MASS SEIZURE AND MASS SEARCH

Gregory Brazeal[*]

ABSTRACT

As courts attempt to develop Fourth Amendment doctrine to address the threats to privacy created by digital surveillance technologies, a valuable doctrinal resource has been largely neglected: the law governing the seizure of persons. Just as courts today struggle with the specter of mass search using digital technologies, courts in the 1960s were confronted with the problem of mass seizure through the growing use of stop-and-frisk by police departments. The responses to mass seizure developed by the Supreme Court in Terry v. Ohio, *592 U.S. 1 (1968), and its progeny provide lessons for courts today considering how to respond to the risks of digital mass search. By adopting the "mosaic theory," the Supreme Court has already begun to apply to digital search a form of aggregative reasoning that has long been used to define the seizure of persons.*

The analogy between seizure doctrine and search doctrine also sheds light on the significance of the Supreme Court's recent, landmark decision in Carpenter v. United States, *138 S. Ct. 2206 (2018), which responded to the declining cost of digital surveillance in a way that resembles* Terry*'s response to the rising use of stop-and-frisk in the 1960s.* Carpenter *opens the door for courts to develop a two-tiered doctrinal scheme for digital search, with less invasive searches requiring reasonable suspicion and more invasive searches requiring probable cause. Among other virtues, such an approach would provide a doctrinal foothold for subjecting the bulk collection of metadata and other digital mass surveillance programs to Fourth Amendment review.*

* Assistant Professor, University of South Dakota School of Law. Thank you to Jane Bambauer, Evan Caminker, Adam Feibelman, Jancy Hoeffel, Aziz Huq, Tracey Meares, Shira Scheindlin, Sarah Seo, Christopher Slobogin, and the participants in a faculty workshop at Tulane Law School on April 22, 2019 for valuable comments. Thank you also to Jonah Seligman for research assistance.

TABLE OF CONTENTS

INTRODUCTION

This Article offers a proposal for how courts might finally subject digital mass surveillance by state actors to judicial scrutiny under the Fourth Amendment. Along the way, the Article addresses a number of related topics, including the bureaucratization of American policing; the history of programmatic stop-and-frisk before *Terry v. Ohio*;[1] and how courts adjust constitutional doctrine to respond to increases in the frequency of a constitutionally problematic activity, even when the frequency of the activity is, strictly speaking, legally irrelevant. But the ultimate aim of the Article is to provide a roadmap for arriving at reasonable constitutional restrictions on digital mass surveillance that are grounded as much as possible in existing Fourth Amendment doctrine.

As digital privacy scholars and activists have long argued,[2] digital mass surveillance—the government's use of digital technologies to surveil large numbers of people in the United States who have not been individually targeted for surveillance—poses a historically unprecedented threat to the privacy values that the Fourth Amendment is supposed to protect.[3] Yet the Fourth Amendment, which remains "the primary form of regulation of government information gathering" in the United States,[4] currently provides no protection against the vast majority of existing and possible forms of digital mass surveillance.[5]

A narrow majority of the Supreme Court recently acknowledged the problem in a landmark decision, *Carpenter v. United States*,[6] which removed a doctrinal obstacle to Fourth Amendment review of certain particularly serious intrusions of privacy using digital technology.[7] But even in the wake of *Carpenter*, it remains unclear how, precisely, it might be possible to subject digital mass surveillance to judicial scrutiny under the Fourth Amendment when the surveillance in question, viewed in isolation, represents a relatively minor intrusion of privacy.

---

1 392 U.S. 1 (1968).

2 *See infra* note 22.

3 *See generally infra* Part I.

4 DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 12 (2011).

5 *See infra* Part I.

6 138 S. Ct. 2206, 2223 (2018).

7 *See infra* Part III.A.

What is the shortest, most plausible route from existing Fourth Amendment case law to the reasonable constitutional regulation of digital mass surveillance?

The novelty of this Article's proposal is that it suggests Fourth Amendment doctrine already contains the resources necessary to address many of the threats to privacy created by government surveillance using digital technologies. These resources have been largely overlooked, however, because they appear in the underlying reasoning of Fourth Amendment *seizure* doctrine, while digital surveillance is largely a matter of Fourth Amendment *search* doctrine. In particular, once the Supreme Court's development of Fourth Amendment doctrine to govern stop-and-frisk in *Terry* is understood as a response to the rising threat of mass seizure, it becomes possible to see that the Fourth Amendment has encountered threats from the mechanistic proliferation of problematic but constitutionally unregulated government acts in the past, and has attempted to address them in ways that provide lessons for the current moment.

The Article's proposal for the Fourth Amendment regulation of digital mass surveillance has two parts. First, courts should adopt a two-tiered approach to digital search that is analogous to the two-tiered approach to the seizure of persons under *Terry* and its progeny. Just as *Terry* holds that an arrest must be supported by probable cause, while a temporary detention—a *Terry* stop—need only be supported by reasonable suspicion that the seized person is engaged in criminal activity, so courts should hold that if an act of digital surveillance is sufficiently intrusive of an individual's privacy, the government must obtain a warrant backed by probable cause, but lesser intrusions should require only reasonable suspicion.[8]

Second, courts should sometimes engage in *programmatic* review of digital mass surveillance programs under the Fourth Amendment, rather than reviewing in isolation the individual acts of surveillance that constitute a program. Again, the proposal rests on an analogy to doctrine governing the seizure of persons, and in particular *Illinois v. Lidster*,[9] a 2004 Supreme Court case upholding the constitutionality of the brief, suspicionless seizure of drivers at a highway checkpoint.[10]

---

8 *See infra* Part III.B.

9 540 U.S. 419 (2004).

10 *See infra* Part III.C.

The need for both parts of the doctrinal solution can be understood by considering a hypothetical case involving a Fourth Amendment challenge to a digital mass surveillance program. Imagine, for example, that there is a surveillance program focused on preventing domestic terrorism that collects intuitively private information—say, web browsing histories, or location data from a smartphone app, or phone call records—about a relatively large number of Americans that the government has no reason to suspect of involvement in terrorism or any other crime. Imagine that some of the affected Americans learn that the government collected their information and file a lawsuit alleging that the surveillance program is unconstitutional under the Fourth Amendment.

Next, assume that the court believes the surveillance program's benefits to public safety outweigh its harms to Americans' privacy.[11] The court does not want to order the termination of the program, and is highly unlikely to do so. Although the surveillance program is focused on terrorism rather than crime in general, assume further that in the course of ordinary criminal investigations, the police frequently collect the same type of information that is at issue in our case—although, when domestic law enforcement collects the information, it does so through narrow requests focused on specific individuals suspected of criminal activity. Assume also that law enforcement representatives can persuasively argue that the police need the ability to collect this information without probable cause, early in an investigation, in order to develop probable cause and effectively enforce criminal laws against serious crimes such as hacking, white-collar financial crime, or child pornography.[12]

---

11 Some readers might object on principle that this could never be the case, and that safety interests could never justify the bulk collection of intuitively private digital data from Americans. For the purposes of this Article, however, it is not necessary to settle this normative issue. *See infra* note 165.

12 Evan Caminker observes:

> Many . . . types of third-party records (especially financial, credit card purchases, internet protocol addresses, and phone/text noncontent metadata) are routinely relied upon in early-stage investigations. And certain types of crimes would largely defy successful prosecution without early access to such third-party records. Obvious examples include white-collar financial crimes, identity theft, "[m]alicious hacking, possession of child pornography, laundering money through gambling websites, and insider trading**,**" which among other crimes "leave very few clues in the physical world." And proactive efforts to identify and thwart potential acts of terrorism require lots of background location and movement data from which computer algorithms can predict conventional behavior in order to discern unconventional and perhaps threatening aberrations.

Evan Caminker, *Location Tracking and Digital Data: Can* Carpenter *Build a Stable Privacy Doctrine?*, 12 S. CT. REV. 411, 465–66 (2018) (citations omitted); *see also* SUSAN LANDAU, LISTENING IN:

Assume, finally, that the court also believes that allowing the government to collect this category of intuitively private information without any Fourth Amendment restriction whatsoever would gravely undermine Americans' constitutional privacy interests. The court wants to issue a ruling that is protective of privacy.

How can the court reconcile these tensions between national security, law enforcement, and privacy? In particular, how can it do so while adhering as closely as possible to existing Fourth Amendment doctrine?

It would be unsatisfactory for the court to conclude that Americans do not have a reasonable expectation of privacy in the type of information at issue in the case, despite its intuitively very private nature. This is the status quo approach, and it remains the most likely outcome based on existing Fourth Amendment case law. The outcome preserves the surveillance program, but at the cost of allowing the government to collect, with no Fourth Amendment restrictions, an unlimited quantity of this private information about an unlimited number of Americans, into perpetuity, and to do whatever it wishes with this information once it has been collected. The status quo approach protects national security and law enforcement, but fails to protect privacy.

Another unsatisfactory outcome would be for the court to adopt only the first part of the doctrinal solution above. The court could take a two-tiered approach to digital search and conclude that the government only requires reasonable suspicion to collect from Americans the type of information collected by the surveillance program. By requiring a reasonable evidentiary basis for collection, but stopping short of requiring a warrant supported by probable cause, this approach could reconcile the needs of ordinary law enforcement with Americans' interest in privacy. But it would leave the terrorism-focused surveillance program unconstitutional, because the government lacks even reasonable suspicion that the information collected from each of the affected Americans will reveal evidence of a crime.

Yet another unsatisfactory outcome would be for the court to engage in programmatic review of the surveillance program, but maintain the one-tiered, current approach to Fourth Amendment search, according to which searches almost always require a warrant backed by probable cause. That is, the court could conclude that the Fourth Amendment requires probable

---

CYBERSECURITY IN AN INSECURE AGE 117–51 (2017) (describing the use of digital data in criminal investigations including hacking, terrorism, and child pornography).

cause to collect from Americans the type of private information collected by the surveillance program. The court could recognize that the government cannot establish it has probable cause to justify the searches at issue in the plaintiffs' lawsuit. But the court could nevertheless uphold the program by concluding that when the program is viewed as a whole, a balancing of the constitutionally relevant considerations leads to the conclusion that the program is reasonable under the Fourth Amendment. In this scenario, the court would be able to preserve the surveillance program and the privacy of most Americans—but would sacrifice the ability of domestic law enforcement to effectively enforce the criminal law.

Only by adopting both the two-tiered approach to digital search and the programmatic review of digital mass surveillance programs can the court reconcile the competing interests in national security, law enforcement, and privacy described above—while maintaining a grounding in existing Fourth Amendment doctrine, even if the doctrine in question is the Fourth Amendment law of seizure rather than of search.

Part I presents in greater detail the threats to privacy created by digital mass surveillance, and the obstacles to addressing those threats under existing Fourth Amendment case law. Part II begins the development of the structural analogy between seizure doctrine and search doctrine by presenting *Terry v. Ohio* as a response to the threat of mass seizure. Part III.A extends the analogy between seizure and search doctrine by arguing that *Carpenter* bears significant similarities to *Terry*. Part III.B argues that *Carpenter* opens the door to the development of a two-tiered doctrinal scheme for digital search, with less invasive searches requiring reasonable suspicion and more invasive searches requiring a warrant based on probable cause.

It is worth emphasizing at the outset that even if one believes *Terry* was a mistake, and that the Fourth Amendment should be understood to require probable cause for any seizure of a person, one should still embrace the two-tiered approach in the context of digital search. The only realistic alternative to a *Terry*-like, two-tiered approach to digital search is the status quo, in which the vast majority of digital surveillance by the state remains ungoverned by any constitutional restrictions.

Turning more specifically to the problems of digital *mass* surveillance, Part III.C addresses how Fourth Amendment doctrine can and should respond not only to the threats created by digital surveillance of individual criminal suspects, but to digital surveillance of larger numbers of people, communities, or the public as a whole. Once again, Fourth Amendment

seizure doctrine, and in particular *Lidster*, can provide a useful model. Finally, Part IV notes that the recent "mosaic theory" cases dealing with digital search simply apply to search the same aggregative form of reasoning that courts have long applied in the context of the seizure of persons. The mosaic theory cases represent a promising step toward the greater reconciliation of search and seizure doctrine that this Article recommends.

The Conclusion emphasizes the role that judicial enforcement of the Fourth Amendment can continue to play in protecting privacy from digital intrusion by the government, even as many of the most serious digital threats to privacy do not involve government actors and thus fall outside the reach of the Fourth Amendment. The Conclusion also notes the overlap between the Fourth Amendment concerns of this Article and the Fourteenth Amendment equal protection concerns that will often be raised by programs of digital mass surveillance.

I. THE FOURTH AMENDMENT IN THE AGE OF DIGITAL REPRODUCTION

The potential reach of state power has been transformed in recent years by developments in digital technology, from the arrival of email and web browsing in mainstream use a little over two decades ago, to the increasingly prominent role of smartphones and social media in everyday life over the last decade, to the rising significance of big data, artificial intelligence, and the "Internet of Things" in smart homes, vehicles, and cities today.[13] The proliferation of digital sensors and digital records in our daily lives has arrived so suddenly that constitutional doctrine has hardly begun to recognize the seriousness of the change. In particular, the Fourth Amendment has not yet come to terms with the government's historically unprecedented ability to conduct digital surveillance on a mass scale.

States and other powerful institutions have always had an appetite for legible, actionable knowledge about what they seek to control—whether their objects of concern are forests, markets, or the human populations of

---

13 For an accessible survey of the increasingly voluminous data produced in everyday life, and its relation to government and commercial surveillance, see BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 13–87 (2015). The distinguishing feature of digital data is the reduction of information to binary digits ("bits"). *See generally* C.E. Shannon, *A Mathematical Theory of Communication*, 27 BELL SYS. TECH. J. 379 (1948).

cities.[14] At the same time, this appetite has always been checked by technological and other material barriers that have effectively limited what even the most voracious and unconstrained institution might "see" and "know." Even Jeremy Bentham's imagined "panopticon" was premised on the notion that the prison could not afford enough watchmen to observe all the inmates individually.[15] So long as surveillance relied on paper records and the machinery of the flesh—the eyes and ears of watchmen and functionaries, the whispers of informants—the relatively high cost of human labor and the difficulty of storing and using collected information placed severe limits on the state's ability to monitor the public as a whole. The Stasi could not afford to place microphones in every home in East Germany, much less listen to and make use of the resulting intelligence.[16]

But the combination of inexpensive technologies for collecting, transmitting, storing, and analyzing digital data with the increasing public use of digital technologies—for communication, shopping, entertainment, and virtually every other facet of contemporary life—has created unprecedented opportunities for mass surveillance. It is technologically feasible for the state to simultaneously and continuously monitor the lives of the public as a whole, or of entire subsets of the public that the state finds deserving of interest, in ways that were not practical only a generation ago. The dystopian and discriminatory potential of digital mass surveillance is already being realized in some parts of the world—perhaps most notoriously in Xinjiang, a majority-Muslim region of northwestern China where party leaders have begun to develop the world's first digital prison state, alongside

---

14 *See* JAMES C. SCOTT, SEEING LIKE A STATE: HOW CERTAIN SCHEMES TO IMPROVE THE HUMAN CONDITION HAVE FAILED 2–5, 11–22 (1998) (discussing how powerful institutions impose order in part by creating "legibility" through simplification and using scientific forestry as an illustration).

15 *See* Jerome E. Dobson & Peter F. Fisher, *The Panopticon's Changing Geography*, 97 GEOGRAPHICAL REV. 307, 312–13 (2007) (describing cost reduction by the panopticon); Andrew B. Talai, Comment, *Drones and* Jones*: The Fourth Amendment and Police Discretion in the Digital Age*, 102 CALIF. L. REV. 729, 775 (2014) (describing the structure of the panopticon and its reception by various philosophers).

16 The Ministry for State Security of the German Democratic Republic (the "Stasi") was "[p]erhaps the most effective organization to engage in mass surveillance for social control in history." TIMOTHY H. EDGAR, BEYOND SNOWDEN: PRIVACY, MASS SURVEILLANCE, AND THE STRUGGLE TO REFORM THE NSA 8 (2017). This estimation is probably no longer true in light of the mass surveillance in Xinjiang, China. *See* Chris Buckley et al., *How China Turned a City into a Prison*, N.Y. TIMES (Apr. 4, 2019), https://www.nytimes.com/interactive/2019/04/04/world/asia/xinjiang-china-surveillance-prison.html.

a more traditional archipelago of totalitarian concentration camps.[17] In more liberal states, the uses of digital mass surveillance have been less intrusive. But the appetite of even relatively liberal governments for knowledge about those within their jurisdictions remains strong, as seen, for example, in the National Security Agency's ("NSA") bulk collection of Americans' digital data,[18] or the Los Angeles Police Department's use of digital surveillance and data-mining software to identify likely criminals before their criminal acts have occurred.[19]

In sum, digital technologies and the public's use of them have created an unprecedented threat to the private sphere that, on many accounts, rests at the core of liberalism.[20] What has been the response of the Constitution, and particularly the Fourth Amendment?

The general claim that Fourth Amendment search doctrine requires reform in order to address the novel threats of the digital age will be familiar to anyone who has followed the scholarship on digital privacy and the Fourth

---

17 *See* Buckley et al., *supra* note 16.

18 The reformed version of one of the NSA's bulk collection programs may recently have ended, but others remain in place. *See* Charlie Savage, *Disputed N.S.A. Phone Program Is Shut Down, Aide Says*, N.Y. TIMES (Mar. 4, 2019), https://nyti.ms/2Vy3gDW; Zack Whittaker, *NSA Says Warrantless Searches of Americans' Data Rose in 2018*, TECHCRUNCH (Apr. 30, 2019), https://techcrunch.com/2019/04/30/nsa-surveillance-spike/ (summarizing intelligence community's annual transparency report). According to Edward Snowden, at least, not all of the NSA's use of Americans' data has been incidental to foreign surveillance. *See, e.g.*, Glenn Greenwald, *XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet'*, GUARDIAN (July 31, 2013), https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data (describing an NSA tool that can target American citizens for extensive electronic surveillance without a warrant).

19 Peter Waldman et al., *Palantir Knows Everything About You*, BLOOMBERG BUSINESSWEEK (Apr. 19, 2018), https://www.bloomberg.com/features/2018-palantir-peter-thiel/.

20 *See* STEVEN LUKES, INDIVIDUALISM 61–62 (1973); JUDITH N. SHKLAR, *The Liberalism of Fear*, *in* POLITICAL THOUGHT AND POLITICAL THINKERS 3, 6 (Stanley Hoffmann ed., 1998) (defining liberalism as committed to securing "the political conditions that are necessary for the exercise of personal freedom," and noting that Shklar's "liberalism of fear" "must reject only those political doctrines that do not recognize any difference between the spheres of the personal and the public"). The philosopher Charles Taylor suggests the stakes of current constitutional debates over privacy and digital surveillance when he notes that without "the private domain" serving as a kind of anti-structure opposing the structure of our increasingly disciplined and comprehensively ordered world, "life in modern society would be unliveable." CHARLES TAYLOR, A SECULAR AGE 52 (2007) (drawing on the anthropologist Victor Turner's discussion of structure and anti-structure in human societies to suggest that "[t]he public/private distinction, and the wide area of negative freedom, is the equivalent zone" in liberal, pluralist societies to the vital zones of anti-structure in earlier societies, such as medieval European carnivals and other "festivals of reversal").

Amendment in the last two decades.[21] The ultimate focus of this Article is one aspect of digital surveillance that has not always been at the center of conversations about the Fourth Amendment law of digital search, perhaps in part because it is rarely the subject of Fourth Amendment case law: the failures of existing Fourth Amendment search doctrine to protect against digital *mass* surveillance.[22]

Current Fourth Amendment case law does more than fail to provide adequate constitutional restrictions on governmental collection of digital

---

21 *See, e.g.*, Laura K. Donohue, *The Fourth Amendment in a Digital World*, 71 N.Y.U. ANN. SURV. AM. L. 553, 556 (2017); Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 574 (2017) ("[B]lind application of non-digital precedent to a digital problem did not offer much Fourth Amendment protection."); David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 67 (2013); Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1311 (2012); Christopher Slobogin, *Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine*, 102 GEO. L.J. 1721, 1723 (2014) (noting that current Fourth Amendment jurisprudence "has nothing to say about . . . surveillance even when it takes place in the absence of any suspicion about the people targeted")); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1084 (2002). An earlier wave of privacy concerns regarding computerized records and "data banks" arrived in the mid-1960s to 1970s. *See generally* SARAH E. IGO, THE KNOWN CITIZEN: A HISTORY OF PRIVACY IN MODERN AMERICA 221–63 (2018); ALAN F. WESTIN, PRIVACY AND FREEDOM 3 (1967).

