Bergman, Internal Documents Show How Close the F.B.I. Came to Deploying Spyware, N.Y. TIMES (Nov. 15, 2022), https://perma.cc/XCT5-TVV6.

[275] *See supra* notes 272–274.

[276] Davey Winder, *How to Stop Your Smart Home Spying on You*, THE Guardian (Mar. 8, 2020), https://perma.cc/C4YF-PS9S.

[277] *See supra* note 273.

government.[278] Despite that order, journalists have reported that government agencies may be continuing their efforts to access and use spyware, either directly or through intermediaries.[279]

To sum up a bit, most of the surveillance programs conducted by "private" corporations like Google qualify as "searches" for purposes of the Fourth Amendment. The case is particularly strong for location tracking. The question with respect to historical cell site location information was settled in *Carpenter*.[280] In terms of breadth, scale, precision, and the ability to reveal intimate details about the lives of millions of citizens, location tracking conducted by the likes of Google, Meta, Amazon, and TikTok is indistinguishable from cell site location tracking. If anything, their tracking is more intrusive because it uses multiple means to determine location (such as GPS, Wi-Fi, and Bluetooth[281]), crosses devices and platforms (tracking users through their phones, tablets, smartwatches, and computers), and accesses multiple sources (such as metadata associated with calls, texts, pictures, and social media posts[282]). Although less well-settled, location tracking conducted through aerial and networked terrestrial surveillance programs also qualifies as a search. So too does data surveillance. Finally, some eavesdropping and tracking may also qualify as "seizures" of electronic devices when it is facilitated by spyware and other malware.

If the foregoing is right, then corporations like Google frequently engage in conduct constituting Fourth Amendment "searches" and "seizures." Much of the time, they do so as state agents because they routinely share the fruits of their efforts with government agencies, including law enforcement. Sometimes that sharing is willing and enthusiastic. Sometimes it is not. Either way, law enforcement knows these companies are conducting searches and expects to benefit. The companies also know they will be called upon to share the fruits of their searches with the government. Separately, technology companies often occupy positions in society traditionally the province of government. When they exploit those positions to conduct surveillance that intrudes upon reasonable expectations of privacy, they threaten the right of the people to be

---

[278] Exec. Order No. 14,093, 88 Fed. Reg. 18957 (Mar. 27, 2023) (Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security).
[279] *See supra* note 274.
[280] Carpenter v. United States, 585 U.S. 296, 309 (2018).
[281] *Learn How to Manage Your Location*, FACEBOOK PRIVACY CENTER, https://perma.cc/D2PV-GZE6 (last visited May. 19, 2024).
[282] Thomas Germain, *How a Photo's* Hidden *'Exif' Data Exposes Your Personal Information*, CONSUMER REPORTS (Dec. 6, 2019), https://perma.cc/RP9L-BZCC.

secure against unreasonable searches as state agents. This does not end the Fourth Amendment analysis, however. That is because the Fourth Amendment guards not against searches and seizures generally, but against threats of *unreasonable* searches and seizures.[283]

B. Do We Consent to Corporate Surveillance?

The challenge implicit in Justice Alito's observation that "today, some of the greatest threats to individual privacy may come from powerful private companies" [284] is how can legislatures, executive agencies, and courts guarantee the right of the people to be secure against threats that these companies will "misuse vast quantities of data about the lives of ordinary Americans" [285] or otherwise threaten their right to be secure against unreasonable searches and seizures. The familiar Fourth Amendment solution is to interpose a warrant requirement.[286] But, as the Court repeatedly has counselled, the "touchstone" of the Fourth Amendment is reasonableness.[287] Reasonableness, in turn, requires striking a balance among the competing interests at stake when government agents conduct searches.[288] Requiring warrants issued by detached and neutral magistrates based on probable cause may strike the right balance in some circumstances, but the Court has recognized that there are alternatives.