22 There are, of course, many exceptions, including the works of Christopher Slobogin. *See, e.g.*, Christopher Slobogin, *Policing, Databases, and Surveillance*, *in* 2 REFORMING CRIMINAL JUSTICE 209–32 (Erik Luna ed., 2017); Christopher Slobogin, *Policing as Administration*, 165 U. PA. L. REV. 91, 122 (2016); Slobogin, *supra* note 21; Christopher Slobogin, *Government Dragnets*, 73 L. & CONTEMP. PROBS. 107, 108 (2010); Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 321 (2008). There is also a voluminous scholarship on the bulk collection of digital communications metadata. *See, e.g.*, Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL'Y 757 (2014). But in many cases, the scholarship on Fourth Amendment digital search doctrine has tended to mirror Fourth Amendment case law by focusing on surveillance of targeted individuals or small groups. *See, e.g.*, ORIN S. KERR, *Implementing* Carpenter, *in* THE DIGITAL FOURTH AMENDMENT 50 (forthcoming). One reason that digital mass surveillance appears so rarely in Fourth Amendment case law may be that the subjects of such surveillance often do not know they are being surveilled. In addition, even when potential litigants suspect they are being surveilled, they often lack sufficient evidence to establish standing. *See infra* note 26 (describing an instance where plaintiffs lacked standing because their theory was "too speculative"). Another reason may be that state actors have deliberately concealed the role of digital mass surveillance in the collection of evidence used in criminal cases. *See, e.g.*, HUMAN RIGHTS WATCH, DARK SIDE: SECRET ORIGINS OF EVIDENCE IN CRIMINAL CASES (2018), *available at* https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases (describing the practice of "parallel construction," where "an official who wishes to keep an investigative activity hidden from courts and defendants—and ultimately from the public—can simply go through the motions of re-discovering evidence in some other way"); Charlie Savage, *D.E.A. Secretly Collected Bulk Records of Money-Counter Purchases*, N.Y. TIMES (Mar. 30, 2019), https://nyti.ms/2UiUigP.

data about individuals who are under investigation—as scholars have long argued and the Court itself has begun to recognize.[23] The existing case law also fails to protect members of the public who are not under investigation, but whose privacy may be invaded in less obvious ways by large-scale, relatively indiscriminate surveillance programs that rely on digital technologies, such as programs for the bulk collection of communications metadata.[24] It is especially unclear, based on the existing case law, how Fourth Amendment search doctrine could protect members of the public from forms of digital surveillance that might seem relatively uninvasive when viewed in isolation—at a single moment, in a single place, with regard to a single individual—but that might threaten core privacy interests if allowed to proliferate across whole populations without any constitutional check.

The trouble results in part from the fact that in any context in which Fourth Amendment doctrine holds that digital data is not protected by a reasonable expectation of privacy, it also holds that the Fourth Amendment places no restriction on the government collection of that data regarding *an unlimited number of individuals*. As the Foreign Intelligence Surveillance Court ("FISC") stated in one of its decisions approving the constitutionality of the NSA's warrantless collection of Americans' phone call metadata: "where one individual does not have a Fourth Amendment interest, grouping together a large number of similarly-situated individuals cannot result in a Fourth Amendment interest springing into existence *ex nihilo*."[25] The implications of

---

23 *See supra* note 21; *infra* Part III.A.

24 *See generally* Donohue, *supra* note 22, at 863–97. It is because digital mass surveillance tends to be indiscriminate that some writers have used the term "dragnet" to refer to it. *See, e.g.*, JULIA ANGWIN, DRAGNET NATION: A QUEST FOR PRIVACY, SECURITY, AND FREEDOM IN A WORLD OF RELENTLESS SURVEILLANCE 3 (2014) ("We are living in a Dragnet Nation—a world of indiscriminate tracking where institutions are stockpiling data about individuals at an unprecedented pace."); Slobogin, *Government Dragnets*, *supra* note 22, at 210–11.

25 *In re* F.B.I., No. BR 13-109, 2013 WL 5741573, at *2 (FISA Ct. Aug. 29, 2013). The metadata collected in *In re F.B.I.* was ostensibly collected pursuant to section 215 of the USA Patriot Act. *See id.* at *1. For a similar expression of the principle of nonaggregation, see *United States v. Jones*, 625 F.3d 766, 769 (D.C. Cir. 2010) (Sentelle, C.J., dissenting) ("The reasonable expectation of privacy as to a person's movements on the highway is . . . zero. The sum of an infinite number of zero-value parts is also zero."); *cf.* Wainwright v. Lockhart, 80 F.3d 1226, 1233 (8th Cir. 1996) ("Errors that are not unconstitutional individually cannot be added together to create a constitutional violation."). *But see generally* Kerry Abrams & Brandon L. Garrett, *Cumulative Constitutional Rights*, 97 B.U. L. REV. 1309 (2017) (collecting exceptions to the rule that a series of constitutional acts cannot be aggregated into an unconstitutional act).

this principle of nonaggregation in an age of low-cost digital technologies are remarkable.

In order to understand why, it is helpful to understand how courts analyze the constitutionality under the Fourth Amendment of a government act of digital surveillance. Assuming a party has standing to contest the constitutionality of the surveillance at all,[26] courts generally begin by asking whether the act of surveillance constituted a "search" under the Fourth Amendment. The latter inquiry is in turn based on whether the government violated a reasonable expectation of privacy.[27] Two limitations on the scope of constitutional privacy are especially significant in the context of digital mass surveillance.

---

26 "To establish Article III standing, an injury must be 'concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.'" Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401, 409 (2013) (internal citation omitted) (holding that plaintiffs lacked standing to challenge surveillance activities in part because their theory that "there is an objectively reasonable likelihood that their communications will be acquired" was "too speculative"); *see also* David Gray, *Collective Standing Under the Fourth Amendment*, 55 AM. CRIM. L. REV. 77, 97–103 (2018) (proposing a solution to the problem of standing and digital mass surveillance by arguing that "[a]ny member of 'the people' forced to live in fear of unreasonable searches or seizures by definition has standing to challenge search and seizure means, methods, and programs"); Christopher Slobogin, *Standing and Covert Surveillance*, 42 PEPP. L. REV. 517, 518 (2015) (analyzing the difficulty of establishing standing to challenge covert digital surveillance programs). A premise of this Article, however, is that standing doctrine is sufficiently flexible that if a court wished to confront the constitutionality of a program of digital mass surveillance under the Fourth Amendment, standing would not always pose an insurmountable hurdle. *See, e.g.*, Parents Involved in Cmty. Schs. v. Seattle Sch. Dist. No. 1, 551 U.S. 701, 718–19 (2007) (brushing aside standing concerns in order to address claim of discrimination against whites). In fact, despite *Clapper v. Amnesty International*, at least some plaintiffs have succeeded in establishing standing to challenge the collection of their data through digital mass surveillance programs. *See, e.g.*, ACLU v. Clapper, 785 F.3d 787, 801 (2d Cir. 2015) (holding that appellant civil liberties organizations had established standing because "the government's own orders demonstrate that appellants' call records are indeed among those collected as part of the telephone metadata program").

27 *See* Carpenter v. United States, 138 S. Ct. 2206, 2213, 2217 (2018) (citing Katz v. United States, 389 U.S. 347, 351–52 (1967)); *Katz*, 389 U.S. at 361 (Harlan, J., concurring). Scholars have offered many critiques of the "reasonable expectation of privacy" test, including critiques based on its manipulability, circularity, and failure to capture the purposes of the Fourth Amendment. *See, e.g.*, Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1515 (2010) (arguing that the reasonable expectation of privacy test should be abandoned). The Court has also reaffirmed that a search takes place whenever the government engages in a physical intrusion of a constitutionally protected area. *See* Florida v. Jardines, 569 U.S. 1, 5–7 (2013).

First, because the Supreme Court has held that there is no reasonable expectation of privacy in what is exposed to the public,[28] existing search doctrine suggests that nothing under the Fourth Amendment prevents the government from surveilling a *public* space. The principle seems uncontroversial enough. Surely the police, for example, should be at least as free to observe a public space as any member of the public.

But once the general principle that the Fourth Amendment does not apply to the surveillance of public spaces is combined with the introduction of low-cost digital surveillance technologies and the principle of nonaggregation, more troubling possibilities emerge. Is it consistent with the underlying values of the Fourth Amendment for the government to continuously, comprehensively surveil every public space in a city using a panoply of digital video cameras, microphones, and other sensors—including not only fixed cameras but police dashboard cams and bodycams, cameras in public transportation, and cameras mounted on drones—with the results continuously transmitted to a centralized system for real-time facial recognition, license plate analysis, and permanent storage?[29] Is it consistent with the Fourth Amendment for the government to keep a

---

28 *See, e.g.*, California v. Greenwood, 486 U.S. 35, 40–41 (1988) (holding that there was no search where the police inspected garbage that was "exposed . . . to the public," because "the police cannot reasonably be expected to avert their eyes from evidence of criminal activity that could have been observed by any member of the public"); California v. Ciraolo, 476 U.S. 207, 213 (1986) (holding that there was no search where the police conducted aerial surveillance of defendant's backyard); United States v. Karo, 468 U.S. 705, 707, 716 (1984) (holding that use of beeper to track a can of ether into private home was a search because, unlike in *Knotts*, the property had been "withdrawn from public view"); United States v. Knotts, 460 U.S. 276, 281–82, 285 (1983) (holding that use of beeper to track vehicle as it traveled along public roads was not a search because "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another," and the driver "voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads"). David Gray refers to this principle as "the public observation doctrine," in order to distinguish it from the "third-party doctrine," discussed below. *Compare* Gray, *supra* note 26, at 77, *with* sources cited *infra* note 35.

29 On the Fourth Amendment problems created by facial recognition technology in particular, see Andrew Guthrie Ferguson, *Facial Recognition and the Fourth Amendment*, 105 MINN. L. REV. (forthcoming). Current Fourth Amendment case law also places no constraints on the government collection of DNA samples from public spaces. *See generally* Elizabeth E. Joh, *DNA Theft: Recognizing the Crime of Nonconsensual Genetic Collection and Testing*, 91 B.U. L. REV. 665, 666 (2011) ("[T]he nonconsensual collection and analysis of another person's DNA is virtually unconstrained by law."); Elizabeth E. Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 NW. L. REV. 857, 858 (2006) (questioning the consequences of allowing DNA collection by the government to remain largely unregulated).

permanent, searchable[30] record of every step, every trip to the psychiatrist, bar, or mosque, every discernable movement of the lips, every sign of illness or anger, by every inhabitant of a city in the United States, into perpetuity?[31] Under current doctrine, all such surveillance is categorically outside the scope of Fourth Amendment protection, because it simply collects information exposed to the public. If the installation of one camera in a public space is constitutional, so is the installation of ten thousand, or ten million.[32]

Second, the principle of nonaggregation and the development of low-cost digital surveillance technology interacts in an even more troubling way with the Supreme Court's long-disputed,[33] recently limited,[34] but still very much alive "third-party doctrine," which holds that when an individual exposes materials to a third party, the individual loses any reasonable expectation

---

30 *See* Emily Berman, *When Database Queries Are Fourth Amendment Searches*, 102 MINN. L. REV. 577, 578 (2017) ("So long as its collection is lawful, the Fourth Amendment has nothing to say about how information is employed."); Slobogin, *Databases*, *supra* note 22, at 212 (citing Erin Murphy, *DNA in the Criminal Justice System: A Congressional Research Service Report* (*From the Future)*, 64 UCLA L. REV. DISCOURSE 340, 364 (2016)) (noting that "the Constitution appears to have little to say about law enforcement agencies' access to . . . information once they or other government entities legitimately collect it").

31 Against the objection that political forces would prevent the development of city-wide digital surveillance in our democracy, it might be argued that the limits of political tolerance for the surveillance of public spaces are far from clear, and may be especially weak if the surveillance is covert or if it is concentrated in, for example, "high crime areas" or politically marginalized communities. *See infra* Conclusion (discussing equal protection issues in digital mass surveillance). It might also be noted that democratic forces did not prevent, to take one example, the NYPD from establishing a "Domain Awareness System" that integrates public and private surveillance camera footage with information from license plate readers and MetroCard swipes. *See* Faiza Patel & Michael Price, *Keeping Eyes on NYPD Surveillance*, BRENNAN CTR. FOR JUST. (June 13, 2017), https://www.brennancenter.org/our-work/analysis-opinion/keeping-eyes-nypd-surveillance.

32 *See generally* EYES EVERYWHERE: THE GLOBAL GROWTH OF CAMERA SURVEILLANCE (Aaron Doyle et al. eds., 2012). Analysts estimate there are roughly 770 million security cameras in the world today, roughly half of them in China, and that the global total will increase to more than one billion by the end of 2021. Liza Lin & Newley Purnell, *A World With a Billion Cameras Watching You Is Just Around the Corner*, WALL STREET J. (Dec. 6, 2019), https://www.wsj.com/articles/a-billion-surveillance-cameras-forecast-to-be-watching-within-two-years-11575565402 (noting the "number of surveillance cameras in the U.S. would grow to 85 million by 2021, from 70 million last year, as American schools, malls and offices seek to tighten security on their premises"); *see also* Paul Mozur, *Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras*, N.Y. TIMES (July 8, 2018), https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html.

33 *See, e.g.*, Jane Bambauer, *Other People's Papers*, 94 TEX. L. REV. 205, 208 (2015) (arguing that there is "good reason" to dismantle the third-party doctrine, because it "always strained the logic and common sense of search and seizure law").

34 *See* discussion of *Carpenter infra* Part III.A.

that what has been exposed will remain private.[35] Because, again, the Fourth Amendment does not generally offer protections against search where there is no reasonable expectation of privacy, the third-party doctrine generally holds that the government is free to obtain the exposed materials from the third party without any Fourth Amendment restrictions.[36]

The FISC's conclusion that the NSA's warrantless bulk collection of Americans' phone call metadata did not violate the Fourth Amendment illustrates the troubling consequences when the third-party doctrine meets digital technology and the principle of nonaggregation.[37] Based on a 1979 Supreme Court holding that there was no search when the police collected a list of the numbers dialed on a single suspect's phone as part of a criminal investigation,[38] the FISC effectively concluded that under the Fourth Amendment, the government may collect, analyze, and permanently store the digital communications metadata of every American, continuously and for all time, without ever showing any evidentiary basis or law enforcement need.[39] Again, we might wonder: is it consistent with the underlying values

---

35 *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (finding no reasonable expectation of privacy in record of telephone numbers dialed because the numbers were conveyed to the third-party phone company); United States v. Miller, 425 U.S. 435, 443 (1976) (holding that there was no reasonable expectation of privacy in financial records at a bank because "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities"). *See generally* Solove, *supra* note 21 (discussing third-party doctrine in the context of digital data collection). If location tracking cases such as *Knotts* and *Karo* analyze the boundaries of the reasonable expectation of privacy by emphasizing the distinction between public spaces and private spaces, third-party doctrine cases such as *Miller* and *Smith* emphasize, by contrast, the "assumption of risk" principle—that is, the notion that someone takes a "risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government." *See Smith*, 442 U.S. at 743–44; *Miller*, 425 U.S. at 443 (citing Hoffa v. United States, 385 U.S. 293, 302 (1966)) ("Neither this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."); *see also supra* note 28 (discussing *Knotts* and *Karo*). From an abstract point of view, of course, holding that there is no reasonable expectation of privacy in what is exposed to the public could be seen as a special case of the more general principle that there is no reasonable expectation of privacy in what is exposed to a specific third party entity.

36 *See supra* note 35.

37 *See In re* F.B.I., No. BR 13-109, 2013 WL 5741573, at *2–3 (FISA Ct. Aug. 29, 2013).

38 *See Smith*, 442 U.S. at 745–46.

39 *See generally* Donohue, *supra* note 22 (discussing the relation between bulk telephone metadata collection and *Smith*). Of course, a variety of statutes regulate the government collection of digital data. *See* Solove, *supra* note 21, at 1085–86, 1138–51 (describing how "[i]n the void left by the absence of Fourth Amendment protection, a series of statutes provide some limited restraints on government access to third party records," and analyzing some of the relevant statutes); *infra* Conclusion (arguing that legislation, regulation, and social mobilization are likely the most

of the Fourth Amendment for the government to keep a comprehensive, permanent, searchable digital record of every person or entity with whom I have ever exchanged a phone call,[40] email, text message, or for that matter physical letter?[41]

In fact, the perils of combining the principle of nonaggregation with the third-party doctrine in an era of low-cost digital technology extend even further than the bulk collection of digital communications metadata. The digital data Americans share with third parties potentially include streaming video and audio from our smartphones and smart home appliances;[42] any

---

significant and urgent avenues for the protection of digital privacy in the United States today). Perhaps the most important statutory protection for the communications metadata records that have been one of the primary focuses of digital mass surveillance in the United States is the Stored Communications Act ("SCA"). *See* Electronic Communications Privacy Act (ECPA) of 1986, P.L. 99-508, 100 Stat. 1848, 1860–68 (1986) (codified at 18 U.S.C. §§ 2510–2523, 2701–2713); Susan Freiwald & Stephen Wm. Smith, *The* Carpenter *Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 208 (2018) (discussing the SCA); *infra* note 128 (same). It is also worth emphasizing that the Fourth Amendment has been interpreted to protect the *contents* of communications in many contexts, even when the contents are transmitted through a third party such as a mail carrier, a telephone service provider, or an email or Internet service provider. *See, e.g.*, United States v. Warshak, 631 F.3d 266, 283–88 (6th Cir. 2010) (protecting the contents of e-mails); *Ex parte* Jackson, 96 U.S. 727, 733 (1878) (protecting the contents of letters). *See generally* Chris Conley, *Non-Content Is Not Non-Sensitive: Moving Beyond the Content/Non-Content Distinction*, 54 SANTA CLARA L. REV. 821, 824 (2014) ("The distinction between content and non-content has been part of the Supreme Court's Fourth Amendment jurisprudence since the nineteenth century."); Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105 (2009) ("Whether a component of an Internet communication is classified as 'content' or 'envelope' information determines in large part the privacy protection it receives under constitutional and statutory law.").

40 *See Smith*, 442 U.S. at 741–42, 745–46 (determining that Fourth Amendment protections do not apply to call records); KERR, *supra* note 22, at *45 (arguing that even in the wake of *Carpenter*, "[n]umbers dialed for phone calls should continue to be unprotected under *Smith v. Maryland*").

41 The United States Postal Service ("USPS") has begun "photographing and recording the outside of each of the roughly 160 billion mail parcels it handles each year." Julie Lynn Rooney, Note, *Going Postal: Analyzing the Abuse of Mail Covers Under the Fourth Amendment*, 70 VAND. L. REV. 1627, 1629 (2017). In addition, through its "mail cover" surveillance program, "throughout 2014 the USPS documented, at the request of law enforcement agencies, the addresses, return addresses, postal dates, and other information appearing on the outside of each parcel of mail sent and received by over 50,000 individuals for extended periods of time." *Id.* at 1628–29. The Supreme Court has held that the outsides of envelopes are not protected by the Fourth Amendment. *See Ex parte Jackson*, 96 U.S. at 733; discussion *supra* note 39.