One way to establish the reasonableness of searches and seizures is to secure permission from a person who has "standing" to consent.[289] "Consent" in the Fourth Amendment context must be voluntary but does not entail a formal waiver of rights.[290] It is instead judged from a colloquial, non-technical perspective taking into account prevailing social norms.[291] The question is whether, on a totality of the circumstances, a reasonable person would have believed they had permission to search from a person with lawful authority to

---

[283] Maryland v. King, 569 U.S. 435, 440–41 (2013); Florida v. Jimeno, 500 U.S. 248, 250 (1991).
[284] *Carpenter*, 585 U.S. at 386 (Alito, J., dissenting).
[285] *Id.*
[286] Johnson v. United States, 333 U.S. 10, 13–15 (1948).
[287] Brigham City v. Stuart, 547 U.S. 398, 403 (2006) ("[B]ecause the ultimate touchstone of the Fourth Amendment is 'reasonableness,' the warrant requirement is subject to certain exceptions.").
[288] Wyoming v. Houghton, 526 U.S. 295, 300 (1999); Terry v. Ohio, 392 U.S. 1, 21 (1968); Camara v. Mun. Ct. of S.F., 387 U.S. 523, 536–37 (1967).
[289] Florida v. Jimeno, 500 U.S. 248, 250–51 (1991).
[290] Bumper v. North Carolina, 391 U.S. 543, 548 (1968).
[291] Florida v. Jardines, 569 U.S. 1, 8 (2013); Georgia v. Randolph, 547 U.S. 103, 111 (2006).

give it.[292] Certainly, explicit verbal permission will do the trick, but consent may also be expressed non-verbally,[293] or even implied by circumstances.[294] For example, in *United States v. Drayton*, the Supreme Court held that a suspect consented to a search of his person by "lifting his hands about eight inches from his legs" in response to an officer's request to "check" him.[295] Later, in *Florida v. Jardines*, the Court held that having a front walkway, porch, and door provides implicit permission for girl scouts, trick-or-treaters, and police to enter the curtilage of a residence in order to knock and see if anyone is home.[296]

Consent may also be implied by the way technologies or commercial practices operate.[297] For example, in *Smith v. Maryland*, the Court held that telephone customers implicitly consent to their service providers' collecting location information, call numbers, and other "metadata" necessary to route their calls and accurately bill for service.[298] For similar reasons, the Court held in *United States v. Miller* that customers implicitly consent to banks' gathering information about financial transactions that is necessary to complete those transactions.[299]

Searches that exceed the scope of consent are not "reasonable."[300] While architecture and prevailing social norms may imply consent to knock on a front door, they do not provide permission to loiter or to root around in the front yard.[301] While technical necessity may imply consent for telephone companies to gather telephonic metadata, that permission would not extend to eavesdropping on conversations.[302]

---

[292] *Jimeno*, 500 U.S. at 251.

[293] United States v. Drayton, 536 U.S. 194 (2002).

[294] *Jardines*, 569 U.S. at 10.

[295] *Drayton*, 536 U.S. at 199.

[296] *Jardines*, 569 U.S. at 8. *See also id.* at 12–14 (Kagan, J., concurring) (pointing out that the same rules and result would obtain by applying the *Katz* framework).

[297] *See* Smith v. Maryland, 442 U.S. 735 (1979) (telephones); United States v. Miller, 425 U.S. 435, 442–43 (1976) (banking); Cal. Bankers Ass'n v. Shultz, 416 U.S. 21 (1974) (banking).

[298] *Smith*, 442 U.S. at 742–46.

[299] *Miller*, 425 U.S. at 442–43.

[300] *Jimeno*, 500 U.S. at 252.

[301] *Jardines*, 569 U.S. at 8–9.

[302] *Smith*, 442 U.S. at 741; *cf.* Katz v. United States, 389 U.S. 347, 353 (1967) (holding that the Fourth Amendment protects the contents of telephone communications); *Ex parte* Jackson, 96 U.S. 727, 733 (1877) (protecting the contents of sealed letters placed in mail despite the fact that addressee information is voluntarily revealed by the sender); United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016) (holding that viewing contents of email attachments is a "search").