42 *See, e.g.*, Chavie Lieber, *Amazon's Alexa Might Be a Key Witness in a Murder Case*, VOX (Nov. 12, 2018), https://www.vox.com/the-goods/2018/11/12/18089090/amazon-echo-alexa-smart-speaker-privacy-data (describing how a court ordered Amazon to produce audio records from an Echo device, and recounting other investigative requests for data from devices such as iPhones and Fitbits); Ben Popken, *Your Smart TV Is Watching You Watching TV, Consumer Reports Finds*, NBC NEWS (Feb. 7, 2018), https://www.nbcnews.com/tech/security/your-smart-tv-watching-you-watching-tv-consu

private documents we save in the cloud;[43] any records of our digital activity captured by social media platforms or other websites, apps, or devices, including, for example, location data or health-related information; financial records from banks and credit card companies;[44] Internet service provider records of web sites visited, which in many cases might indirectly reveal the contents of communications;[45] similar tracking information provided by a web browser's cookies or extensions; and even digitized medical records from doctors' offices, which the Supreme Court has never held to be protected by a reasonable expectation of privacy.[46] Would it be consistent with the values underlying the Fourth Amendment for the government to collect, store, and

---

mer-reports-finds-n845456 (describing how "[m]illions of smart TVs sitting in family living rooms . . . could be tracking the household's personal viewing habits much more closely than their owners realize"); Amy B. Wang, *'I'm in Your Baby's Room': A Hacker Took Over a Baby Monitor and Broadcast Threats, Parents Say*, WASH. POST (Dec. 20, 2018), https://www.washingtonpost.com/technology/2018/12/20/nest-cam-baby-monitor-hacked-kidnap-threat-came-device-parents-say/ (describing surveillance through hacked home security and baby monitoring devices). The government would presumably require a warrant to engage in video surveillance within someone's home, which the Fourth Amendment has always treated as the quintessentially private space. *See, e.g.*, United States v. Cuevas-Sanchez, 821 F.2d 248, 251–52 (5th Cir. 1987) (holding that the government needed a warrant to engage in video surveillance of a backyard). But to the extent that a person sent a video to a business with the expectation that someone at the business would view it, the sender would presumably have no reasonable expectation of privacy under the third-party doctrine. *See supra* note 35. The case is less clear when the video is transmitted to a business as a routine part of its creation, such as when wireless cameras transmit videos to a third party for viewing on an app, or when a video is saved in cloud storage. *Cf.* KERR, *supra* note 22 (implying that Fourth Amendment might not protect digital data stored by a third-party business if "participation in modern society" did not require use of the technology, if "a user made a voluntary decision to allow a third-party to generate that record," or if "a person volunteers to reveal information about himself to others, beyond what the technology requires"); Eric Johnson, Note, *Lost in the Cloud: Cloud Storage, Privacy, and Suggestions for Protecting Users' Data*, 69 STAN. L. REV. 867 (2017) (suggesting Fourth Amendment protection of data stored in the cloud depends in part on the terms of service).

43 *See generally* Neil Richards, *The Third Party Doctrine and the Future of the Cloud*, 94 WASH. U. L. REV. 1441 (2017); Johnson, *supra* note 42.

44 *See* United States v. Miller, 425 U.S. 435, 437 (1976). Credit card companies already sell records of credit card transactions to other businesses. *See, e.g.*, Mark Bergen & Jennifer Surane, *Google and Mastercard Cut a Secret Ad Deal To Track Retail Sales*, BLOOMBERG (Aug. 31, 2018), https://www.bloomberg.com/news/articles/2018-08-30/google-and-mastercard-cut-a-secret-ad-deal-to-track-retail-sales.

45 *See* Donohue, *supra* note 21, at 556.

46 *See* Solove, *supra* note 27, at 1532 (noting that *Miller* would seem to dictate that the Supreme Court should "hold that people lack an expectation of privacy in their medical data because they convey that information to their physicians," even though the result would "strike many as absurd"). *But see* Stephen E. Henderson, *After* United States v. Jones*, After the Fourth Amendment Third Party Doctrine*, 14 N.C. J.L. & TECH. 431, 444 (2013) (noting that some lower courts have "granted Fourth Amendment protection to medical records residing with a third party provider").

analyze all of the preceding categories of data, simply because that data was transmitted to a third-party business?

In the landmark 2018 decision *Carpenter v. United States*,[47] the Supreme Court took a significant step toward addressing the threats to privacy created by the third-party doctrine in the digital age, recognizing for the first time an exception to the doctrine in the context of the government collection of digital data.[48] But Chief Justice Roberts' majority opinion in *Carpenter*, discussed at greater length below,[49] only explicitly excludes from the third-party doctrine certain cell-site location information ("CSLI") generated by cell phones.[50] In addition, rather than grappling with how the rise of low-cost digital surveillance technologies radically alters the privacy effects of the doctrine that what is exposed to the public is not protected by the Fourth Amendment, Roberts' opinion explicitly notes that "[o]ur decision today" does not "call into question conventional surveillance techniques and tools, *such as security cameras*."[51] Based on this cautionary note, and in the interest of simplicity, the examples and hypothetical scenarios in the remainder of this Article will largely focus on the constitutional protection of digital data shared with third parties, rather than the surveillance of public spaces using digital technologies.[52]

---

47 138 S. Ct. 2206 (2018).

48 *See id.* at 2217.

49 *See infra* Part III.

50 *Carpenter*, 138 S. Ct. at 2217.

51 *Id.* at 2220 (emphasis added).

52 An attempt to apply the reasoning in this Article to the problem of the digital mass surveillance of public spaces might begin by noting that nearly all of the most dystopian privacy implications of the mass surveillance of public spaces depend on some automated technological means of identifying and recording the locations and behaviors of individuals, such as facial recognition, gate recognition, or license plate reading. A case could be made that in a world where low-cost digital technologies facilitate the pervasive, constant surveillance of public spaces, automated recognition technologies pose such a profound and unprecedented threat to privacy that they justify a dramatic departure in Fourth Amendment doctrine, similar to the departure *Carpenter* carried out with regard to the third-party doctrine. *Cf.* Evan Selinger & Woodrow Hartzog, Opinion, *What Happens When Employers Can Read Your Facial Expressions?*, N.Y. TIMES (Oct. 17, 2019), https://www.nytimes.com/2019/10/17/opinion/facial-recognition-ban.html ("Facial recognition is truly a one-of-a-kind technology—and we should treat it as such."). Thus, rather than attempting to carve out an exception to the doctrine that what is exposed to the public is not protected by the Fourth Amendment—an exception that seems especially unlikely in light of *Carpenter*'s dictum regarding surveillance cameras—the constitutional problem of the mass digital surveillance of public spaces could perhaps be addressed by carving out an exception to the doctrine that the Fourth Amendment does not regulate the government's *use* of information it has already collected. *See* Berman, *supra* note 30, at 578 ("[T]here are no constitutional restrictions at all on how the government uses this

Even with regard to digital data held by third parties, however, it remains deeply unclear how far and in what ways the Supreme Court will extend Fourth Amendment privacy protections based on *Carpenter*.[53] Above all, it remains unclear, even in the wake of *Carpenter*, how the Court might respond to the particular problems of digital *mass* surveillance. It has often been remarked that Fourth Amendment doctrine has been distorted by being developed, for the most part, in the context of motions by criminal defendants to suppress evidence.[54] A court may be more likely to find a practice constitutionally unobjectionable if the court only sees examples of the practice that resulted in the decision to prosecute. Courts might perceive a practice very differently if they were instead routinely exposed to the individuals who were subjected to the practice without any charges ultimately being filed.[55]

Less attention has been paid to the way that the "transactional"[56] focus of the Fourth Amendment effectively eliminates the possibility of recognizing

---

vast expanse of data."). Courts could, for example, develop Fourth Amendment restrictions on the application of automated recognition technologies to the surveillance of public spaces. *Cf.* LAURA K. DONOHUE, THE FUTURE OF FOREIGN INTELLIGENCE 153–54 (2016) (arguing for a "use restriction for Fourth Amendment doctrine," and citing as indirect support *Riley v. California*, 573 U.S. 373 (2014)); Harold J. Krent, *Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment*, 74 TEX. L. REV. 49, 51 (1995) (arguing for use restrictions under the Fourth Amendment).

But it must be conceded that this would be a very significant departure from Fourth Amendment doctrine and could be seen as opening up a Pandora's box of Fourth Amendment challenges to the government use of data in other contexts. Because this Article is focused on plausible doctrinal responses to digital mass surveillance that are grounded in existing Fourth Amendment case law, it will not address the problem of the digital mass surveillance of public spaces further. Under existing Fourth Amendment doctrine, this problem may simply have no plausible solution.

53 *See, e.g.*, KERR, *supra* note 22 (considering how to apply *Carpenter* to contexts involving digital data other than historical CSLI records); Eunice Park, *Objects, Places and Cyber-Spaces Post-*Carpenter*: Extending the Third-Party Doctrine Beyond CSLI*, 21 YALE J.L. & TECH. 1 (2019).

54 *See, e.g.*, William J. Stuntz, *Warrants and Fourth Amendment Remedies*, 77 VA. L. REV. 881, 912–13 (1991); *see also* Nancy Leong, *Making Rights*, 92 B.U. L. REV. 405, 428 (2012).

55 To take the familiar example of "stop-and-frisk," if courts were routinely exposed to the stories of the thousands of individuals who are stopped, questioned, and frisked without any further evidence of criminal activity being uncovered, rather than only to the stories of those comparatively few individuals who are arrested, charged, and then move to suppress the evidence obtained through their stops, it is easy to imagine courts insisting on a more exacting standard of "reasonable suspicion" than police departments have sometimes employed.

56 For the critique of Fourth Amendment doctrine as excessively shaped by a focus on individual encounters or "transactions" rather than programmatic or systemic considerations, see generally Aziz Z. Huq, *The Consequences of Disparate Policing: Evaluating Stop and Frisk as a Modality of Urban Policing*, 101 MINN. L. REV. 2397 (2017); Tracey L. Meares, *Programming Errors: Understanding the Constitutionality of Stop-and-Frisk as a Program, Not an Incident*, 82 U. CHI. L. REV. 159 (2015). For a

any constitutional difference between a potentially objectionable act being carried out in relation to a single individual, in an *ad hoc* manner, on one occasion, and the same act being carried out programmatically in relation to a hundred or indeed three hundred and fifty million individuals. Intuitively, it might seem that it should sometimes make some difference under the Fourth Amendment whether an act of surveillance is carried out on a one-time, individually focused basis, or through perpetual mass surveillance affecting nearly every member of the population. But as the FISC suggested, under existing doctrine, if an act is not a "search" when carried out once, then it requires no evidentiary justification under the Fourth Amendment to be carried out on an unlimited number of subjects.[57]

In the Founding Era, when every search tended to require a significant expenditure of human labor, and the federal government had relatively few employees, the threat of a constitutional form of investigation increasing in quantity until it became a qualitatively different threat to the values protected by the Fourth Amendment might have seemed minor.[58] But as Warren and Brandeis already recognized in 1890, the development of technologies capable of mechanical reproduction can change what permissions and prohibitions are necessary to protect privacy.[59] Their insight is even more true in the age of digital reproduction. As noted above, it has now become technologically feasible for governments to replicate certain forms of centralized, digital surveillance across whole populations. Yet the Fourth Amendment has thus far appeared incapable of recognizing that this replication has any legal significance.

The next Part will turn to a discussion of seizure doctrine, with the ultimate goal of suggesting that it shows a way in which Fourth Amendment doctrine can respond to problematic increases in the frequency of constitutionally problematic acts. But before entering that discussion, it will

---

more general critique of the way transactions are framed in constitutional law, see generally Daryl J. Levinson, *Framing Transactions in Constitutional Law*, 111 YALE L.J. 1311 (2002).

57 *See In re* F.B.I., No. BR 13-109, 2013 WL 5741573, at *2 (FISA Ct. Aug. 29, 2013).

58 It might be noted, however, that even in the Founding Era, the drafters of the Fourth Amendment were particularly hostile to general warrants, and digital mass surveillance practices such as bulk collection of metadata could be seen as the contemporary equivalents of general warrants. *See* Slobogin, *supra* note 21, at 1722–23 (discussing the Fourth Amendment's hostility to general warrants in relation to "panvasive" digital surveillance).

59 *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195–96 (1890) (arguing for a common-law right to privacy partly in response to the growing use of photographs in mass-produced newspapers).

be helpful to clarify certain distinctions that the preceding discussion deliberately blurred in order to draw attention to the inadequacies of the existing Fourth Amendment law of digital search.

Going forward, this Article will keep distinct two senses of the "quantity" of surveillance. The principle of nonaggregation only applies to one of the two. On the one hand, we can speak of the quantity of surveillance conducted on an individual over some period of time, or—viewing the same surveillance in terms of its results—the quantity of information collected about an individual. As discussed in Part IV, the "mosaic theory" of digital search already allows for the aggregation of this quantity. As a result, existing Fourth Amendment doctrine already provides a basis, at least in principle, for placing constitutional limits on the quantity of surveillance directed toward an individual, or the quantity of information collected about her.

On the other hand, we can speak of the quantity of individuals subjected to some form of surveillance. In the interests of clarity, the Article will henceforth refer to this sense of quantity as the "frequency" of surveillance. As the quotation from the FISC opinion above suggested,[60] current Fourth Amendment doctrine does not allow for the aggregation of acts of surveillance across individuals. As a result, the Fourth Amendment is doctrinally blind to increases or decreases in the frequency of constitutionally problematic acts. Because the ultimate goal of this Article is to propose a path for the reasonable constitutional regulation of digital mass surveillance that departs as little as possible from existing Fourth Amendment doctrine, the Article assumes that this "principle of nonaggregation" will remain in place.

It might be objected at this point that the *frequency* of digital surveillance *should* make no difference whatsoever to the Fourth Amendment, because it does not matter to any individual's privacy.[61] If the quantity of information collected regarding any given individual remains low enough, why does it matter if that quantity is collected regarding a handful of individuals, or three

60 *See supra* text accompanying note 25.

61 Generally speaking, aggregative reasoning will often be a useful doctrinal tool when courts are attempting to address constitutional harms that have a cumulative nature, especially where the accumulation of harm results from an accumulation of government acts—as in both the cumulative harm to liberty of repeated acts of coercion during a street encounter, and the cumulative harm to privacy of prolonged surveillance. It will also be useful when courts are attempting to determine whether an act was justified, and the justification has a cumulative nature—as in the accumulation of suspicious acts that can together constitute reasonable suspicion or probable cause. It is often harder to see how increases in the *frequency* of surveillance have cumulative effects.

hundred million of them? In response to any of the ominous hypotheticals discussed above—the pervasive use of digital cameras, the collection of credit card records—it might be argued that either the practice, left unregulated, results in a constitutionally unacceptable quantity of surveillance of some individual, or it does not. In the former case, the practice should be constitutionally regulated, while in the latter case, it should not be. But in any case, the *number* of individuals affected makes no normative difference.

At least three objections might be offered to this line of argument. First, intuitively, it might be argued that the frequency of surveillance within a society can alter the effect of that surveillance on the character of the society, or the lives of those individuals living within it. It is one thing to know that an arbitrary but moderate intrusion on privacy may happen to a few unlucky individuals. It is another thing entirely to know that the same intrusion is happening to everyone, or everyone fitting some description. In the former case, most people may ignore the risk and continue to think and act as they wish, without fear of their acting and thinking being monitored and recorded for future, potentially adverse use. But to the extent that surveillance becomes more likely, individuals may become more cautious, self-censoring, and less free. The Fourth Amendment is concerned not only with individuals but with "[t]he right of *the people*"—collectively—to be secure from unreasonable search.[62] If changes in the frequency of a surveillance practice can alter the people's sense of security, then it seems unwise to dismiss the relevance of frequency to the Fourth Amendment out of hand.

Second, a sufficient increase in the frequency of moderately intrusive surveillance may in some circumstances result in a greater intrusion of the privacy of all or many of the individuals surveilled. Assume that the government collects information from a social media platform about the social network of one individual, and happens to have the same type of information about five of the individual's connections. The government may be able to draw certain inferences about the first individual based on the data from the five other individuals, and these inferences may represent a mild intrusion into the privacy of the first individual. Assume the quantity of the privacy intrusion is x, and that this quantity falls below the threshold necessary to constitute a Fourth Amendment search. By contrast, assume that the government collects information from the social media platform with

62 U.S. CONST. amend. IV (emphasis added); *see* Gray, *supra* note 26, at 97–103 (emphasizing the Fourth Amendment as a collective right).

a far greater frequency, such that the government possesses data about virtually all of the first individual's connections, and their connections, and their connections as well. It seems plausible that as a result of this greater frequency of surveillance, the government might be able to draw inferences about the first individual that represent a quantity of privacy intrusion far greater than *x*. Again, contrary to the objection offered above, a change in the frequency of surveillance seems to have resulted in an increased threat to the privacy values that the Fourth Amendment is supposed to protect.

Third, the two preceding points can intersect in the context of digital surveillance using "big data," machine learning, or other forms of artificial intelligence. The greater the frequency of surveillance, the larger the data set that the government can aggregate and then mine for predictive patterns. An increase in the *frequency* of surveillance may ultimately enable the government to make more privacy-invasive predictions about an individual than otherwise would have been possible based on a given *quantity* of information about the individual. A change in the frequency of surveillance, in other words, can bring about a change in the degree to which an individual's privacy has been invaded, even if the quantity of information the government has about that specific individual remains the same.[63]

Fortunately, Fourth Amendment doctrine has shown itself able to respond, albeit indirectly, to changes in the frequency of constitutionally problematic practices, despite the principle of nonaggregation. As Part II suggests, *Terry* can be understood as a response to a perceived rise in the frequency of stop-and-frisk. Part III.A argues that *Carpenter* similarly responds, in part, to a threatened rise in the frequency of location tracking using cell phones.

II. *TERRY* AS A RESPONSE TO MASS SEIZURE

A. Stop-and-Frisk in the Years Before Terry

Outside of legal circles, if *Terry v. Ohio* is known at all today, it is known by association with the racially unequal "stop-and-frisk" programs expanded

63 On the privacy-invasive potential of data-mining, big data, and machine-learning technology, see generally Slobogin, *Data Mining*, *supra* note 22; Aziz Z. Huq, *Racial Equity in Algorithmic Criminal Justice*, 68 DUKE L.J. 1043 (2019); Mariano-Florentino Cuéllar & Aziz Z. Huq, *Privacy's Political Economy and the State of Machine Learning: An Essay in Honor of Stephen J. Schulhofer*, 72 NYU ANN. SURV. AM. L. (forthcoming).

by urban police departments beginning in the 1990s.[64] A closer look at the historical background of *Terry* suggests a potential irony in this association. Despite the uses and abuses of *Terry* in the era of mass incarceration, the history behind *Terry* suggests that it was originally intended in part to foreclose the kind of large-scale, individually indiscriminate but racially discriminatory uses of stop-and-frisk with which the case later became associated. *Terry* attempted to prevent mass stops by requiring individualized, reasonable suspicion as a basis for any stop. It was intended as a reaction *against* the growing use of aggressive, indiscriminate stops by urban police departments in the 1960s, not as an authorization for such stops.

To begin with, the history of programmatic stop-and-frisk preceded *Terry* and was not created by it. As Tracey Meares has noted, the police chief of San Francisco, Thomas Cahill, deployed a program resembling systematic stop-and-frisk "in the 1950s, a full decade before *Terry* was decided."[65]

> Cahill launched "Operation S" on the streets of San Francisco. "S" stood for *saturation*, and the program called for flooding San Francisco's high crime areas with roughly fifty officers who stopped, questioned, frisked, and

---

64 *See generally* Floyd v. City of New York, 959 F. Supp. 2d 540 (S.D.N.Y. 2013) (holding that New York City's stop-and-frisk practices violated the Fourth and Fourteenth Amendments); MICHAEL D. WHITE & HENRY F. FRADELLA, STOP AND FRISK: THE USE AND ABUSE OF A CONTROVERSIAL POLICING TACTIC 2–6 (2016) (summarizing the rising use of stop-and-frisk and its racially unequal application). For an example of the popular conflation of *Terry* stops with the unconstitutional, programmatic abuse of stop-and-frisk, see Steven A. Holmes, *Reality Check: Who's Right About Constitutionality of Stop-and-Frisk?*, CNN (Oct. 1, 2016), https://www.cnn.com/2016/10/01/politics/fact-check-stop-and-frisk/index.html (clarifying the ambiguity that allowed Lester Holt and Hillary Clinton to claim, defensibly, during a 2016 presidential debate, that stop-and-frisk had been ruled unconstitutional in New York City, and former New York City Mayor Rudy Giuliani to claim, also defensibly, that stop-and-frisk had not been ruled unconstitutional).

For a sophisticated scholarly account that also treats *Terry* as "the foundation" for programmatic stop-and-frisk, rather than an attempt to limit its excesses, see Rachel A. Harmon & Andrew Manns, *Proactive Policing and the Legacy of* Terry, 15 OHIO ST. J. CRIM. L. 49, 49–50, 57–58 (2017) (presenting "proactive policing," which has "very often . . . in practice meant aggressively stopping and frisking individuals on the street," as "enabled by *Terry*," which "[o]ne might reasonably call . . . the foundation on which proactive policing is built," while also recognizing that programmatic stop-and-frisk "depart[s] from the kind of policing that the *Terry* decision described").

65 Meares, *supra* note 56, at 167; *cf.* Huq, *supra* note 56, at 2413 n.84 (2017) (citing Alex Elkins, *The Origins of Stop-and-Frisk*, JACOBIN (May 9, 2015), https://www.jacobinmag.com/2015/05/stop-and-frisk-dragnet-ferguson-baltimore) (noting that "[t]he earliest programmatic use of SQF I have been able to identify occurred in Cincinnati's Avondale neighborhood in 1958"). Meares also co-authored one of the few previous articles offering a sustained reflection on the similarities between mass digital search and the mass seizure of persons through stop-and-frisk. *See generally* Bernard E. Harcourt & Tracey L. Meares, *Randomization and the Fourth Amendment*, 78 U. CHI. L. REV. 809 (2011); *see also* Gray, *supra* note 26.

> arrested on vagrancy charges suspicious characters who police believed were about to break the law. In situations that did not result in arrest, police were instructed to fill out identification cards . . . . The number of stops that Operation S generated was prodigious for the times. Historian Robert Fogelson reported that, in its first year, Operation S tallied twenty thousand stops, most of which were of young black men.[66]

Similarly, the Kerner Commission, appointed by President Johnson in response to the summer 1967 riots in Newark and Detroit, singled out the excessive use of field interrogations as a source of police-community conflict, noting that field interrogations were "universally resented" by minorities.[67]

It is revealing that already in the early 1960s, "the police practice commonly and euphemistically referred to as 'stop and frisk' [was] a most popular topic in the law reviews, and was dealt with by a number of courts."[68]

---

66 Meares, *supra* note 56, at 167 (footnotes omitted) (citing ROBERT M. FOGELSON, BIG-CITY POLICE 187–88 (1977)).

67 SAMUEL WALKER, THE POLICE IN AMERICA: AN INTRODUCTION 21, 206 (1983) (quoting NAT'L ADVISORY COMM'N ON CIVIL DISORDERS, REPORT OF THE NATIONAL ADVISORY COMMISSION ON CIVIL DISORDERS (1968), *available at* https://www.ncjrs.gov/pdffiles1/Digitization/8073NCJRS.pdf [hereinafter "KERNER COMMISSION REPORT"]); Huq, *supra* note 56, at 2413. Of course, field interrogations were not the only cause of police-community tensions. Most of the race riots of the 1960s were sparked by a specific "incident involving the police," often "shootings of African American men by white police officers." SAMUEL WALKER, POPULAR JUSTICE: A HISTORY OF AMERICAN CRIMINAL JUSTICE 197 (2d ed. 1998). In testimony for the Kerner Commission, Kenneth Clark noted that a number of earlier commissions had identified similar police abuses as the causes of even earlier riots:

> I read the report of the 1919 riot in Chicago, and it is as if I were reading the report of the investigating committee on the Harlem riot of '35, the report of the investigating committee on the Harlem riot of '43, the report of the McCone Commission on the Watts riot [of 1965]. . . . [I]t is a kind of Alice in Wonderland—with the same moving picture reshown over and over again, the same analysis, the same recommendations, and the same inaction.

KERNER COMMISSION REPORT, *supra*, at 13.

68 4 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 9.1, (5th ed. 2012 & Supp. 2019) (footnotes omitted). The legal recognition of a category of detention short of arrest goes back to at least the seventeenth century, when English law recognized the right of night watchmen to temporarily detain suspicious persons. *See* Harmon & Manns, *supra* note 64, at 70 (citing 2 WILLIAM HAWKINS, A TREATISE OF PLEAS OF THE CROWN 128–29 (8th ed. 1824)); *see also* WHITE & FRADELLA, *supra* note 64, at 35–36 (citing 2 MATTHEW HALE, THE HISTORY OF THE PLEAS OF THE CROWN 96 (W. A. Stokes & E. Ingersoll eds., Robert H. Small 1847)); Richard M. Leagre, *The Fourth Amendment and the Law of Arrest*, 54 J. CRIM. L. CRIMINOLOGY & POLICE SCI. 393, 408–11 (1963). Harmon and Manns note that "[w]hen stops and frisks emerged as a more frequently used tactic in the late 19th Century, courts in New York and California debated whether the practice was permitted under pre-existing statutory authority," and "[t]o resolve the question, a number of states passed statutes authorizing—and limiting—stops and frisks." Harmon & Manns, *supra* note 64, at 70. Although the stop-and-frisk scholarship and case law in the early 1960s, like *Terry* itself, focused on individual rather than programmatic stop-and-frisk, the fact that legal

Stop-and-frisk was a growing practice, and a growing focus of concern, long before *Terry* "authorized" the practice under the Fourth Amendment.

The Supreme Court's decision in *Terry* itself suggests that it was self-consciously reacting against problematic aspects of the growing use of stop-and-frisk, rather than attempting to legalize the expansion of stop-and-frisk to a mass scale. The Court quotes another presidential commission that, like the Kerner Commission, found that "[i]n many communities, field interrogations are a major source of friction between the police and minority groups."[69] As the Court notes:

> It was reported that the friction caused by "[m]isuse of field interrogations" increases "as more police departments adopt 'aggressive patrol' in which officers are encouraged routinely to stop and question persons on the street who are unknown to them, who are suspicious, or whose purpose for being abroad is not readily evident." While the frequency with which "frisking" forms a part of field interrogation practice varies tremendously with the locale, the objective of the interrogation, and the particular officer, it cannot help but be a severely exacerbating factor in police-community tensions.[70]

It might also be noted that at a pivotal moment in the development and drafting of the *Terry* decision, when Justice Brennan delivered to Chief Justice Warren a proposed rewrite shifting the analysis from probable cause to reasonableness, Justice Brennan attached a cover letter noting:

> I've become acutely concerned that the mere fact of our affirmance in *Terry* will be taken by the police all over the country as our license to them to carry on, *indeed widely expand*, present "aggressive surveillance" techniques which the press tell us are being deliberately employed in Miami, Chicago, Detroit + other ghetto cities.[71]

---

attention to stop-and-frisk rose in the early 1960s suggests an awareness of the growing use of the tactic.

69 Terry v. Ohio, 392 U.S. 1, 14 n.11 (1968) (quoting PRESIDENT'S COMM'N ON LAW ENF'T & ADMIN. OF JUSTICE, TASK FORCE REPORT: THE POLICE 183 (1967)).

70 *Id.* (citations omitted) (quoting PRESIDENT'S COMM'N, *supra* note 69, at 184). The Court continues: "This is particularly true in situations where the 'stop and frisk' of youths or minority group members is 'motivated by the officers' perceived need to maintain the power image of the beat officer, an aim sometimes accomplished by humiliating anyone who attempts to undermine police control of the streets.'" *Id.* Meares notes that "while it is not clear whether the justices deciding *Terry* appreciated this fact, there is a great deal of evidence indicating that, at least in major cities, programmatic stop-and-frisk was regular police practice before *Terry* was decided." Meares, *supra* note 56, at 178. *Terry*'s reference to "more" police departments adopting "aggressive patrol" seems to suggest some awareness of a programmatic shift in tactics. *See Terry*, 392 U.S. at 14 n.11 (quotation marks omitted).

71 John Q. Barrett, *Deciding the Stop and Frisk Cases: A Look Inside the Supreme Court's Conference*, 72 ST. JOHN'S L. REV. 749, 825 (1998) (emphasis added) (quoting Letter from William J. Brennan, Jr.,

Many scholars have observed the difference between the "systematic," "programmatic," or "wholesale" use of stop-and-frisk by police departments, especially starting in the 1990s,[72] and the individualized, *ad hoc*, "retail" use of stop-and-frisk envisioned by the *Terry* court.[73] Meares distinguishes the programmatic use of stop-and-frisk from the kind of "one-off intervention into a crime in progress"[74] ostensibly carried out by Officer McFadden in *Terry* and apparently contemplated by the *Terry* court:

> In the program context, police on patrol looking to prevent crime do not seek out particular crimes in progress. Instead, they engage in assessments of suspicious characteristics—clothes that are out of season, suspicious bulges

---

Assoc. Justice, U.S. Supreme Court, to Earl Warren, Chief Justice, U.S. Supreme Court 2 (Mar. 14, 1968) (on file with the Library of Congress)); *see also id.* at 838 (noting that "Warren, the author of *Terry*, actually used much of an opinion that Justice Brennan, who is not identified as an opinion writer in the case, had ghost-written for Warren and persuaded him to use").

72 *See* Huq, *supra* note 56, at 2398; Meares, *supra* note 56, at 165. The programmatic use of stop-and-frisk in the 1990s has intellectual roots in a 1978 article by James Q. Wilson and Barbara Boland, and in a Kansas City policing experiment from the early 1990s that "seemed to confirm . . . Wilson's hypothesis." *See* Meares, *supra* note 56, at 167–69 (first citing James Q. Wilson & Barbara Boland, *The Effect of the Police on Crime*, 12 L. & SOC'Y REV. 367, 370 (1978); then citing Lawrence W. Sherman & Dennis P. Rogan, *Effects of Gun Seizures on Gun Violence: "Hot Spots" Patrol in Kansas City*, 12 JUST. Q. 673, 675–76 (1995)). Wilson famously went on to promote the theory of "broken windows" policing in a popular article, and also helped to popularize programmatic stop-and-frisk in the 1990s. *See* James Q. Wilson & George L. Kelling, *Broken Windows: The Police and Neighborhood Safety*, ATLANTIC (Mar. 1982), https://www.theatlantic.com/magazine/archive/1982/03/broken-windows/304465/; James Q. Wilson, *Just Take Away Their Guns*, N.Y. TIMES MAG. 47, Mar. 20, 1994.

73 *See* Jeffrey Fagan & Amanda Geller, *Following the Script: Narratives of Suspicion in* Terry *Stops in Street Policing*, 82 U. CHI. L. REV. 51, 61 (2015) ("Stop-and-frisk as envisioned by the *Terry* Court was largely a set of distinct 'retail' transactions, characterized by individualization, material or visual indicia, and specificity. But the current 'wholesale' practice is quite different from the vision of the *Terry* Court."); *see also* Huq, *supra* note 56, at 2402 (offering a critique of programmatic stop-and-frisk but noting "I have no cavil with the retail use of *Terry* stops as an element of nonprogrammatic street policing"). Judge Scheindlin made a similar point in one of the 2013 stop-and-frisk cases:

> Not only are the consequences of stops different today than they were in 1968, but the frequency of stops is far higher as well. As the stops have increased in frequency, they have also become more standardized and predictable. In *Terry*, the Supreme Court emphasized "the myriad daily situations in which policemen and citizens confront each other on the street." "No judicial opinion can comprehend the protean variety of the street encounter, and we can only judge the facts of the case before us." In the instant case, by contrast, the contested police encounters are strikingly uniform. The stops in the decline to prosecute forms echo the stops of plaintiffs, which in turn echo aspects of the training materials introduced at the hearing. *Terry* envisions street stops as uniquely tailored to unforeseen circumstances. The stops in the instant case are more like the products of fixed, repeatable processes.

Ligon v. City of New York, 925 F. Supp. 2d 478, 540–41 n.445 (S.D.N.Y. 2013) (internal citations omitted).

74 Meares, *supra* note 56, at 163.

> in clothing, furtive movements, age, gender, and so on. . . . [T]he officer [may] act simply on the basis of suspicious characteristics, making an assumption that anyone who looks a certain way is someone who *could* be a person about to engage in crime.[75]

In practice, it is probably inevitable that many of the stops resulting from such a program will lack the kind of individualized evidentiary basis that the *Terry* court attempted to require.[76] Yet in a perverse turn of history, police departments have routinely used *Terry* as a source of legal authority for such programs—arguably the kinds of programs of "aggressive patrol" that the Court intended *Terry* to curtail.[77]

It might be objected that this outcome illustrates the weakness of *Terry*'s approach to the Fourth Amendment, and perhaps suggests the wisdom of Justice Douglas's demand, in his dissent, that every seizure be supported by probable cause, even when the seizure does not rise to the level of a formal arrest.[78] But such an objection probably assumes an unrealistic view of the force of Supreme Court doctrine to resist the pressures of political change. If *Terry* eventually came to be used as an authorization for the very programs of widespread, non-individualized field interrogation that the decision was originally intended to constrain or prohibit, and if courts for the most part did nothing to correct the misunderstanding,[79] this outcome probably tells us less about the weakness of *Terry*'s doctrinal approach than it does about the general malleability of constitutional precedent, the inevitable role of politics in constitutional law, and the changing politics of crime, race, and civil liberties in the years after 1968. It is difficult to imagine any Fourth Amendment decision issued in 1968 providing an effective bulwark against the demands for aggressive, proactive policing during an era of rising violent crime that also happened to be dominated by a politics of racist backlash.[80]

---

75 *Id.*

76 This certainly seems to be what happened in New York. *See, e.g.*, Floyd v. City of New York, 959 F. Supp. 2d 540 (S.D.N.Y. 2013).

77 *See, e.g.*, *Ligon*, 925 F. Supp. 2d at 520.

78 *See Terry*, 392 U.S. at 35 (Douglas, J., dissenting); *see also* Paul Butler, *"A Long Step Down the Totalitarian Path": Justice Douglas's Great Dissent in* Terry v. Ohio, 79 MISS. L.J. 9 (2009).

79 *See* Barrett, *supra* note 71, at 827–28 n.465 (citing Adams v. Williams, 407 U.S. 143, 161–62 (1972) (Marshall, J., dissenting)) (describing how Justice Marshall came to regret his vote with the majority in *Terry*, praising the prescience of Justice Douglas's dissent); Carol S. Steiker, Terry *Unbound*, 82 MISS. L.J. 329, 332 (2013) (arguing that "a comparison of Warren's opinion for the Court in *Terry* with Rehnquist's opinions on later *Terry* issues reveals some crucial differences in emphasis").

80 *See generally* MICHELLE ALEXANDER, THE NEW JIM CROW: MASS INCARCERATION IN THE AGE OF COLORBLINDNESS (2010); WILLIAM J. STUNTZ, THE COLLAPSE OF AMERICAN CRIMINAL

In particular, one suspects that if Justice Douglas's proposal had been adopted in 1968, the result might have been a gradual redefinition over the following decades of "seizure" and "search" so that, for example, courts would eventually have held that the stops and frisks in the New York Police Department's ("NYPD") program in the early 2010s were in the vast majority of cases not so coercive as to justify Fourth Amendment protection. Perhaps the Supreme Court would have dismissed everything short of Officer McFadden's use of force as implicitly "consensual."[81] As Christopher Slobogin has noted, "[w]hen a search requires probable cause to be constitutional, courts are naturally more reluctant to denominate every police attempt to find evidence a search."[82]

In sum, the Supreme Court's decision in *Terry* to require that police officers have reasonable suspicion of a suspect's criminal activity before they

---

JUSTICE (2011). Indeed, temporary detentions based on less than probable cause were a routine police practice long before *Terry*, even when they were widely recognized as illegal under the common law of arrest. *See* SARAH A. SEO, POLICING THE OPEN ROAD: HOW CARS TRANSFORMED AMERICAN FREEDOM 148 (2019) (quoting a drafter of the Uniform Arrest Act stating that "the new laws 'would probably have no effect on police practices' because the police were already stopping and frisking notwithstanding their present illegality'"). To the extent that most police, most courts, and most of the public, or at least parts of the public with relevant legal influence and political power, believed that temporary detentions based on less than probable cause were an important and reasonable tool of policing, it seems almost inevitable that Fourth Amendment law would ultimately, one way or another, have accommodated the practice. *See id.* at 150 (noting that in the years leading up to *Terry*, "[s]ome reformers eventually came around to the view that only by legalizing brief seizures and frisks could the law at least regulate practices that were going to continue anyway"). Christopher Slobogin has described the tendency of an unyielding insistence on probable cause to lead to the exclusion of certain government actions from Fourth Amendment regulation altogether. *See generally* Christopher Slobogin, *The Liberal Assault on the Fourth Amendment*, 4 OHIO ST. J. CRIM. L. 603 (2007). Slobogin has been arguing against what he calls the "probable-cause-forever" approach to Fourth Amendment search doctrine, and in favor of what he calls "the proportionality principle," since the 1990s. *See, e.g.*, Christopher Slobogin, *The World Without A Fourth Amendment*, 39 UCLA L. REV. 1, 68 (1991).

81 On the fiction of "consent" in Fourth Amendment doctrine, see, for example, Tracey Maclin, *The Good and Bad News About Consent Searches in the Supreme Court*, 39 MCGEORGE L. REV. 27, 27–30 (2008) (noting the widely recognized "surreal quality about the Court's consent search jurisprudence"); Tracey Maclin, *"Black and Blue Encounters": Some Preliminary Thoughts About Fourth Amendment Seizures: Should Race Matter?*, 26 VAL. U. L. REV. 243, 249–50 (1991); *see also* David K. Kessler, *Free to Leave? An Empirical Look at the Fourth Amendment's Seizure Standard*, 99 J. CRIM. L. & CRIMINOLOGY 51, 53 (2009) (emphasis omitted) (empirically demonstrating that actual people would not "feel free to terminate simple encounters with law enforcement officers" in two situations that "are similar to situations in which the Court has held that people would feel free to leave").

82 Slobogin, *supra* note 80, at 605.

stop him,[83] and to have reasonable suspicion that the stopped person "may be armed and presently dangerous" before frisking him,[84] can be understood in part as a reflection of rising concerns in the late 1960s about the aggressive use of stop-and-frisk by police departments operating in minority communities.[85] *Terry* attempted to refashion Fourth Amendment doctrine to address the troubling rise in the number of stops and frisks, and the prospect of further rises to come.

---

83 In fact, *Terry* does not use the phrase "reasonable suspicion." The Court focused its holding primarily on the propriety of Officer McFadden's frisk, and even noted that "[w]e . . . decide nothing today concerning the constitutional propriety of an investigative 'seizure' upon less than probable cause for purposes of 'detention' and/or interrogation." *Terry*, 492 U.S. at 19 n.16; *see also id.* at 32–33 (Harlan, J., concurring) (noting a "logical corollar[y]" of the majority's decision "that I do not think the Court has fully expressed," namely that "the right to frisk in this case depends upon the reasonableness of a forcible stop to investigate a suspected crime"). But future case law referred back to *Terry*'s language regarding a police officer who "reasonably . . . conclude[s] . . . that criminal activity may be afoot" as a formulation of the reasonable suspicion standard. *Terry*, 492 U.S. at 30; *see, e.g.*, United States v. Sokolow, 490 U.S. 1, 7, 12 (1989) (characterizing *Terry* as holding that "the police can stop and briefly detain a person for investigative purposes if the officer has a reasonable suspicion supported by articulable facts that criminal activity 'may be afoot'"). *See generally* LAFAVE, *supra* note 68, § 9.5(b) (surveying the development of the "reasonable suspicion" standard).

84 *See Terry*, 492 U.S. at 30. For a more recent formulation, see Arizona v. Johnson, 555 U.S. 323, 326–27 (2009) ("[T]o proceed from a stop to a frisk, the police officer must reasonably suspect that the person stopped is armed and dangerous.").