At least to some degree, many of the searches conducted by "private" corporations like Google are reasonable because customers have provided at least implicit consent. But that permission is limited. Here again, *Carpenter* provides useful guidance. As the *Carpenter* Court points out, cellphone service providers must be able to determine their customers' locations in order to properly route calls.[303] They therefore have the consent of their customers, implicit though it may be, to monitor the locations of the phones they service in real time. In order to build and sustain a sufficiently robust network, service providers may also need to aggregate and store some general historical location information so they can decide where to deploy and expand infrastructure. But these technical and business requirements do not justify aggregating and storing historical location information documenting the precise locations of individual customers going back months and years. This critical distinction explains why the *Carpenter* Court made clear that its treatment of historical cell site location information does not implicate real-time location data and tower dumps—wherein cellphone providers can identify all the cellular phones in contact with a particular cellular base station during a specific period of time.[304] These means and methods of establishing a person's location at a particular time tend to reveal very little about a person's life, and therefore do not pose major threats to reasonable expectations of privacy.[305] Moreover, gathering this kind of discrete location information is perfectly consistent with the consent implied by technical necessity.

By similar logic, it would be relatively easy to establish the reasonableness of discrete visual surveillance conducted by "private" corporations. For premises. In most cases, there are legitimate business reasons for the deployment and use of these technologies, such as security and assessing foot traffic. Both to enhance the efficacy of these cameras as security measures and provide notice, owners often have signs notifying those who enter that they are being surveilled. In addition, the cameras themselves are often pretty obvious, providing fair warning to anyone who chooses to enter a monitored premises

---

[303] Carpenter v. United States, 585 U.S. 296, 301 (2018).
[304] *Id.* at 316.
[305] *See* Stephen Henderson, *Real-Time and Historic Location Surveillance After United States v. Jones: An Administrable, Mildly Mosaic Approach*, 103 J. CRIM. L. & CRIMINOLOGY 803, 825-26, 831 (2013) (arguing that tower dumps and discrete real-time cell site location information should be subject to lesser protections than longer term tracking because these techniques do not produce revealing mosaics of peoples' lives).

that they are being watched. As a consequence of these factors, the deployment and use of discrete surveillance cameras is probably reasonable due to the consent implied by entering monitored premises, if the limited surveillance conducted even constitutes a "search" at all. But matters change considerably if surveillance cameras are linked to large networks and the images they collect are aggregated and stored on servers where they can be searched and recalled. These kinds of networked surveillance systems not only infringe on reasonable expectations of privacy, they also violate any consent implied by those who choose to pass through any particular camera's field of vision.

The foregoing analysis suggests that reasonable expectations of privacy and implied consent are aligned when it comes to assessing the Fourth Amendment status of many visual and data surveillance programs. Relatively discrete surveillance does not disturb reasonable expectations of privacy. In many circumstances, limited surveillance can also be defended as "reasonable" because those surveilled have provided consent, either express or implied. By contrast, large scale surveillance programs capable of documenting intimate details about individuals' lives both violate reasonable expectations of privacy and the terms of any consent that can reasonably be implied by referring to technical necessity, business practices, or cultural context.[306] Unsurprisingly, these are also the kinds of surveillance programs that pose the most significant privacy concerns because they affect all of us and present real dangers of exploitation. How, then, might we go about ensuring that the searches conducted by new and emerging technologies capable of facilitating these kinds of programs of broad and indiscriminate surveillance are "reasonable" for purposes of the Fourth Amendment? The answer lies in the Court's instruction that ensuring "reasonableness" requires striking an appropriate balance between the competing interests at stake in searches and seizures.

C. *Guaranteeing the Right of the People to be Secure Against Unreasonable Searches*

What are the competing interests at stake in searches and seizures? In the context of conventional police investigations, the Court has recognized that searches and seizures infringe upon citizens' interests in privacy, property, and

---

[306] GRAY, AGE OF SURVEILLANCE, *supra* note 5, at 264–65; Gray & Citron, *supra* note 134, at 107–09.

personal security.[307] On the other side of the scale, searches and seizures advance law enforcement's interests in detecting, investigating, and prosecuting crime.[308] They may also protect officers and the public from threats of physical violence.[309] Law enforcement searches are "reasonable," according to the Court, to the extent they strike an appropriate balance among these competing interests.[310]

The Supreme Court has endorsed different approaches to striking a reasonable balance among the competing interests at stake in government searches and seizures. In some cases, officers must secure a warrant from a detached and neutral magistrate before conducting a search.[311] In explaining this requirement, the Court has emphasized the value of having a neutral decisionmaker assess whether a proposed search strikes a reasonable balance among the competing interests at stake rather than leaving that judgment to interested, and therefore biased, officers.[312] This warrant preference is not universal, however. For example, in cases of emergency, asking officers to go through a warrant application process might unreasonably compromise the legitimate law enforcement and public safety interests at stake.[313] In these circumstances, the Court allows officers to make an initial judgment about whether their intended search is reasonable, subject to later review by a court in the context of a suppression hearing or lawsuit.[314] For similar reasons, the Court grants officers authority to conduct stops and frisks—limited investigative seizures and searches for weapons—based in the first instance on their own determinations of reasonableness.[315]

Law enforcement is not the only government entity whose interests are served by searches and seizures. Searches may also serve regulatory interests, such as ensuring that premises are in compliance with administrative codes.[316] As with law enforcement searches, these "special needs" searches are

---

[307] Wyoming v. Houghton, 526 U.S. 295, 300 (1999).
[308] *Id.*
[309] Brigham City v. Stuart, 547 U.S. 398, 403; Terry v. Ohio, 392 U.S. 1, 23–24.
[310] Johnson v. United States, 333 U.S. 10, 13–15.
[311] *Id.*
[312] *Id.*
[313] *See, e.g.*, Kentucky v. King, 563 U.S. 452 (2011); United States v. Santana, 427 U.S. 38 (1976); Warden v. Hayden, 387 U.S. 294 (1967).
[314] *See, e.g.*, *King*, 563 U.S. at 457; Hudson v. Michigan, 547 U.S. 586, 596–97 (2006).
[315] *See* Terry v. Ohio, 392 U.S. 1, 27 (1968).
[316] *See, e.g.*, See v. City of Seattle, 387 U.S. 541 (1967); Camara v. Mun. Ct. of S.F., 387 U.S. 523 (1967).

constitutional to the extent they strike a reasonable balance between the privacy and property interests of targets and the legitimate government interests at stake.[317] But, in contrast with law enforcement searches, regulatory searches usually do not require warrants, because those subject to regulatory regimes have diminished expectations of privacy, and warrant application processes would unreasonably compromise the regulatory interests at stake.[318] Instead, special needs searches are administered through their own regulatory regimes.

Where law enforcement searches are evaluated on a case-by-case basis, the reasonableness of special needs searches usually is evaluated on a programmatic basis.[319] Rather than requiring warrants or other case-by-case assessments to determine whether individual special needs searches are reasonable, the Court asks whether a search regime serves legitimate government interests separate from normal law enforcement, the regime provides proper notice to those subject to regulation and inspection, the regime is tailored to the government interests at stake, and the regime limits the discretion of government agents with respect to time, place, manner, and scope of searches. [320] Applying this framework, the Supreme Court has sanctioned, *inter alia*, home inspections conducted to ensure compliance with health and safety regulations,[321] inspections of junk yards,[322] roadblocks to identify intoxicated drivers,[323] and border searches.[324] It has also declined to endorse, among other endeavors, drug detection road blocks,[325] warrantless strip searches of children,[326] and discretionary inspection of hotel registries.[327]

The Court's flexible approach to guaranteeing that searches and seizures are reasonable based on the competing interests at stake in both the criminal and special needs contexts provides useful guidance as we think through how the Fourth Amendment would apply to Google and other corporations who act