85 *Terry* refers to "[t]he wholesale harassment by certain elements of the police community, of which minority groups, particularly Negroes, frequently complain." *Terry*, 392 U.S. at 14. As noted above, *Terry* also cited a presidential commission on the abuse of stop-and-frisk as a "major source of friction between the police and minority groups." *Id.* at 14 n.11. Carol Steiker notes that as Chief Justice Warren wrote "*Terry* in the flashpoint year of 1968, [he] was exquisitely sensitive to the issue of racial discrimination in law enforcement," and that Justice Brennan similarly expressed concern "[i]n his extensive correspondence with Warren over the drafting of *Terry*" about "unleashing police tactics that would 'aggravate the already white heat resentment of ghetto Negroes against the police.'" Steiker, *supra* note 79, at 349; *see also* Carol S. Steiker, *Second Thoughts About First Principles*, 107 HARV. L. REV. 820, 841 (1994) (arguing that the Warren Court's criminal procedure revolution, including its "focus on warrants, probable cause, and the exclusionary rule[,] was in some significant sense a response to the problems of racial discrimination that it . . . [was] forced to confront"). *But see* Barrett, *supra* note 71, at 772 (noting evidence "that the Court wanted the stop and frisk cases to be understood generally as police, but not as race, cases," including the fact that *Terry* does not mention any individual's race, thus leaving the reader unaware that it was "a case where a white police officer saw two young black men on a public street, thought they looked suspicious, kept watching them, followed them, and ultimately questioned and frisked them").

B. Police Bureaucratization and the Rise of Stop-and-Frisk

As noted in the introduction, Part III will explore certain similarities between *Terry*'s revision of existing seizure doctrine and *Carpenter*'s revision of existing search doctrine, as well as considering how *Carpenter* might be extended to address the challenges of digital mass surveillance. In order to understand the similarities between the two cases, it will be helpful to take a deeper look at the changing historical conditions that ultimately led to the concern about large-scale stop-and-frisk beginning in the early 1960s. The argument in Part III will be that an analogous transformation is currently taking place in the realm of digital surveillance.

The history of policing in the United States is in part a story of rising professionalization and bureaucratization.[86] The standard account begins by noting that throughout the Colonial Era and until the mid-nineteenth century, there were no uniformed police forces.[87] Instead, local communities tended to rely on three institutions whose origins lay in medieval England: a sheriff appointed at the county level, constables at the level of the town or city, and amateur watchmen who were drafted from the male citizenry and originally served mostly at night.[88] As the legal historian Lawrence Friedman has stated, criminal law enforcement in colonial times was "a business of amateurs."[89]

---

86 It might be argued that a tension exists between these two terms. To belong to a "profession" generally implies a certain autonomy and independence of judgment, while "bureaucrats," as discussed below, are sometimes conceived of as, ideally, interchangeable cogs. But the contrast probably means less in practice than in theory, given that most positions, whether viewed as bureaucratic or professional or some combination of the two, require a balance of discretion and rule-following. In any case, both terms contrast with the notion of the untrained amateur.

87 *See* Steiker, *Second Thoughts*, *supra* note 85, at 824 (describing "[t]he invention in the nineteenth century of armed, quasi-military, professional police forces, whose form, function, and daily presence differ dramatically from that of the colonial constabulary"). William Stuntz called the rise of police forces "the great story of *nineteenth*-century criminal justice." William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393, 434 (1995).

88 *See* WALKER, THE POLICE IN AMERICA, *supra* note 67, at 2–5; Steiker, *Second Thoughts*, *supra* note 85, at 830–32 (noting that the citizenry could also be called to assistance through the "hue and cry and the *posse comitatus*").

89 Steiker, *Second Thoughts*, *supra* note 85, at 830 (quoting LAWRENCE M. FRIEDMAN, CRIME AND PUNISHMENT IN AMERICAN HISTORY 27 (1993)); *see also* David Sklansky, *The Private Police*, 46 UCLA L. REV. 1165, 1193–1229 (1999) (emphasizing the extent to which those responsible for law enforcement in earlier eras of Anglo-American criminal law—especially the response to crime, as opposed to its prevention—were not merely amateurs, but private actors).

In response to the rioting and disorder that accompanied urbanization, industrialization, and immigration in the 1830s and 1840s, the amateur model of policing foundered.[90] Reformers looked to two models: slave patrols used in Southern communities to police the slave population, and the recently established London Metropolitan Police, created by then-Home Secretary Robert Peel in part based on the paramilitary "Peace Preservation Force" he had established in Ireland to control the restive population there.[91] Throughout the remainder of the nineteenth century, uniformed American police forces grew in size, and were increasingly expected to engage in investigation as well as peacekeeping; but they remained "completely unprofessional," corrupt, and inefficient.[92] Neighborhood politicians dispensed police jobs as a form of patronage, little training existed, brutality was rampant, and "police officers habitually evaded their responsibilities, spending much of their time in saloons and barbershops."[93]

---

90 *See* WALKER, THE POLICE IN AMERICA, *supra* note 67, at 6.

91 *Id.* at 3–4; John F. McEldowny, *Policing and the Administration of Justice in Nineteenth-Century Ireland*, *in* POLICING WESTERN EUROPE: POLITICS, PROFESSIONALISM, AND PUBLIC ORDER, 1850–1940, at 18–19 (Clive Emsley & Barbara Weinberger eds., 1991); James W. E. Sheptycki, *Police*, *in* ENCYCLOPEDIA OF LAW & SOCIETY: AMERICAN AND GLOBAL PERSPECTIVES (David S. Clark ed., 2007); *see also* STUNTZ, *supra* note 80, at 86 (noting that "urban police forces existed neither in eighteenth-century Britain—London's metropolitan police force was founded in 1829, thanks to then-Home Secretary Robert Peel (hence the name given London's officers: 'bobbies')—nor in the newly independent United States"); *id.* at 73 ("Local police forces arose in response to the first waves of European immigration in the 1840s and 1850s.").

An alternative, broader conception of "policing" had existed in continental Europe and especially Prussia and France, where Louis XIV first established a centralized office of police not only to regulate crime, but to administer all aspects of the health of the social body. *See* Sheptycki, *supra* (noting that the office of police was responsible for maintaining political order through spying, as well as "diverse matters including firefighting, sanitation, street lighting, relief of the poor, care of the sick, inspection of weights and measures, securing and distributing the food supply, licensing of news publications and manufacturing enterprises, and many other functions crucial to the maintenance of a healthy population"); *see also* BERNARD E. HARCOURT, THE ILLUSION OF FREE MARKETS 2–8 (2011) (describing the manifold functions of *ancien régime* French police). But this broader, continental model of policing may not have seemed a live option in the 1830s through the 1850s in the United States, because Anglo-American observers had long viewed the more expansive and intrusive regulatory police states of Prussia and then Austria and France with suspicion. *See* DAVID ALAN SKLANSKY, DEMOCRACY AND THE POLICE 16–17 (2008); WALKER, THE POLICE IN AMERICA, *supra* note 67, at 2. *But see* Steiker, *supra* note 85, at 831 (noting that constables and night watchmen had certain responsibilities outside of peacekeeping and investigating, including "announcing marriages").

92 *See* WALKER, THE POLICE IN AMERICA, *supra* note 67, at 7–10; Steiker, *supra* note 85, at 834.

93 WALKER, THE POLICE IN AMERICA, *supra* note 67, at 7–9; Steiker, *supra* note 85, at 834–35. In William Stuntz's revisionist account of the history of American crime and punishment, however,

Starting in the later nineteenth century, progressive reformers spearheaded a movement for police professionalism, sometimes arguing based on an analogy to the military that American police should be "engaged in a war on crime."[94] Progressive urban police chiefs such as August Vollmer attempted to centralize and reform police forces, narrow the police function, "protect the officers from political interference, keep them from temptation, place them under military discipline, and otherwise treat them like soldiers."[95]

A "second wave" of police professionalization began in the 1950s, this time led more by police administrators than by civic activists.[96] Against the conventional wisdom at the time that police could do little to prevent crime, and thus should focus above all on reacting effectively to crime when it occurred,[97] theorists of this second wave of professionalization such as

---

the "grubby, politicized institutions" of policing and prosecution "functioned reasonably well (outside the South—an important qualification)" before the mid-twentieth century. STUNTZ, *supra* note 80, at 68. Steiker summarizes policing in the South: "[D]uring Reconstruction . . . the new police in the South, and to a lesser degree in the North as well, treated blacks and black communities with extraordinary harshness, while often ignoring, and sometimes actively encouraging, illegal white-on-black violence." Steiker, *supra* note 85, at 839 (footnotes omitted).

94 FOGELSON, *supra* note 66, at 54; *see also id.* at 40–92 (recounting the rise of "the military analogy" in policing); WALKER, *supra* note 67, at 10; Steiker, *supra* note 85, at 836–37 ("[N]ineteenth-century police reformers turned to the military as a model for the organization of law enforcement."). By contrast, "[i]n the nineteenth century, the police had been distinctly unmilitaristic—sloppy, ill-disciplined, poorly managed." WALKER, THE POLICE IN AMERICA, *supra* note 67, at 12. *But see* Steiker, *supra* note 85, at 824, 833, 839 (suggesting that the uniformed, full-time "new police" that began to emerge after the 1830s were "quasi-military," with "their uniforms, arms, and military drilling" inspired by "the early nineteenth-century 'slave patrols' organized by many Southern cities"). It might be noted that the idea of the military as a paragon of discipline and efficient management is only somewhat older than the idea of uniformed, quasi-military police. *See, e.g.*, PAUL KENNEDY, THE RISE AND FALL OF THE GREAT POWERS 75 (1989) (describing the development of professional, bureaucratized standing armies in the eighteenth century). No one would have described the marauding, pillaging mercenaries of the Thirty Years' War, for example, as a model of rational organization. *See* MICHAEL HOWARD, WAR IN EUROPEAN HISTORY 37 (rev. ed. 2009). The story of modernity has been, in part, the story of a rising culture of discipline across various social contexts and institutions. *See generally* NORBERT ELIAS, THE CIVILIZING PROCESS (Eric Dunning et al. eds., Edmund Jephcott trans., rev. ed. 2000); MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON (Alan Sheridan trans., 1995) (1975); CHARLES TAYLOR, A SECULAR AGE (2007).

95 FOGELSON, *supra* note 66, at 75, 79, 84; WALKER, THE POLICE IN AMERICA, *supra* note 67, at 11.

96 FOGELSON, *supra* note 66, at 167–92; SKLANSKY, *supra* note 91, at 36.

97 *See* Huq, *supra* note 56, at 2413 n.84 (citing James J. Willis, *A Recent History of the Police*, *in* THE OXFORD HANDBOOK OF POLICE AND POLICING 3, 6–7 (Michael D. Reisig & Robert J. Kane eds., 2014); Lawrence W. Sherman, *The Rise of Evidence-Based Policing: Targeting, Testing, and Tracking*, 42 CRIME & JUST. 377, 378 (2013).

Vollmer's protégé O.W. Wilson "argued that police *could* deter criminal activity by increasing the likelihood that offenders would be caught or by reducing the opportunities for offenders to commit crime."[98] One tool of deterrent policing was to "seek out offenders rather than wait for victims to report crime," for example through "the systematic use of field interrogation."[99]

The second wave of police professionalization also overlapped with a number of broader historical shifts affecting policing and criminal justice. Because prosecutors and judges in the United States tend to be elected at the county level, the great migration of southern African Americans to northern cities and the parallel flight of white city-dwellers to the suburbs resulted in white suburban voters exercising increasing power over criminal justice in minority urban communities.[100] At the same time, the rate of violent crime exploded, with, for example, murder tripling between 1950 and 1972 in Chicago and quintupling in New York.[101] The Warren Court's criminal

---

98 Meares, *supra* note 56, at 166 (citing O.W. WILSON & ROY CLINTON MCLAREN, POLICE ADMINISTRATION 320–21 (4th ed. 1977)).

99 Meares, *supra* note 56, at 166, 166 n.42. As Harmon and Manns note, the idea of "police-initiated or 'proactive' policing" can be found in scholarship as early as the late 1960s, but "did not develop fully or spread widely in its contemporary form until the 1980s and 1990s, after a series of reports in the 1970s and early 1980s"—including the famous Kansas City Preventive Patrol Experiment in 1972–1973—"raised serious doubts about the effectiveness of the traditional patrol model." Harmon & Manns, *supra* note 64, at 55–56 (footnotes omitted); *see also* WALKER, THE POLICE IN AMERICA, *supra* note 67, at 23, 112–18. It is not entirely clear how to reconcile the apparent prevalence of large-scale stop-and-frisk in the early 1960s, as reflected in, for example, the Kerner Commission Report, discussed *supra* Part II.A, with the history of policing persuasively summarized by Harmon and Manns, according to which proactive policing did not develop as a theory until the late 1960s, and as a practice until the 1980s and 1990s. *Compare* Harmon & Manns, *supra* note 64, at 55–58, *with* Meares, *supra* note 56, at 178.

100 STUNTZ, *supra* note 80, at 7, 16, 35–36.

101 STUNTZ, *supra* note 80, at 5. Although not mentioned by Stuntz, one explanation of the sudden rise in violent crime during this period, and its equally sudden fall beginning in the 1990s, is that children who were exposed to rising levels of gasoline lead in the decades after World War II went on to commit more violent crime, while children who were exposed to less lead after its use declined beginning in the 1970s went on to commit less violent crime. *See* Kevin Drum, *Lead: America's Real Criminal Element*, MOTHER JONES (Feb. 2013), https://www.motherjones.com/environment/2016/02/lead-exposure-gasoline-crime-increase-children-health/ (summarizing the evidence for the lead-crime hypothesis, including one study that found "if you add a lag time of 23 years, lead emissions from automobiles explain 90 percent of the variation in violent crime in America"); Kevin Drum, *An Updated Lead-Crime Roundup for 2018*, MOTHER JONES (Feb. 1, 2018), https://www.motherjones.com/kevin-drum/2018/02/an-updated-lead-crime-roundup-for-2018/ (collecting studies since 2012, including natural experiments such as Stephen B. Billings & Kevin

procedure rulings in the 1960s created "new public expectations about police performance," just as the civil rights movement encouraged African Americans to be "less willing to suffer abuses at the hands of police."[102] "For many blacks, the cop on the street became the symbol . . . for a systematic pattern of racial discrimination in the United States."[103] When urban riots began breaking out in 1964, they were usually sparked by incidents involving the police.[104]

Meanwhile, the bureaucratization of police forces continued its decades-long march, driven forward by organizational ideas such as those contained in O.W. Wilson's "enormously influential" treatise *Police Administration*, first published in 1950, whose "precepts trained an entire generation of police officials."[105] The push toward bureaucratic efficiency was facilitated by technological changes in police work, especially the two-way radio, which had entered common use in the late 1930s and facilitated supervisors' ability to monitor whether patrol officers were in fact on duty, rather than shirking.[106]

Indeed, bureaucratization itself can be viewed as a kind of technological development. According to conventional theories of bureaucratization, a bureaucracy aims to standardize the behaviors of human beings so that their performance becomes as predictable, reliable, and adjustable as the behaviors of parts in a machine.[107] Like the parts in a machine, the workers in a bureaucracy are meant to be interchangeable with replacements.[108]

T. Schnepel, *Life After Lead: Effects of Early Interventions for Children Exposed to Lead*, 10 AM. ECON. J. 315 (2018)).

102 WALKER, THE POLICE IN AMERICA, *supra* note 67, at 19–20.

103 *Id.* at 20.

104 *Id.* at 20.

105 *Id.* at 14.

106 *See Id.* at 13–14. In addition, the increasing use of patrol cars reduced the amount of face-to-face contact between police and members of the community. "By the 1950s most departments converted exclusively to motorized patrol. Foot patrol remained common only in the densely populated cities of the Northeast." *Id.* at 13. To be clear, programmatic stop-and-frisk is compatible with the use of patrol cars. The police officer drives up to a pedestrian and then steps out of the vehicle to carry out the stop. *See, e.g.*, Floyd v. City of New York, 959 F. Supp. 2d 540, 628 (S.D.N.Y. 2013).

107 The general model of bureaucracy I have in mind is described in Gregory Brazeal, *Bureaucracy and the U.S. Response to Mass Atrocity*, 1 U. MIAMI NAT'L SEC. & ARMED CONFLICT L. REV. 57 (2010–2011) (drawing in particular on GRAHAM ALLISON & PHILIP ZELIKOW, ESSENCE OF DECISION: EXPLAINING THE CUBAN MISSILE CRISIS (2d ed. 1999)).

108 *See, e.g.*, JAMES F. RICHARDSON, URBAN POLICE IN THE UNITED STATES 121 (1974) (noting that "[b]ureaucrats can be considered as interchangeable parts who fill certain slots in an organizational chart").

That is, the outputs of any part of the bureaucratic machine should not depend on the variable, idiosyncratic, personal characteristics of the individual person who happens to be filling the role at any given time. Instead, the outputs are intended to be predictable based on the impersonal position that the worker fills in the bureaucracy—in other words, the person's "office" (hence "bureau-cracy," or "rule by offices"). The holder of each position is assigned to carry out various routine behaviors according to standard operating procedures, not entirely unlike the algorithms in a piece of software.

If we think of bureaucracies as similar to machines, then we can see the bureaucratization of police forces in the mid-twentieth century as similar in some ways to the introduction of a new technology to policing. Among other things, these new bureaucratic "machines" reduced the cost of implementing proactive policing policies, including the widespread use of stop-and-frisk. If the leaders of a police department decided that officers should try to deter, prevent, and detect crime by engaging in more frequent street stops, bureaucratic organization made it easier to carry out the new objective. The increased use of street stops could simply be introduced as an addition or adjustment to the standard operating procedures.[109]

The process of introduction might begin with the issuing and dissemination of orders and training, accompanied by incentives for those who increase their stop activity and disincentives for those who do not.[110] A bureaucratized police force will also likely have record-keeping systems in place that will facilitate monitoring how many stops and frisks officers are

---

109 As Judge Scheindlin suggested in the context of the NYPD's stop-and-frisk training:

> NYPD officers are trained to carry out their duties according to a set of standard operating procedures. The NYPD's training reduces the unpredictable, confusing challenges that arise on patrol to a manageable set of standard situations and orderly procedures for addressing them. . . . In this sense, the NYPD's training follows the model of a traditional Western military academy, which aims "to reduce the conduct of war to a set of rules and a system of procedures—and thereby to make orderly and rational what is essentially chaotic and instinctive."

Ligon v. City of New York, 925 F. Supp. 2d 478, 520–21 & n.305 (S.D.N.Y. 2013) (quoting JOHN KEEGAN, THE FACE OF BATTLE 18 (1976)).

110 *Cf.* Wilson & Boland, *supra* note 72, at 370–71 (noting that implementing a strategy of "aggressive patrol"—that is, "field interrogations or 'street stops'"—requires a police executive to "recruit certain kinds of officers, train them in certain ways, and devise requirements and reward systems (traffic ticket quotas, field interrogation obligations, promotional opportunities) to encourage them to follow the intended strategy," which Wilson notes "used to be . . . the core of the concept of 'police professionalism'").

carrying out. To the extent that the records are accurate, officers' knowledge that their stops are being monitored will provide a further incentive to comply with the directive to carry out more stops.[111]

It might have been assumed that the continuing bureaucratization of police forces in the 1950s and 1960s would lead to improved police-community relations. After all, if the police are doing their job more effectively, would it not follow that the community would benefit, and therefore be grateful? But the Kerner Commission, which found "deep hostility between police and the ghetto communities" to be a "primary cause" of the recent urban riots,[112] also found that "many of the serious disturbances took place in cities whose police are among the best led, best organized, best trained and most professional in the country."[113] How could it be that bureaucratization might lead to more, rather than less, conflict between the police and the community?

Once we recognize that bureaucratization facilitated the implementation of programmatic stop-and-frisk, the puzzle disappears. If the leaders of increasingly bureaucratized police forces used their enhanced control over police officers to expand the practice of proactive field interrogations and frisks, it is easy to see how bureaucratization and police-community conflict might be positively rather than negatively correlated.[114] To decide that one of the jobs of the police is to stop, question, and frisk suspicious characters on a large scale, in a social context where police officers often associate young black men with crime, risks suggesting, in effect, that the job of the police *is* race-based harassment.[115] The better the police do their job in such a setting, the more police-community hostility will likely result. To the extent that

---

111 For an example of a highly developed bureaucratic stop-and-frisk program, see *Floyd*, 959 F. Supp. 2d at 591–620 (describing the training, supervision, record-keeping, and incentives in the NYPD's stop-and-frisk program).