---

[317] Wayne R. LaFave et al., Criminal Procedure 257 (5th ed. 2009).
[318] *Id.* at 257–58.
[319] *Id.*
[320] *Id.*
[321] *See Camara*, 387 U.S. at 540.
[322] *See* New York v. Burger, 482 U.S. 691 (1987).
[323] *See* Mich. Dep't of State Police v. Sitz, 496 U.S. 444 (1990).
[324] *See, e.g.*, United States v. Flores-Montano, 541 U.S. 149 (2004); United States v. Martinez-Fuerte, 428 U.S. 543 (1976).
[325] *See* Indianapolis v. Edmond, 531 U.S. 32 (2000).
[326] *See* Safford Unified Sch. Dist. v. Redding, 557 U.S. 364 (2009).
[327] *See* Los Angeles v. Patel, 576 U.S. 409 (2015).

as state agents when conducting surveillance or installing software on electronic devices. We start by identifying the various interests at stake. On the government's side, accessing or leveraging surveillance conducted by "private" corporations may serve normal law enforcement interests in detecting, investigating, and prosecuting crime. The facts in *Carpenter* provide a ready example. In others, government interests will be more regulatory or administrative in character. For example, public health officials may access aggregated or individual cell site location information to assist public health officials battling a pandemic.[328] The interests of those subject to surveillance are also familiar, including expectations of privacy in the whole of their movements in public places[329] and activities in their homes that otherwise would not be subject to scrutiny absent physical intrusion into constitutionally protected areas.[330] To this we can add security in the integrity of their effects, including electronic and internet-connected devices. More novel is the need to include as part of the calculus the business interests of companies like Google in the surveillance they conduct and the information they collect. For example, in *Carpenter* the Court recognized that cellphone service providers collect, store, and analyze historical cell site location data to facilitate business decisions about developing and maintaining infrastructure.[331] That information may also play a role in billing.[332]

Focusing on the various interests at stake when "private" corporations deploy and use surveillance technologies suggests four broad categories of cases. First, there are cases where private corporations develop, deploy, and use surveillance technologies for the direct and largely exclusive benefit of government entities. Persistent Surveillance Systems, the private contractor responsible for the aerial surveillance program at issue in *Baltimore Air,* is a prime example. In these kinds of cases, the corporation is acting directly as an extension of the government. Its interests, mediated only by profit motive, are coextensive with the government's interests. They are Big Brother's willing helpers.

---

[328] *See* Natalie Ram & David Gray, *Mass Surveillance in the Age of COVID–19*, 7 J. L. & BIOSCI., 1, 3 (2020).

[329] *See* Carpenter v. United States, 585 U.S. 296, 313–14 (2018).

[330] *See* Kyllo v. United States, 533 U.S. 27, 40 (2001).

[331] *See Carpenter*, 585 U.S. at 301–02.

[332] *See id.*; *See also* Smith v. Maryland, 442 U.S. 735, 742 (1979) (describing how phone companies use metadata for billing purposes).

In a second class of cases, government agents seek to exploit technologies deployed by corporations for their own business purposes. The cellular service providers at issue in *Carpenter* provide a ready example, as do Google and other technology companies who regularly receive requests from government agents to disclose the results of data surveillance. In these cases, corporate interests underwriting searches are often distinct from government interests. These corporations conduct surveillance of their own accord. Often, they are Big Brother's grudging helpers.

In a third group of cases, corporations engage in conduct that might fairly be described as "searches" wholly for their own business reasons and free from government exploitation. For example, a transportation company might install GPS trackers on their vehicles in order to predict delivery times and identify inefficiencies in their routing and scheduling. That kind of monitoring surely would generate detailed historical location data, perhaps implicating drivers' reasonable expectations of privacy, but, unless some government agency regularly requested this information, we would not regard these surveillants as Big Brother's helpers.

Finally, there are circumstances where private corporations assume roles and responsibilities usually reserved for the government. Here we might consider the deployment of networked surveillance cameras and aerial drones in a gated residential community that are used to monitor residents and guests, deploy resources, and monitor compliance with rules and regulations. Government agents are not involved; but these are the kinds of activities and responsibilities that normally fall within the purview of government.

This brief sketch, and the various permutations it suggests, points us to a critical conclusion: Guaranteeing the security of the people against unreasonable searches and seizures facilitated by new and emerging surveillance technologies will require bespoke measures. There is no off-the-rack solution that will strike a reasonable balance among the competing interests at stake in all circumstances. This is the conclusion drawn by an emerging literature that explores ways to bring the Fourth Amendment to bear on means and methods of conducting systemic surveillance.[333] What is called for instead is developing decisional and regulatory infrastructures that

---

[333] *See, e.g.*, GRAY, AGE OF SURVEILLANCE, *supra* note 5, at 249–75; Citron & Friedman, *supra* note 256; Barry Friedman, *Lawless Surveillance*, 97 N.Y.U. L. REV. 1143 (2022); Andrew Ferguson, *Surveillance and the Tyrant Test*, 110 GEO. L.J. 205 (2021); Andrew Ferguson, *Structural Sensor Surveillance*, 106 IOWA L. REV. 47 (2020); Gray, *Categorical Imperative*, *supra* note 5, at 37; Gray & Citron, *supra* note 134, at 105–24.

accommodate the competing interests at stake by allowing for the reasonable deployment and use of new and emerging surveillance technologies while preserving the right of the people to be secure against unreasonable searches and seizures. The process would of course start with identifying the interests at stake.[334] The next step would be to strike a reasonable balance among the competing interests at stake by paying attention to the lifecycle of a technology, including deployment, information gathering, information aggregation, information storage and retention, access to information, analysis of information, and access to analysis.[335]

This flexible, tailored approach would of course lead to different results depending on the circumstances. In some cases, the proper conclusion will be that the Fourth Amendment simply bars the implementation of a program altogether. Consider again the aerial surveillance program reviewed by the Fourth Circuit in *Baltimore Air*.[336] The program was approved by the City of Baltimore (the City) and the Baltimore Police Department (BPD) on a pilot basis to determine the utility of the program as a law enforcement tool.[337] A group of city residents backed by the American Civil Liberties Union (ACLU) sued to enjoin the program.[338] They lost at trial and appealed. While that appeal was pending, the City and the BPD determined that the program did not provide substantial benefits to law enforcement and, on that basis, shut it down.[339] Then the Fourth Circuit determined that the program violated residents' reasonable expectations of privacy.[340] In light of the City and BPD's determination that the program served no significant governmental interest, the Fourth Circuit's holding largely bars the City and BPD from restarting the program. After all, the program violates the reasonable expectations of privacy of hundreds of thousands of Baltimore residents and visitors while not advancing any legitimate government interests. It is hard to imagine a clearer case of unreasonable search.

---

[334] GRAY, AGE OF SURVEILLANCE, *supra* note 5, at 267.

[335] *See* GRAY, AGE OF SURVEILLANCE, *supra* note 5, at 267–75 (elaborating and explaining this approach as applied to Big Data); Gray, *Bertillonage*, *supra* note 243, at 38–62 (describing such an approach to regulating facial recognition technologies).

[336] Leaders of a Beautiful Struggle v. Baltimore Police Dep't, 2 F.4th 330 (4th Cir. 2021).

[337] *Id.* at 333.

[338] *Id.* at 335.

[339] *Id.* at 333, 335–36.

[340] *Id.* at 342.