112 WALKER, THE POLICE IN AMERICA, *supra* note 67, at 21 (quoting KERNER COMMISSION REPORT, *supra* note 67).

113 *Id.*

114 *Cf. id.* (noting that "[a]ggressive patrol—a style of policing that resulted in frequent police-citizen contacts—appeared to be a problem" that contributed to community hostility toward many of "the best led, best organized" police forces).

115 *Cf. id.* ("A frequent complaint voiced by minority spokespersons is that the police harass minority citizens, especially young males. *Harassment* is usually defined as a greater tendency to stop, question, and frisk."); Steiker, *Second Thoughts*, *supra* note 85, at 840 (noting the "deeply entrenched . . . widespread use by police of race as a proxy for criminality," with the result that African Americans are "much more likely to be stopped, searched, and subjected to brutal treatment than similarly situated white people").

bureaucratization enhances the ability of a police force to do whatever task is assigned to it, bureaucratization would thus increase rather than reduce police-community hostility.

* * *

The historical background of *Terry* recounted above illustrates how Fourth Amendment doctrine can respond when a practice that has not previously been identified as unconstitutional, and that might once even have been seen as too marginal to merit constitutional scrutiny, increases in frequency in such a way that it threatens to interfere with a significant constitutional interest. Without rejecting the principle of nonaggregation and concluding that the increased frequency of the practice itself makes it unconstitutional, courts can respond to the novel constitutional threat by adjusting the doctrinal rules governing the practice. In particular, courts can attempt to reduce the frequency of the practice by imposing costly procedural burdens on it, and can attempt to reduce the threat that the practice poses to constitutional interests by restricting its use to circumstances where it is reasonably justified.[116]

Just as the bureaucratization of American policing had, by the early 1960s, reduced the difficulty of carrying out large-scale programs of stop-and-frisk, so in recent years the steadily falling costs and rising sophistication of digital technologies have facilitated the practice of mass surveillance.[117] Therefore, just as the increasing use of aggressive, large-scale stop-and-frisk called for a response from the Supreme Court in *Terry*, so today the increasing use of digital mass surveillance calls for the Supreme Court to

---

116 In fact, an increase in procedural burdens can by itself reduce the risk of unjustified police actions. *See* William J. Stuntz, Commentary, *O.J. Simpson, Bill Clinton, and the Transsubstantive Fourth Amendment*, 114 HARV. L. REV. 842, 848 (2001) (noting that because "[w]arrants raise the costs of searching," they "also raise the substantive standard applied to the search," because "[i]f an officer knows he must spend several hours on the warrant, he is likely not to ask for it unless he is pretty sure he will find the evidence").

117 For an attempt to quantify the relative costs of different methods of one form surveillance—location tracking—see Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of* United States v. Jones, 123 YALE L.J. ONLINE 335, 341–50 (2014). Drawing on Orin Kerr's "equilibrium-adjustment theory," Bankston and Soltani propose that Fourth Amendment doctrine should "impose new legal costs" whenever "a new surveillance technique" makes it "extremely inexpensive for the government to collect information that otherwise would have been impossible or prohibitively costly to obtain." *Id.* at 350–51; *see also* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011).

recognize the constitutional problems of digital mass search under the Fourth Amendment. Part III proposes a doctrinal path for doing so.

III. DIGITAL MASS SURVEILLANCE AFTER *CARPENTER*

A. Carpenter *as the* Terry *of Digital Search*

In 2018, the Supreme Court held in *Carpenter v. United States* that the Fourth Amendment generally requires the government to obtain a warrant based on probable cause in order to acquire seven days or more of a mobile phone number's historical CSLI from a third-party wireless carrier.[118] CSLI is generated "[e]ach time the phone connects to a cell site,"[119] and "[w]ireless carriers collect and store CSLI for their own business purposes."[120] The Court's opinion emphasizes that its holding is "narrow,"[121] and as phrased in the preceding sentences, the holding might seem to be a minor technical clarification. In fact, however, *Carpenter* is a momentous decision. It is the first time that the Supreme Court has recognized an exception to the third-party doctrine for digital data. It opens the door to further limitations on the third-party doctrine in contexts where consumers "share" digital data with third parties, as consumers routinely do whenever they carry a cell phone, send a text message or email, log into a Wi-Fi network, use a web browser, participate in social media, store data in the cloud, or use an app that collects data concerning location, health, or other arguably private matters.[122]

At first glance, *Carpenter* and *Terry* might seem to have very little in common other than being landmark Fourth Amendment decisions. *Carpenter* deals with what it presents as a deeply invasive form of search using a digital technology, while *Terry* deals with what it presents as a minimally invasive form of seizure (a "stop") and of search (a "frisk").[123] In terms of the ultimate values at stake in the Fourth Amendment, it might be argued that *Carpenter*, like many search cases, seems concerned above all with the protection of the

---

118 Carpenter v. United States, 138 S. Ct. 2206, 2214, 2217 n.3, 2220–21 (2018). The Court emphasizes that the holding in *Carpenter* addresses the acquisition of historical CSLI for individual phone numbers, not "real-time CSLI or 'tower dumps' (a download of information on all the devices that connected to a particular cell site during a particular interval)." *Id.* at 2220.

119 *Id.* at 2211.

120 *Id.* at 2212.

121 *Carpenter*, 138 S. Ct. at 2220.

122 *See supra* Part I.

123 *See Carpenter*, 138 S. Ct. 2206; Terry v. Ohio, 392 U.S. 1 (1968); discussion *supra* note 83.

"privacies of life,"[124] while the equivalent concern of *Terry*, as in many cases regarding the seizure of persons, might be seen as the protection of "the right to be let alone."[125]

In fact, if *Carpenter* and *Terry* are to be juxtaposed at all, it might seem that they should be placed in contrast. *Terry* created a two-tiered system for the constitutional review of the seizure of persons, with the lower tier ("stops") requiring only reasonable suspicion, and the upper tier ("arrests") requiring probable cause.[126] By contrast, *Carpenter* follows the standard rule for searches and requires the government to obtain a warrant based on probable cause in order to access historical CSLI records extending over a week or more.[127] The decision implicitly rejects the constitutional sufficiency of the statutory scheme for obtaining CSLI records under the Stored Communications Act ("SCA"), a scheme that requires something resembling reasonable suspicion and that may in fact have been influenced by *Terry*.[128]

---

124 *Carpenter*, 138 S. Ct. at 2214 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)); *see also* Riley v. California, 573 U.S 373, 403 (2014) (quoting *Boyd*, 116 U.S. at 630) (noting that modern cell phones contain "the privacies of life").

125 It is appropriate that Justice Douglas would have imposed a probable cause requirement even for street stops, *see Terry*, 392 U.S. at 35 (Douglas, J., dissenting), given his belief that "[t]he right to be let alone is . . . the beginning of all freedom." Pub. Utilities Comm'n v. Pollak, 343 U.S. 451, 467 (1952) (Douglas, J., dissenting); *cf.* Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) (referring to "the right to be let alone" as "the most comprehensive of rights, and the right most valued by civilized men"), *overruled by* Berger v. New York, 388 U.S. 41 (1967), *and* Katz v. United States, 389 U.S. 347 (1967); Warren & Brandeis, *supra* note 59, at 195 (quoting THOMAS M. COOLEY, A TREATISE OF THE LAW OF TORTS 29 (2d ed. 1888)) (referring to "the right 'to be let alone'").

126 *See Terry*, 392 U.S. at 27. In 1979, the Supreme Court summarized what remains the prevailing view of *Terry*:

> *Terry* departed from traditional Fourth Amendment analysis in two respects. First, it defined a special category of Fourth Amendment "seizures" so substantially less intrusive than arrests that the general rule requiring probable cause to make Fourth Amendment "seizures" reasonable could be replaced by a balancing test. Second, the application of this balancing test led the Court to approve this narrowly defined less intrusive seizure on grounds less rigorous than probable cause, but only for the purpose of a pat-down for weapons.

Dunaway v. New York, 442 U.S. 200, 209–10 (1979).

127 *Carpenter*, 138 S. Ct. at 2221.

128 The SCA states that in order for the government to obtain "a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)," the government must first obtain a court order ("D order") based on "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(c)(1) & (d) (2012); United States v. Perrine, 518 F.3d 1196, 1202 (10th Cir. 2008) (stating that the SCA's "'specific and articulable facts' standard derives from the Supreme Court's

But closer inspection reveals similarities between the ways that *Terry* and *Carpenter* altered the landscape of previously existing Fourth Amendment doctrine, and the Court's motivations for doing so. As Part II argued, the increasing bureaucratization of police forces in the United States in the decades leading up to *Terry* facilitated the carrying out of street stops and frisks on a mass scale, which in turn created a threat to Fourth Amendment interests that would not have existed if street stops had been carried out exclusively on an *ad hoc*, infrequent basis.[129] The Court in *Terry* responded by recognizing street stops as seizures that would be subject to Fourth Amendment reasonableness review.[130] By transforming mass stops into mass

---

decision in *Terry*"); *see also Carpenter*, 138 S. Ct. at 2212 (discussing prosecutors' use of the SCA to acquire Timothy Carpenter's CSLI). *But see* Caminker, *supra* note 12, at 466–67 (noting that "the SCA's 'reasonable grounds to believe . . . relevant' standard" may be "somewhat less stringent than the more commonplace 'reasonable suspicion' standard").

129 *See supra* Part II.

130 *See supra* note 83. To be clear, although the Supreme Court passed through a number of sometimes unclear positions on its way to the final decision in *Terry*, *see generally* Barrett, *supra* note 71, it would be inaccurate to suggest that *Terry extended* new Fourth Amendment protections to an area of police activity that had been previously assumed to lie *outside* the scope of the Fourth Amendment. Non-lawyers might not have understood that even a temporary detention by the police constituted a seizure under the common-law understanding of arrest. *See* United States v. Bonanno, 180 F. Supp. 71, 78 (S.D.N.Y. 1960) ("A layman, if asked if he had even been arrested, would not be likely to describe situations where he had been stopped by a police officer, or situations where his car had been stopped, or even situations where his questioning had been continued at a police station, as arrests."); SEO, *supra* note 80, at 146–47, 308 n.68 (citing *Bonanno*, 180 F. Supp. 71). But in the years leading up to *Terry*, it seems to have been generally assumed by courts, commentators, and legal practitioners that temporary detentions fell within the definition of seizure under the Fourth Amendment. *See* LAFAVE, *supra* note 68, § 9.1 nn.3–4 (collecting scholarship and cases in the years leading up to *Terry*); SEO, *supra* note 80, at 142–55 (discussing police practices leading up to *Terry*). *But see* SEO, *supra* note 80, at 151 (suggesting that at least one presidential commission in the mid-1960s feared the Warren Court might prohibit temporary detention, interrogations, and frisking without probable cause altogether). The primary question was how to categorize such seizures in relation to existing doctrine, and whether such seizures must be based on probable cause, or something less—the latter possibility having been suggested by a number of statutes, judicial opinions, and scholarly articles before *Terry*. *See, e.g.*, Sibron v. New York, 392 U.S. 40, 43–44 (1968) (quoting reasonable suspicion standard for temporary, investigative detention in N.Y. CODE CRIM. PROC. § 180); WHITE & FRADELLA, *supra* note 64, at 36–38 (discussing wide variety in arrest practices in lead-up to Uniform Arrest Act). *See generally* LAFAVE, *supra* note 68, § 9.1 nn.3–4 (collecting scholarship and cases dealing with the application of the Fourth Amendment to seizures before *Terry*). Even the pro-government amicus briefs submitted in *Terry* conceded that a limited, investigatory detention must be reasonable under the Fourth Amendment. *See, e.g.*, Brief of the United States as Amicus Curiae at 5, *Terry*, 392 U.S. 1 (No. 67) (arguing that during a "limited detention in the course of a police investigation," "[t]he Fourth Amendment does apply, to be sure, insofar as it guarantees the right of the people to be secure from unreasonable search and seizure of any kind").

seizures, the Court brought under Fourth Amendment judicial scrutiny a growing practice that intuitively seemed to impinge on Fourth Amendment interests such as privacy and "the right to be let alone," but that prior to *Terry* had never been addressed by the Court as a potential Fourth Amendment violation.[131]

Similarly, the Court's decision in *Carpenter* arose against a backdrop of extralegal change in which the reduced cost of digital surveillance, such as through the acquisition of third-party CSLI, resulted in the increased use of such surveillance by law enforcement, and the increased use in turn seemed to create a new threat to core Fourth Amendment privacy interests. Chief Justice Roberts' opinion explicitly presents the decision in part as a response to the falling costs and rising ease of surveillance using digital technologies. At the outset of a survey of the dangers to privacy posed by CSLI, the Court notes that "cell phone location information is . . . effortlessly compiled."[132] Quoting Justice Alito's concurrence in *United States v. Jones*, the Court emphasizes the relatively lower cost of digital as opposed to earlier forms of surveillance:

> Prior to the digital age, law enforcement might have pursued a suspect for a brief stretch, but doing so "for any extended period of time was difficult and costly and therefore rarely undertaken." For that reason, "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."[133]

In addition, and in line with this Article's concerns regarding digital *mass* surveillance, the majority opinion in *Carpenter* gives weight to the fact that CSLI could be used to track "everyone" in the United States who carries a cell phone: "Critically, because location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone."[134] It is a critical part of the Court's reasoning that the digital surveillance technology at issue in the case has the

---

131 *See* LAFAVE, *supra* note 68, § 9.1 n.5 (noting that the Supreme Court had previously avoided confronting the status of temporary investigative detentions under the Fourth Amendment in *Rios v. United States*, 364 U.S. 253 (1960), and *Henry v. United States*, 361 U.S. 98 (1959)).

132 *Carpenter*, 138 S. Ct. at 2216.

133 *Id.* at 2217 (internal citations omitted) (quoting United States v. Jones, 565 U.S. 400 (2012) (Alito, J., concurring)).

134 *Id.* at 2218.

capacity to be used for mass surveillance, or at least for government "fishing expeditions through databases," in the words of a recent scholarly analysis of *Carpenter*.[135] The Court again highlights the significance of the risk of digital mass surveillance when it notes that "[t]he Government's position fails to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter's location *but also everyone else's*."[136]

In place of Justice Jackson's invocation of an individual "Everyman" who is threatened with arbitrary search in the absence of Fourth Amendment protections,[137] Chief Justice Roberts repeatedly invokes a mass "everyone" who could now be subjected to systematic, comprehensive surveillance in the absence of such protections. Responding to Chief Justice Roberts' language, and the Court's stated wish in *Carpenter* "to place obstacles in the way of a too permeating police surveillance,"[138] one scholar notes:

> Concerns over frequency do not typically play a role in determining whether an investigatory method constitutes an atomistically intrusive search. But, in the end, I suspect such concerns are driving much of the distinction here between high- and low-tech surveillance methods for those justices who worry that the former "may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'"[139]

In other words, *Carpenter* appears to be concerned with the likelihood that the lower cost of digital surveillance might increase not only the quantity of surveillance directed at a targeted individual such as Timothy Carpenter, but also the frequency of surveillance in the sense of the number of people subject

---

135 Freiwald & Smith, *supra* note 39, at 220. Incidentally, another possible analogy between *Carpenter* and *Terry* is that critics of the decisions can point to a certain distance between the facts in the judicial record and the facts addressed by the Court. *Compare* KERR, *supra* note 22, (describing how the *Carpenter* Court's presentation of technological threats goes beyond, and even misrepresents, the record concerning the CSLI collected in *Carpenter*), *with* Lewis R. Katz, Terry v. Ohio *at Thirty-Five: A Revisionist View*, 74 MISS. L.J. 423, 430–32 (2004) (emphasis added) (citations omitted) (noting that Officer McFadden began observing the two black men in *Terry* simply because "*they didn't look right to me at the time*," noting that McFadden's initial memory of the men's subsequent suspicious behavior was that they looked in a shop window "about three times each," and noting that McFadden later revised his estimate upward to perhaps five times each, but that Chief Justice Warren's *Terry* opinion states the men "pace[d] alternately along an identical route, pausing to stare in the same store window roughly *twenty-four times*").

136 *Carpenter*, 138 S. Ct. at 2219 (emphasis added).

137 Brinegar v. United States, 338 U.S. 160, 181 (1949) (Jackson, J., dissenting) ("So a search against Brinegar's car must be regarded as a search of the car of Everyman.").

138 *Carpenter*, 138 S. Ct. at 2214 (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

139 Caminker, *supra* note 12, at 457 (quoting United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring)).

to it. The specter of digital mass surveillance casts a shadow over *Carpenter*,[140] not unlike the shadow cast over *Terry* by the perceived threat of the widespread, expanding use of stop-and-frisk.[141]

Again, as we saw in Part II, *Terry* responded to the actual and potential increase in the frequency of street stops by defining the legal quality of those stops so as to bring them within the definition of "seizure" under the Fourth Amendment, thereby transforming the political problem of mass stops into the constitutional problem of mass seizures. *Carpenter* carries out a similar transformation. It responds to the actual and potential increase in the frequency of CSLI surveillance by altering the legal quality of CSLI surveillance to bring it within the definition of "search" under the Fourth Amendment, thereby transforming the political problem of digital mass surveillance, at least in the context of CSLI, into the constitutional problem of mass search.[142]

In both cases, existing doctrine had failed to bring a government practice within the scope of judicial scrutiny under the Fourth Amendment, despite the growing threat that the practice seemed to pose to the underlying values of the Fourth Amendment. In both cases, the Court addressed the arguable misalignment of doctrine and principle by clarifying how the problematic practice fell within the scope of a Fourth Amendment category ("seizure" and "search," respectively).

---

140 "One can almost hear a background whisper of 'Big Brother' throughout the analysis." *Id.*

141 *See supra* Part II.

142 If we look back even further, another parallel might be found in *Carroll v. United States*, 267 U.S. 132 (1925), the Supreme Court's first case on car searches. SEO, *supra* note 80, at 116. Although *Carroll* is primarily known as the origin of the "automobile exception" in Fourth Amendment doctrine, it also laid the foundation for *Terry* by turning from a categorical analysis of criminal procedure under the Fourth Amendment to an analysis based on reasonableness. *See id.* at 138, 141. Just as *Terry* involved a type of police encounter that was coercive, but not as coercive as a traditional arrest, and that seemed both practically necessary and impossible to carry out based on a requirement of probable cause; so *Carroll* involved a type of police encounter—the stopping and searching of a car for contraband—that was intrusive on privacy, but not as intrusive as a traditional search of a home, and that seemed both practically necessary (to the enforcement of prohibition) and impossible to carry out based on a warrant requirement. *See id.* at 141–42, 148, 151. Just as the *Terry* Court felt compelled to reach a decision in part based on the threatened proliferation of suspicionless stop-and-frisk, so the *Carroll* court felt compelled to reach a decision in part based on the threatened proliferation of suspicionless vehicle stops: "It would be intolerable and unreasonable if a prohibition agent were authorized to stop every automobile on the chance of finding liquor, and thus subject all persons lawfully using the highways to the inconvenience and indignity of such a search." *Carroll*, 267 U.S. at 153–54.

B. Reasonable Suspicion for Digital Search After Carpenter

Despite the underlying similarities between *Carpenter* and *Terry* described above, however, *Carpenter* departs from *Terry* in following the standard Fourth Amendment rule and requiring a warrant backed by probable cause in order for the government to carry out a search by collecting seven days or more of CSLI.[143] This approach has puzzled some scholarly observers.[144] After all, the Court in *Carpenter* had a very *Terry*-like doctrinal option ready at hand, a compromise between the absence of Fourth Amendment regulation and requiring a warrant backed by probable cause. It could have shown deference to Congress and required something like the SCA's "specific and articulable facts"[145] requirement for the production of CSLI, a standard that bears some similarity to, although it may be somewhat weaker than, the "reasonable suspicion" standard for *Terry* stops.[146] Alternatively, the Court could have remanded the case to the district court to consider an appropriate evidentiary standard. Instead, without any explanation, the Court announced that CSLI records require a warrant,[147] and ended the potential common-law-constitutional conversation before it could begin.

At the same time, the Court in *Carpenter* did not close the door to the use of a reasonable suspicion standard in the context of digital surveillance, or even in the context of CSLI. Indeed, the Court arguably left a conspicuous door open to the development of such a rule. In a footnote, the majority opinion states:

> [W]e need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be. It is

143 *Carpenter*, 138 S. Ct. at 2217 n.3, 2221.

144 *See, e.g.*, Caminker, *supra* note 12, at 463–67 (noting that "the *Carpenter* Court wasted no words—literally zero—rejecting" the possibility of a mid-level reasonableness standard such as "reasonable suspicion"); Alan Z. Rozenshtein, *Fourth Amendment Reasonableness After* Carpenter, 128 YALE L.J. FORUM 943, 946 (2019).

145 *See supra* note 39.

146 *See id.*

147 *Carpenter*, 138 S. Ct. at 2221 ("Before compelling a wireless carrier to turn over a subscriber's CSLI, the Government's obligation is a familiar one—get a warrant."). The phrasing echoes Chief Justice Roberts' opinion for the Court in *Riley v. California*, 573 U.S. 373, 403 (2014) ("Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.").

> sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.[148]

Justice Kennedy's dissent suggests that the Court is creating a bright line such that at day seven, a "constitutional framework" enters into action.[149] But the majority's footnote rejects any implication that *Carpenter* holds the Fourth Amendment does *not* apply to historical CSLI records lasting shorter than seven days. Of course, the majority also does not hold that the Fourth Amendment *does* apply. It would be logically consistent for a future court to hold that accessing historical CSLI records lasting less than seven days is not a Fourth Amendment search and is subject to no constitutional constraints.

After *Carpenter* has gone to such lengths to emphasize the gravity of the invasion of privacy resulting from seven days or more of CSLI records, however, it would seem more consistent for a future court to hold that accessing CSLI records of less than seven days intrudes sufficiently upon the Fourth Amendment interest in privacy to constitute a Fourth Amendment search, but one requiring reasonable suspicion that the records will reveal evidence of a crime, rather than probable cause.[150] Requiring reasonable suspicion to access short-term CSLI records, rather than allowing unfettered government discretion or requiring a warrant, would have the added benefit of bringing these lesser privacy intrusions more closely into alignment with Congress's "specific and articulable facts" evidentiary standard under the SCA.[151]

In fact, future courts might interpret *Carpenter* as inviting the development of a more general two-tiered system of Fourth Amendment standards for digital search. Such an approach would be consistent not only with *Carpenter* itself, but with the Supreme Court's general application of mosaic theory in

---

148 *Carpenter*, 138 S. Ct. at 2217 n.3.

149 *Cf. id.* at 2233 (Kennedy, J., dissenting).

150 On the other hand, a case could be made for treating the collection of CSLI records extending over a sufficiently brief period—say, an hour, or several hours—as not constituting a Fourth Amendment search at all. This would allow law enforcement agents to perform "tower dumps," that is, "a download of information on all the devices that connected to a particular cell site during a particular interval." *Carpenter*, 138 S. Ct. at 2220, 2233. Because short-duration tower dumps can be very useful in criminal investigations, and collect relatively little private information about any individual, it seems unlikely that courts would adopt an approach to the Fourth Amendment that effectively prohibits them.

151 *See* discussion *supra* note 128.

digital search cases.[152] The Court appears increasingly willing to recognize the common-sense proposition that the threat to Fourth Amendment privacy interests posed by the government obtaining digital data depends in part on the quantity of potentially intimate data it obtains.

Once the legitimacy of applying the aggregative reasoning of the mosaic theory to digital search is accepted, it follows naturally that more than one tier of scrutiny might be appropriate for the review of digital searches. With regard not only to the collection of CSLI but to any number of methods of obtaining privacy-intrusive digital data, it is reasonable to distinguish between the acquisition of a lesser quantity of data that would likely result in lesser privacy harms and for which a lesser evidentiary standard might be appropriate, and a greater acquisition likely resulting in greater privacy harms and for which a greater evidentiary standard should be required.[153]

---

152 *See infra* Part IV; *Carpenter*, 138 S. Ct. at 2215 (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring); *id.* at 430 (Alito, J., concurring)) ("[Five] concurring Justices [in *Jones*] concluded that 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy'—regardless whether those movements were disclosed to the public at large."). Although *Riley* dealt with the constitutionality of a search incident to arrest, rather than with the definition of a search, its treatment of the privacy interest in the digital data stored on a cellphone echoes the quantity-focused definition of digital search in the *Jones* concurrences and in *Carpenter*. *See Riley*, 573 U.S. at 393 (drawing legal significance from the fact that "[c]ell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person").

153 It might be objected that the Supreme Court foreclosed the use of a two-tiered, *Terry*-like approach to search in *Arizona v. Hicks*, where the Court held that a police officer conducted a search in violation of the Fourth Amendment when he moved a turntable to read its serial number based on a reasonable suspicion that the turntable was stolen, but without probable cause. 480 U.S. 321, 323, 326–27 (1987); *see also id.* at 333, 338 (O'Connor, J., dissenting) (citing *Terry*, 392 U.S. at 24–25) (arguing that "the balance of the governmental and privacy interests strongly supports a reasonable-suspicion standard for the cursory examination of items in plain view"). But *Hicks* was narrowly addressing the logic of the "plain view" doctrine, an exception to the warrant requirement. *Id.* at 325–27. The decision is driven by a concern to keep the plain view exception within tight limits, to ensure "that 'the "plain view" doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges.'" *Id.* at 328 (quoting Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971)). Just because the Supreme Court wanted to keep the plain view exception within tight limits does not imply that the Court has foreclosed the possibility of a two-tiered approach to search in all contexts.

In fact, *Hicks* suggests that unless there is a reason to distinguish the two, the degree of justification required for a search should generally be the same as the degree of justification required for a seizure. *See id.* at 328 ("[N]either [a search] nor [a seizure] is of inferior worth or necessarily requires only lesser protection. We have not elsewhere drawn a categorical distinction between the two insofar as concerns the degree of justification needed to establish the reasonableness of police action . . . ."). In light of this baseline, the fact that the Court has already recognized two tiers of

If CSLI can reveal a person's "familial, political, professional, religious, and sexual associations" by "follow[ing] its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales,"[154] a list of a person's email or social media contacts could surely do the same. The records of a person's website visits, especially if they revealed search terms entered on websites, could reveal even more intimate details. With regard to each of these forms of digital metadata, the aggregative reasoning underlying the mosaic theory would be consistent with drawing some temporal or other quantitative line above which probable cause would be required, but below which the government could obtain records based only on reasonable suspicion.

For example, the Fourth Amendment could be interpreted to allow the government to obtain up to a day's, or a week's, worth of a person's browsing history from an Internet service provider based on a reasonable suspicion that the records would reveal evidence of a crime.[155] Access beyond that temporal line, wherever it is drawn, would require probable cause. On the one hand, requiring probable cause to obtain a brief period of records could make it too difficult, if not practically impossible, to investigate certain crimes, such as child pornography and online terrorist recruiting.[156] On the other hand, interpreting the Fourth Amendment to allow the government

---

justification in the context of seizure argues in favor of recognizing two tiers in the context of search. It might also be noted that the Court has already applied a "reasonable suspicion" test to a search for criminal evidence in at least one context, *see* United States v. Knights, 534 U.S. 112, 121 (2001) (searching a probationer's home), and has recognized that digital technology sometimes creates unique threats to privacy that require departing from traditional Fourth Amendment search doctrine. *See Riley*, 573 U.S. at 386; *Carpenter*, 138 S. Ct. at 2222 ("When confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents."). For further discussion of the Supreme Court's "special needs" cases, see Part III.C below.

154 *Carpenter*, 138 S. Ct. at 2217–18 (Sotomayor, J., concurring) (quoting United States v. Jones, 565 U.S. 400, 415 (2012)).

155 The precise temporal line would of course be a matter for debate based on differing estimations of the importance of privacy and law enforcement needs. The point of this Section's argument is not to determine the appropriate boundary lines between the two tiers of Fourth Amendment scrutiny for digital search, but rather to suggest that the aggregative reasoning at work in the mosaic theory fits comfortably with a two-tiered approach.

156 *See* Caminker, *supra* note 12, at 440–41 & n.165 ("Requiring a warrant for short-term CSLI monitoring might hinder criminal investigations much more severely than requiring a warrant only for long-term monitoring.").

entirely unfettered discretion to collect even brief periods of such potentially private records would needlessly weaken constitutional privacy protections.

Similar reasoning could potentially be applied to any category of digital data that the government might seek to obtain from a third party in the course of a criminal investigation. Accessing some types of data that are especially likely to reveal private information, such as the contents of files stored in the cloud, might be held always to require a warrant, regardless of the quantity of information obtained—as is currently the case for the contents of emails.[157] But for digital data that is relatively less likely to reveal intimacies when accessed in very limited quantities, like location data from a cell phone or vehicle, web browsing histories, digital communications metadata, or metadata from smart-home devices, a two-tiered approach based on reasonableness could provide the optimal balance between the protection of privacy and the practical needs of law enforcement investigations.

The third-party doctrine itself would pose no hurdle to a two-tiered approach to Fourth Amendment digital search doctrine. With regard to any category of digital data held by a third party, courts could evaluate whether the person who transmitted the data to the third party meaningfully chose to do so.[158] Where she did not, the Court could follow *Carpenter* and "decline to extend" the third-party doctrine to the category of digital data in question.[159]

---

157 *See supra* note 39 (discussing *Ex parte Jackson* and *Warshak*'s protection of the contents of communications).

158 *Cf. Carpenter*, 138 S. Ct. at 2220 (quoting Smith v. Maryland, 442 U.S. 735, 745 (1979)) ("[I]n no meaningful sense does the user [of a cell phone] voluntarily 'assume[ ] the risk' of turning over a comprehensive dossier of his physical movements."). If a court were interested in protecting the privacy of some type of digital data, it is hard to imagine many contexts in which this line of reasoning could not be applied.

159 *Carpenter*, 138 S. Ct. at 2217. Now that *Carpenter* has introduced the possibility of cabining the reach of the third-party doctrine with regard to digital data, future courts might also consider limiting the reach of *Miller* and *Smith* even with regard to financial and phone call records, the respective subject matters of those cases. *See* United States v. Miller, 425 U.S. 435 (1976); *Smith*, 442 U.S. 735. Kerr has proposed that the reasoning of *Carpenter* should lead to the conclusion that the collection of email metadata constitutes a search, but the collection of telephone metadata does not, because "[t]he digital age has not substantially changed [the] nature" of the latter. *See* KERR, *supra* note 22. In terms of the underlying interests protected by the Fourth Amendment, however, it is difficult to see why a distinction should be drawn between the bulk collection of phone records using digital technology and the bulk collection of email records using the same. An alternative approach would be to take even more seriously *Carpenter*'s emphasis on the difference that digital technology can make, and to conclude that when the government acquires phone call and financial records *using digital technology*, the third-party doctrine does not apply. Of course, the government could in theory

The collection of such data, perhaps beyond some *de minimis* amount, would then constitute a search, and would be subject to either the warrant or the two-tiered reasonableness requirement discussed above.

Establishing a two-tiered system of Fourth Amendment standards for digital search would bring digital search doctrine in line with the doctrine governing the seizure of persons since *Terry*. Indeed, the case for a two-tiered digital search doctrine is arguably even stronger than the case for a two-tiered doctrine governing the seizure of persons. The burdens to law enforcement of requiring probable cause every time the government seeks to obtain digital data from third parties are obvious and significant.[160] The risks to privacy of allowing the government unfettered discretion under the Fourth Amendment to access digital data held by third parties, even if the contents of communications are excluded, are equally obvious and significant.[161]

More importantly, while it is perhaps possible to imagine a counterfactual history in which Justice Douglas's dissenting position in *Terry* prevailed, and the Supreme Court required probable cause even for temporary detentions,[162] such an outcome is simply not plausible in the context of digital search. There is no realistic scenario in which courts in the United States will abruptly reverse position and decide that all of our intuitively private digital information held by third parties, such as web browsing histories, phone and text message metadata, and location data collected by smartphone apps, can only be obtained by the government through warrants backed by probable cause, even if this means that a variety of serious crimes can no longer be effectively investigated and prosecuted. The realistic choice, as suggested in the Introduction,[163] is between subjecting such government data collection to judicial scrutiny based on a standard less than

---

evade this requirement by collecting massive quantities of printed records and then scanning them into a searchable format. But in light of the cost and inconvenience, it seems unlikely that the government would choose to do so, especially if it could obtain the records digitally based on a showing of reasonableness under the Fourth Amendment.

160 *See* Bambauer, *supra* note 33, at 215 ("Most scholars know that recognizing access to third-party records as a full-fledged search requiring a warrant and probable cause is an unworkable solution [because] . . . keeping every last third-party record off limits until the case progresses to probable cause would unacceptably frustrate investigations.").

161 *See, e.g.*, Donohue, *supra* note 22, at 884 (discussing the consequences of bulk metadata collection by the government).

162 *See supra* text accompanying notes 78–80 (discussing Justice Douglas's position and its likely consequences).

163 *See supra* Introduction.

probable cause, or not subjecting such collection to judicial scrutiny under the Fourth Amendment at all.

All of the preceding analysis, like *Carpenter* and most Fourth Amendment case law, applies to government requests for digital data in the course of investigations involving specific, targeted individuals suspected of crimes. But as noted in the Introduction, the ultimate aim of this Article is to arrive at a plausible Fourth Amendment doctrine for governing the digital surveillance of large populations. What relevance might a two-tiered Fourth Amendment doctrine for digital search have for digital *mass* surveillance?

C. A Lidster *for Digital Mass Search?*

Let us assume that there are at least some contexts in which courts might wish, or might even feel compelled, to uphold the constitutionality of the bulk collection of Americans' intuitively private digital records, whether held by third parties or not. The Introduction proposed a hypothetical scenario involving a surveillance program that a court perceives as vital to public safety, but that happens to collect a large number of Americans' private digital records without any basis in individualized reasonable suspicion.[164]

It is worth noting at the outset that if the surveillance program had focused on *foreign* intelligence, and had only incidentally collected Americans' data, then it is possible that a court could have upheld the program by carving out an exception to the Fourth Amendment for surveillance programs whose primary purpose is foreign intelligence. Although the law is unsettled on this point, the Supreme Court in *Carpenter* gestured toward the possibility of special rules governing the application of the Fourth Amendment to the products of foreign intelligence surveillance, or perhaps even programs related to national security in general.[165] A future court may

---

164 *See supra* Introduction.

165 "[O]ur opinion does not consider other collection techniques involving foreign affairs or national security." *Carpenter*, 138 S. Ct. at 2220; *see also* United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 308 (1972) (reserving judgment "on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country"). Laura Donohue notes that the Foreign Intelligence Surveillance Court of Review ("FISCR") recently "asserted, for the first time, a foreign intelligence surveillance exception to the Fourth Amendment," and that the government has since cited the FISCR's opinion in a white paper as support for "an exception to the Fourth Amendment warrant requirement." DONOHUE, *supra* note 52, at 146 (emphasis omitted) (discussing *In re* Directives [REDACTED] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1009–10 (FISA Ct. Rev. 2008)). Donohue, like Solove and others,

determine that national security is a "special need," distinct from ordinary criminal law enforcement, and that courts should develop different Fourth Amendment rules to govern surveillance programs whose primary purpose is national security, just as courts have developed different Fourth Amendment rules to govern safety inspections of homes,[166] administrative inspections of businesses,[167] the searching and drug testing of students,[168] border searches,[169] and so on.[170] In these "special needs" cases, the Supreme Court has carried out a *Terry*-like balancing of all the relevant interests to determine "the reasonableness, under all the circumstances, of the search."[171]

---

generally favors a distinction between a set of surveillance rules for ordinary criminal law enforcement purposes and a set of less restrictive rules for foreign intelligence, espionage, or national security purposes—combined with vigilance toward limiting the ever-expanding reach of "national security" as a category. *See id.* at 145–46, 150–54, 159; SOLOVE, *supra* note 4, at 62–80.

The aim in this Section is to offer a way to uphold a reasonable digital mass surveillance program—if such a thing can exist—without distorting the protections provided by the Fourth Amendment more generally, even where the primary purpose of the program is *not* the protection of national security. For this Article's purposes, it is not necessary to resolve the normative question of whether a digital mass surveillance program ever could be reasonable, in the sense of satisfying some all-things-considered balancing test or proportionality analysis. The point is that if a court is already inclined to uphold such a program, it would be better for civil liberties, *all other things being equal*, for the court to do so through a *Lidster*-like analysis than through holding that the surveillance in question did not constitute a Fourth Amendment search at all, because the latter approach would allow the police and other state actors to collect the type of digital information at issue in all contexts, even where it would not be reasonable to do so.

166 *See* Camara v. Mun. Court, 387 U.S. 523, 538 (1967) (requiring a search warrant for home safety inspections, in the absence of exigency or consent, but requiring only that the warrant be based on "reasonable legislative or administrative standards for conducting an area inspection . . . with respect to a particular dwelling," rather than probable cause).

167 *See* United States v. Biswell, 406 U.S. 311, 316 (1972) (upholding warrantless inspection of a heavily regulated business); See v. City of Seattle, 387 U.S. 541, 542 (1967) (applying *Camara* analysis to inspections of commercial structures).

168 *See* Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 665 (1995) (upholding suspicionless drug-testing of high school student athletes "in furtherance of the government's responsibilities, under a public school system, as guardian and tutor of children entrusted to its care"); New Jersey v. T.L.O., 469 U.S. 325, 340–42 (1985) (upholding warrantless search of a student's handbag based on reasonable suspicion that it contained cigarettes and the special need of maintaining school discipline).

169 *See* United States v. Montoya de Hernandez, 473 U.S. 531, 538, 541 (1985) (requiring only reasonable suspicion of smuggling contraband for "the detention of a traveler at the border, beyond the scope of a routine customs search and inspection," and reaffirming that routine border searches "are not subject to any requirement of reasonable suspicion, probable cause, or warrant").

170 For a summary of the Supreme Court's "special needs" cases, and analysis of their lack of clarity, see Slobogin, *supra* note 21, at 1726–33 (noting that the Court's "focus on whether evidence of ordinary criminal wrongdoing is the goal leaves much to be desired").

171 *T.L.O.*, 469 U.S. at 341.

But let us focus here on the hardest case: a domestic digital mass surveillance program that a court (rightly or wrongly) believes to be vital to public safety, that involves the suspicionless collection of intuitively private digital information, and that is focused on collecting evidence for ordinary criminal law enforcement purposes. Let us assume that the court is unwilling to finesse the issue by holding that the purpose of the program is not *really* criminal law enforcement, but rather some more general, non-punitive, safety-related goal.[172] Is there a way for the court to hold the *program* constitutional under the Fourth Amendment without also holding that the government has unfettered discretion *outside of the program* to conduct the type of surveillance carried out in the program? In other words, is there a way to quarantine the court's upholding of the constitutionality of the collection of private information in the program so as not to contaminate or distort the meaning of the Fourth Amendment in general? Can a precedent be found in Fourth Amendment law for allowing suspicionless searches within some program while continuing to require a higher evidentiary standard for searches outside of the program?

Once again, a solution can be found by turning from the law of search to the law of seizure. As one treatise notes:

> The Court has permitted searches on less than probable cause in only three circumstances: 1) a search for weapons and dangerous people, not evidence, made for purposes of self-protection (*Terry*); 2) a search for evidence, where there are special needs beyond mere law enforcement; and 3) in certain circumstances, a search of a probationer's residence (*Knights*).[173]

None of these exceptions apply to our hypothetical program of domestic digital mass surveillance, assuming (again) that the court is unwilling to obscure the program's actual law enforcement purposes. Thus, there appears to be no precedent under Fourth Amendment search law for upholding the program. A court that is strongly predisposed to uphold the

---

172 The Court in *Edmond* claimed that "each of the checkpoint programs that we have approved was designed primarily to serve purposes closely related to the problems of policing the border or the necessity of ensuring roadway safety," and that "the constitutional defect of the program [in *Edmond*] is that its primary purpose is to advance the general interest in crime control." City of Indianapolis v. Edmond, 531 U.S. 32, 41, 44 n.1 (2000); *cf. id.* at 50 & n.2 (Rehnquist, J., dissenting) (noting that it is "not at all obvious" "that the checkpoints at issue in *Martinez-Fuerte* and *Sitz* were not primarily related to criminal law enforcement").