In other cases, requiring a warrant to deploy a technology will strike the right balance.[341] Here, telephonic wiretaps provide a useful example. Eavesdropping on telephone conversations implicates reasonable expectations of privacy.[342] Wiretaps usually require the assistance of telephone companies—in fact, the Communications Assistance for Law Enforcement Act requires that telecommunications companies maintain the technical capacity to facilitate wiretaps[343]—but wiretapping telephone calls does not serve any obvious business interests of telecommunication companies. By contrast, wiretaps can play a critical role in law enforcement's efforts to detect, investigate, and prosecute crime. In order to strike a reasonable balance among these competing interests, Congress decided to prohibit the deployment of technologies capable of intercepting electronic communications, including telephone calls,[344] but provided an exception for law enforcement where they have exhausted alternative investigative methods and secured a judicial warrant based on probable cause subject to rigorous additional limitations and constraints.[345]

In contrast with wiretaps, requiring warrants to deploy and use the technologies that gather, aggregate, and store historical cell site location information would unreasonably compromise legitimate government and business interests. That is because historical cell site location data is, well, historical. Its value to both cellphone companies and law enforcement derives from its retrospective quality.[346] The only way to create that historical record is to have the technology running in the background.[347] At the same time, historical cell site information threatens reasonable expectations of privacy on an almost unimaginable scale by virtue of the details it reveals about users' lives and the fact that it affects hundreds of millions of individuals.[348] In order to strike a reasonable balance among these competing interests, the *Carpenter* Court interposed a warrant requirement between law enforcement and cellular

---

[341] *See* Berger v. New York, 388 U.S. 41, 63 (1967) (holding that warrants are required for the placement of eavesdropping devices in homes).
[342] Katz v. United States, 389 U.S. 347, 353 (1967).
[343] 47 U.S.C. §§ 1001–1010.
[344] 18 U.S.C. § 2511.
[345] 18 U.S.C. § 2518*; see also Berger*, 388 U.S. at 63 (holding that warrants are required for the placement of eavesdropping devices in homes).
[346] *See* Gray & Citron, *supra* note 134, at 116.
[347] *Id.*
[348] Carpenter v. United States, 585 U.S. 296, 311–12 (2018).

service providers.[349] Cellphone companies remain free to gather, aggregate, store, and review historical cell site location information in any way that serves their business interests while also respecting the privacy and security interests of their customers. So long as they do, the records will be preserved for potential exploitation by law enforcement when officers can persuade a judicial officer that they have probable cause to believe that accessing those records will produce evidence that advances a criminal investigation.[350]

Variations on a warrant requirement may strike the right balance in many cases, but not always. Imagine, as an example, that a coalition of community leaders, businesses, public institutions, city leaders, and law enforcement agencies come together to establish an integrated operations center.[351] The center would gather, aggregate, and store images from surveillance cameras operated by public institutions and private businesses in addition to images from traffic cameras, redlight cameras, and license plate readers.[352] The program would use facial recognition technologies to associate images in the system with specific individuals. The program would gather, aggregate, and store information about cellular phones and other electronic devices that are active in the city using Wi-Fi routers and Bluetooth networks operated by participating organizations. The center would also have access to information about financial transactions. A primary goal of the program would be to enhance the ability of first responders to deal with emergencies and threats to public safety. It would also facilitate the detection, investigation, and prosecution of crime. In addition, the program would guide decisions on a variety of public policy issues ranging from traffic control to the deployment of street sweepers, greeters employed by a city improvement association, and law enforcement. The program would also help businesses to recruit customers and coordinate the provision and delivery of products and services.

Given the program's capacity to document in detail the locations and activities of everyone in the city, there is little doubt that this kind of program would threaten the reasonable expectations of privacy of anyone who came to town. It would also serve a range of legitimate governmental interests,

---

[349] *Id.* at 317.

[350] Congress adopted a similar approach when it reworked its Section 215 telephonic metadata program. *See supra* note 95.

[351] Andrew Ferguson paints a vivid picture of a city organized around these kinds of surveillance measures. *See* Ferguson*, Structural Sensor Surveillance*, *supra* note 333.

[352] This imagined program is not particularly hypothetical. Fusion centers and New York's Domain Awareness System demonstrate both the technical feasibility and attractiveness of this kind of coordinated surveillance program. *See supra* note 104.

including crime control and "special needs," as well as private commercial interests. These interests seem weighty enough to justify the program's existence. But, requiring a warrant before deploying this kind of program would not strike the right balance, because the program would need to be up and running all the time in order to serve the government and business interests at stake. Interposing a warrant requirement before allowing access to information gathered, aggregated, and stored by the program might be appropriate in some circumstances (such as when police want to use it to gather evidence about a particular crime or suspect) but would be unreasonable in others (such as when trying to determine whether and where to send out street sweepers or developing a targeted coupon program). Therefore, ensuring the constitutionality of this kind of program would require a more nuanced approach to regulating who could access data aggregated and stored by the program and how they could use it. Constitutional actors responsible for the program would also need to ask hard questions about data retention, attentive to the fact that governmental and business interests in data wane over time while adding to that history intensifies threats to privacy. The program would need to exercise care in the analytic tools it uses. For example, should it analyze all images using facial recognition software, or should the use of facial recognition technology be more limited?[353]

As we move from straight bans to complex administrative policies, it is natural to wonder who is best situated to strike the balance among competing interests demanded by the Fourth Amendment. Although the ultimate question of constitutionality necessarily rests with the courts, it is important to remember that legislatures and executive agencies are co-equal branches of government. When it comes to setting policy on the deployment and use of surveillance technologies by government entities or corporations acting as government agents, the political branches should take the laboring oar. Although the Supreme Court has made it clear that it will not defer to the executive branch's interpretation of statutes [354] or the political branches' interpretations of the Constitution,[355] that does not mean courts cannot show

---

[353] *See* Gray, *Bertillonage*, *supra* note 243, at 38–62 (elaborating how courts and policy makers should evaluate the Fourth Amendment status of facial recognition technologies).

[354] *See* Loper Bright v. Raimondo, No. 22-451, slip op. at 35 (Jun. 28, 2024) ("Chevron is overruled. Courts must exercise their independent judgement in deciding whether an agency has acted within its statutory authority.").

[355] *See* Marbury v. Madison, 5 U.S. 137, 137–38 (1803).

due respect for policies designed to effectuate statutory and constitutional rights so long as they fall within the broad compass of "reasonableness."[356]

CONCLUSION

So far, data surveillance programs conducted by "private" corporations have not been targets of Fourth Amendment litigation. But, as privacy advocates like Justice Alito have pointed out, there is no doubt that these programs threaten core privacy interests protected by the Fourth Amendment. One reason "private" surveillance and data gathering programs have not been subject to Fourth Amendment scrutiny is because we tend to assume that they are insulated by the state agency requirement. This Article has challenged that assumption. In many cases, "private" corporations are acting as state agents for purposes of the Fourth Amendment when they deploy and use surveillance technology because they are acting at the behest of a government entity, they routinely share the fruits of their searches with a government agency, or they occupy roles traditionally filled by government actors. Once the state agency hurdle is cleared, the question is how to guarantee the right of the people to be secure against unreasonable searches and seizures. The answer will depend on the technology and the interests at stake. Although familiar regulatory interventions like a warrant requirement may sometimes strike the right balance among the various interests of citizens, corporations, and government, more bespoke measures will be required as we face constitutional challenges posed by new emerging technologies.

---

[356] As an example, consider the Wiretap Act. In *Olmstead v. United States*, 277 U.S. 438 (1928), the Supreme Court held that wiretapping a telephone is not a "search." In *Katz v. United States*, 389 U.S. 347 (1967), the Court held that using an eavesdropping device to monitor one side of a telephone conversation is a "search." The facts in *Katz* did not require the Court to overturn *Olmstead*. It was nevertheless apparent that it would do exactly that if called upon. That call has not come because Congress passed the Wiretap Act in 1968 wherein it elaborated a regulatory regime governing both private and governmental use of wiretapping technology. Although the constitutional adequacy of the Wiretap Act has not been challenged in court, there is little doubt that the Court would find it perfectly "reasonable" if anyone asked.