173 STEPHEN A. SALTZBURG ET AL., BASIC CRIMINAL PROCEDURE 242 (7th ed. 2017).

program may, as a result, hold that the collection of private data in the program is not a search governed by the Fourth Amendment at all.

But once we turn to the Fourth Amendment law of seizure, a precedent exists that will allow the court to uphold the program in question without removing the type of surveillance at issue from all Fourth Amendment regulation by concluding it does not constitute a search. In *Illinois v. Lidster*, the Supreme Court upheld a highway checkpoint that had ordinary criminal investigation as its purpose.[174] In *Lidster*, "an unknown motorist traveling eastbound on a highway in Lombard, Illinois, struck and killed a 70-year-old bicyclist."[175] "About one week later at about the same time of night and at about the same place, local police set up a highway checkpoint designed to obtain more information about the accident from the motoring public."[176] The police conducted brief stops "*not* to determine whether a vehicle's occupants were committing a crime, but to ask vehicle occupants, as members of the public, for their help in providing information about a crime in all likelihood committed by others."[177] The Court acknowledged that the vehicle stops constituted seizures under the Fourth Amendment,[178] and that the seizures were not based on "individualized suspicion,"[179] but nevertheless held the checkpoint program constitutionally reasonable under the Fourth Amendment, based on the balancing of "'the gravity of the public concerns served by the seizure, the degree to which the seizure advances the public interest, and the severity of the interference with individual liberty.'"[180]

It might seem dangerous to raise the possibility of adapting the reasoning of *Lidster* to a digital mass surveillance program. After all, *Lidster* upholds the constitutionality of mass, suspicionless intrusions on Fourth Amendment privacy.[181] But if we begin from the premise that a court is inclined to uphold

174 540 U.S. 419, 427–28 (2004).

175 *Id.* at 422.

176 *Id.*

177 *Id.* at 423.

178 *Id.* at 425–26.

179 *Id.* at 424–25.

180 *Id.* at 427 (quoting Brown v. Texas, 443 U.S. 47, 51 (1979)).

181 There is a troubling asymmetry in the Supreme Court's use of programmatic review in Fourth Amendment "special needs" cases, and in *Lidster*. The Court is willing to step back from an individual government act that would be unconstitutional if viewed as an individual transaction, under ordinary Fourth Amendment doctrine, and uphold the act as part of a program if the program overall is constitutionally reasonable, under a "special needs" analysis. But the Court is apparently unwilling, ever, to step back from an individual government act that would be

a digital mass surveillance program because the court finds it reasonable, then the *Lidster* approach may be the best way of limiting the damage—or preventing any damage, depending on one's perspective. The Court in *Lidster* could have concluded that the stops in question were too brief and uncoercive to be seizures, or could have adopted a fiction whereby the stops were not seizures at all because they were in fact consensual encounters. Similarly, a court confronted with a Fourth Amendment challenge to one of the many digital mass surveillance programs that the U.S. government may be carrying out at the moment, with largely unknown effects on Americans' privacy,[182] could follow the lead of the FISC in *In re F.B.I.* and conclude that the type of surveillance at issue in the program does not constitute a Fourth Amendment search.[183] The effect of such an approach in *Lidster* would have been to free the police to set up similar vehicle checkpoints at any time and place across the country, and to allow the police to conduct brief, ostensibly uncoercive stops there without any basis at all, immune from any judicial scrutiny under the Fourth Amendment. The police could have begun establishing these checkpoints throughout the country, or—even more troublingly—at the boundaries of every "high crime area." Similarly, the effect of such an approach in a digital mass surveillance case would be to free the government to conduct a type of digital surveillance with unfettered discretion. Not only could the government collect the information at issue through bulk collection, but local police could collect it about any person that happens to provoke their suspicion.

In both contexts, civil liberties are far better protected by allowing the program of searches or seizures lacking individualized suspicion to proceed, if a court finds the program constitutionally reasonable, while continuing to recognize that the searches or seizures *are* searches or seizures, and require evidentiary justification outside the special context of the program.

Again, it may be that no program of domestic digital mass searches for ordinary law enforcement purposes should ever be held constitutionally reasonable under the Fourth Amendment. Perhaps any threats serious

---

constitutional if viewed as an individual transaction, under ordinary Fourth Amendment doctrine, and strike down the act as part of a program if the program overall is constitutionally unreasonable. If the latter form of analysis existed in Fourth Amendment law, it would allow courts to address the problematic implications of vast increases in frequency more directly—rather than having to accommodate concerns about frequency indirectly, as the Court arguably did in *Terry* and *Carpenter*.

182 *See* Slobogin, *Policing, Databases, and Surveillance*, *supra* note 22, at 76–78.

183 *See In re* F.B.I., No. BR 13-109, 2013 WL 5741573, at *5, *9 (FISA Ct. Aug. 29, 2013).

enough to justify suspicionless digital searches should be identified as "special needs" and therefore distinguished from ordinary law enforcement. Indeed, if the hypothetical digital mass surveillance program we have been considering has as its primary purpose the identification of criminals *from among the subjects of its digital searches*, then it is distinguishable from the program in *Lidster*, where "[t]he police expected the information elicited to help them apprehend, not the vehicle's occupants"—that is, the subjects of the privacy intrusion—"but other individuals."[184]

But there is another type of digital mass surveillance program that would be more closely analogous to the checkpoint in *Lidster*. As Caminker notes, "proactive efforts to identify and thwart potential acts of terrorism require lots of background location and movement data from which computer algorithms can predict conventional behavior in order to discern unconventional and perhaps threatening aberrations."[185] If a generally privacy-protective judge were confronted with a challenge to a program of suspicionless digital mass searches that collected intuitively private information, but only as "background data," and did so in what the judge believed to be a constitutionally reasonable manner under the Fourth Amendment, then *Lidster*'s approach would provide a quite analogous precedent allowing the judge to uphold the program without distorting the Fourth Amendment generally to accommodate the suspicionless searches in the program.

An added benefit of the programmatic review of digital mass surveillance programs, based on *Lidster* or another "special needs" approach, is that such review could provide a basis for ordering injunctive relief including not only the termination of digital mass surveillance programs, but also more finely tuned remedies aimed at ensuring the reasonableness of the programs going forward. Remedial orders could be a vehicle for implementing various sensible proposals that currently have no foothold in Fourth Amendment doctrine. To take one example, scholars who criticize current Fourth Amendment digital search doctrine have sometimes suggested that the Fourth Amendment should be interpreted to regulate not only the collection of private digital data, but the querying (or other use) of such data.[186]

184 540 U.S. at 423.

185 Caminker, *supra* note 12, at 465–66.

186 *See, e.g.*, Berman, *supra* note 30, at 578–79; Donohue, *supra* note 21, at 558; Krent, *supra* note 52, at 53.

Currently, Fourth Amendment doctrine imposes no regulations on the government's use of data once it has collected it.[187] But even if courts continue to refuse to recognize any restrictions on querying under the Fourth Amendment, query restrictions could conceivably play a role in an equitable remedy regarding a digital mass surveillance program that is constitutionally unreasonable as currently constituted.

A number of scholars have noted that changes in technology argue in favor of applying the more flexible tools of administrative law to the regulation of digital surveillance, as opposed to relying exclusively on the slow-moving and informationally limited process of constitutional adjudication.[188] A remedial order directed at bringing a program of digital mass surveillance into line with the Fourth Amendment requirement of reasonableness could conceivably involve the establishment of institutions and procedures familiar from administrative law, perhaps even including the requirement that a municipal police department follow a notice-and-comment procedure before deploying or expanding the use of a digital surveillance technology.[189]

IV. THE MOSAIC THEORY OF SEIZURE

This final Part addresses a possible objection to the two-tiered approach to digital search, and in doing so, draws attention to a way in which the Supreme Court in its recent digital search jurisprudence has already moved toward bringing digital-search doctrine more closely in line with seizure doctrine, as this Article proposes.

It might be argued, against the two-tiered approach to digital search, that there is a natural distinction between a stop and an arrest that justifies *Terry*'s distinction between the reasonable suspicion required for the former and the probable cause required for the latter, while there is no natural dividing line

---

187 *See* Berman, *supra* note 30, at 578.

188 *See* Daphna Renan, *The Fourth Amendment as Administrative Governance*, 68 STAN. L. REV. 1039, 1043–49 & nn.24–25, 29 (2016) (collecting citations).

189 *Cf.* Barry Friedman & Maria Ponomarenko, *Democratic Policing*, 90 N.Y.U. L. REV. 1827, 1834 (2015) (proposing that "administrative notice-and-comment rulemaking, in which public participation is welcomed" could provide "democratic authorization" for policing practices); Floyd v. City of New York, 959 F. Supp. 2d 668, 671–72 (S.D.N.Y. 2013) (ordering broad equitable relief, including "Joint Remedial Process for Developing Supplemental Reforms" with a "community input component").

in digital search that could justify a similar distinction. Thus, the critique would suggest, requiring reasonable suspicion for some digital searches and probable cause for others would be inevitably arbitrary and unjustifiable in a way that has no precedent even in the law of seizure.

In fact, a similar critique has already been offered of the Supreme Court's recent decisions in *Jones* and *Carpenter*, where the Court implicitly endorsed a "mosaic theory" of digital search.[190] According to this theory, the line between a digital search and a non-search may in some contexts be based on how much data the government collects about an individual.[191] David Gray and Danielle Citron have written that "[a]ccording to critics and supporters alike, this quantitative account of Fourth Amendment privacy is revolutionary."[192]

This Part will argue, by contrast, that the mosaic theory may not be as revolutionary of a development in Fourth Amendment doctrine as it seems. In fact, for decades before the Court began drawing lines between digital searches and non-searches based on the mosaic theory, courts used a functionally identical form of aggregative reasoning to draw the line between a seizure of a person and a non-seizure. The application of the mosaic theory to digital search can thus be seen as an example of the Court applying doctrinal structures from the Fourth Amendment law governing the seizure of persons to contemporary problems in Fourth Amendment digital search. In other words, the mosaic theory shows that the Supreme Court has already taken a first step on the general methodological path that this Article recommends.

What is the mosaic theory of digital search, and how is it similar to decades-old doctrines governing the seizure of persons?

Orin Kerr's "The Mosaic Theory of the Fourth Amendment" is probably the most frequently cited work of scholarship on the mosaic theory of search,

---

190 *See* United States v. Jones, 565 U.S. 400 (2012); Carpenter v. United States, 138 S. Ct. 2206 (2018); Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313 (2012) (noting that "concurring opinions signed or joined by five of the justices" in *Jones* "endorsed some form of the . . . mosaic theory"); Orin S. Kerr, *When Does a* Carpenter *Search Start—And When Does It Stop?*, VOLOKH CONSPIRACY (July 6, 2018, 3:34 PM), https://reason.com/2018/07/06/when-does-a-carpenter-search-start-and-w/ ("*Carpenter* seems to have adopted the basic mosaic approach of the *Jones* concurrences."). *But cf.* KERR, *supra* note 22, at 39 (arguing that "*Carpenter* leaves the future of the mosaic theory open").

191 *See supra* note 190.

192 Gray & Citron, *supra* note 21, at 68.

and is one of the foundational scholarly works focusing on aggregation as a central issue in the judicial response to digital surveillance under the Fourth Amendment.[193] Kerr's article begins with an analysis of the reasoning in *United States v. Maynard*,[194] the D.C. Circuit case that became the Supreme Court case *United States v. Jones*.[195] In *Maynard*, the D.C. Circuit held that a GPS tracking device attached to a vehicle twenty-four hours a day for twenty-eight days constituted a Fourth Amendment "search," even though the monitoring of a "single journey" would not have been.[196] Writing for the court, Judge Douglas Ginsburg distinguished the Supreme Court's 1983 decision in *United States v. Knotts*,

> in which the Supreme Court held the use of a beeper device to aid in tracking a suspect to his drug lab was not a search . . . . [because] "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[197]

Judge Ginsburg reasoned that "unlike one's movements during a single journey, the whole of one's movements over the course of a month" is neither actually nor constructively "exposed to the public because the likelihood anyone will observe all those movements is effectively nil," and because "that whole reveals more—sometimes a great deal more—than does the sum of its parts."[198] As in a mosaic, the whole may present a picture that the individual

---

193 *See* Kerr, *The Mosaic Theory of the Fourth Amendment*, *supra* note 190.

194 United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 565 U.S. 400 (2012).

195 United States v. Jones, 565 U.S. 400 (2012), *aff'g sub nom. Maynard*, 615 F.3d 544.

196 *Maynard*, 615 F.3d at 555, 565.

197 *Id.* at 555–56 (quoting United States v. Knotts, 460 U.S. 276, 281 (1983)). Judge Ginsburg also writes:

> [I]n *Knotts* the Court . . . reserved the issue of prolonged surveillance. That issue is squarely presented in this case. Here the police used the GPS device not to track Jones's "movements from one place to another," *Knotts*, 460 U.S. at 281, but rather to track Jones's movements 24 hours a day for 28 days as he moved among scores of places, thereby discovering the totality and pattern of his movements from place to place to place.

Id. at 558.

198 *Id.* at 558. Judge Ginsburg also used the term "mosaic theory" in his opinion in *Maynard*, writing:

> As with the "mosaic theory" often invoked by the Government in cases involving national security information, "What may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene." Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation.

Id. at 562 (internal citation omitted). On the mosaic theory in Freedom of Information Act (FOIA) national security law, see generally David E. Pozen, *The Mosaic Theory, National Security, and the Freedom of Information Act*, 115 YALE L.J. 628 (2005).

pieces of the mosaic would not reveal if someone viewed each of the individual pieces in isolation. The difference between surveillance of an individual trip and "prolonged" surveillance "is not one of degree but of kind, for no single journey reveals the habits and patterns that mark the distinction between a day in the life and a way of life."[199]

In other words, quantity can pass over into quality: a sufficient quantity of surveillance can change the legal quality of that surveillance from a non-search to a search under the Fourth Amendment. The result is achieved through aggregation. By choosing to analyze the twenty-eight days of surveillance in the aggregate, the D.C. Circuit arrived at a different conclusion than it would have reached under *Knotts* if it had treated each of the surveilled trips during the twenty-eight days as an individual, isolated act. Aggregation has apparently transformed a series of non-searches into a single, continuous search extending over nearly a month.

After the Supreme Court upheld the outcome of *Maynard* in *United States v. Jones*,[200] Kerr noted that "concurring opinions signed or joined by five of the justices [in *Jones*] endorsed some form of the D.C. Circuit's mosaic theory."[201] He went on to present the mosaic theory as "a major departure from the traditional mode of Fourth Amendment analysis," precisely because of its use of aggregation:

> The current structure of Fourth Amendment doctrine hinges on what I call a "sequential approach." The sequential approach takes a snapshot of each discrete step and assesses whether that discrete step at that discrete time constitutes a search. This analytical method forms the foundation of existing Fourth Amendment doctrine, ranging from the threshold question of what the Fourth Amendment regulates to considerations of constitutional reasonableness and remedies. By aggregating conduct rather than looking to discrete steps, the mosaic theory offers a fundamental challenge to current Fourth Amendment law.[202]

In stark contrast to the sequential approach, the mosaic theory asks "whether a series of acts that are not searches in isolation amount to a search

---

199 *Maynard*, 615 F.3d at 562.

200 565 U.S. 400 (2012).

201 Kerr, *The Mosaic Theory of the Fourth Amendment*, *supra* note 190, at 313. *Accord* Carpenter v. United States, 138 S. Ct. 2206, 2215 (2018) (internal citation omitted) (noting that, in *Jones*, "the concurring Justices concluded that 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy'—regardless whether those movements were disclosed to the public at large").

202 Kerr, *The Mosaic Theory of the Fourth Amendment*, *supra* note 190, at 314.

when considered as a group."[203] "The mosaic theory is therefore premised on aggregation: it considers whether a set of nonsearches aggregated together amount to a search because their collection and subsequent analysis creates a revealing mosaic."[204] Kerr contrasts this aggregative analysis with the traditional, sequential approach in which, he says, the "existence and duration" of a search or seizure "are clear as they occur . . . and do not require the ex post aggregation and analysis of non-searches."[205] As an example of the sequential approach, Kerr summarizes the analysis in *Terry*:

> If an officer sees suspects preparing for a robbery, stops them, and pats them down for weapons, the court will consider the viewing, the stopping, and the patting down as distinct acts that must be analyzed separately. Each step counts as its own Fourth Amendment event and is evaluated *independently* of the others.[206]

Kerr's presentation of the mosaic theory as a controversial departure from traditional Fourth Amendment analysis has been influential, even among those who, unlike him, believe that the use of the mosaic theory is a good idea.[207] But is there in fact such a categorical distinction between the kind of analysis that appears in *Terry* and the kind that appears in "mosaic theory" decisions such as *Maynard* and, arguably, *Carpenter*?[208]

Kerr's argument seems to assume that there is a natural way of drawing the spatio-temporal lines around certain "acts," at least for Fourth

---

203 *Id.* at 320.

204 *Id.* at 320.

205 *Id.* at 318 n.41.

206 *Id.* at 316 (emphasis added) (citing Terry v. Ohio, 392 U.S. 1, 18 n.15, 27–30 (1968)). Kerr also writes "[T]he issue of what counts as a seizure is comparatively simple, and it therefore has received little scholarly attention. Seizures require governmental assertion of control, so a seizure of property occurs when the government meaningfully interferes with a person's possessory interest." *Id.* at 312 n.2 (citing United States v. Jacobsen, 466 U.S. 109, 113 (1984)).

207 *See* Gray & Citron, *supra* note 21, at 68 (citing Kerr, *infra*); Kerr, *The Mosaic Theory of the Fourth Amendment*, *supra* note 190, at 343–53 (criticizing the mosaic theory). It is difficult to avoid the sense that hostility to the mosaic theory has something to do with a more general preference for bright-line, formalistic rules as opposed to less mechanically applicable standards. Fittingly, Justice Scalia, a devotee of rules over standards, tended like Kerr to emphasize an approach to the definition of search based on clear, synchronic, spatially defined boundaries, as when he wrote in *Kyllo v. United States*: "The Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained." 533 U.S. 27, 37 (2001); *cf.* Antonin Scalia, *The Rule of Law as a Law of Rules*, 56 U. CHI. L. REV. 1175, 1179 (1989) (explaining an "advantage of establishing as soon as possible a clear, general principle of decision" as "predictability").

208 *See* Kerr, *The Mosaic Theory of the Fourth Amendment*, *supra* note 190.

Amendment purposes. Certain acts are "clear as they occur."[209] We all just know when a police officer is viewing a suspect, stopping her, or frisking her, and when each of these distinct acts begins and ends. In Kerr's presentation, the usual transactions dealt with in Fourth Amendment analysis, such as the search of a home or a car, or a seizure of a person during an arrest, seem to exist within naturally occurring frames.[210] The innovation of the mosaic theory, Kerr suggests, is to take a series of these naturally distinct acts and to aggregate them for the purpose of determining whether they collectively constitute something qualitatively different.

But there is no obvious reason to view a *Terry* stop as a single act, while viewing the continuous surveillance of a vehicle for twenty-eight days as a series of discrete acts. In fact, it seems more in line with ordinary linguistic usage to describe the latter surveillance as a single act than to treat it as a series of acts. If the government places a GPS tracking device on a vehicle, and the device remains active for twenty-eight days,[211] it would arguably strain ordinary usage to divide the period of surveillance into some number of segments and call each of these segments a discrete act, even though no new government action takes place at the division between the segments. Is it natural or obvious that the surveillance in *Jones* should be viewed as a series of legally distinct "non-searches"? Where do the temporal lines between these non-searches fall? Perhaps the mosaic theory assumes, based on *Knotts*, that each "trip" taken by the surveilled vehicle should be treated as its own distinct non-search. But is this more natural than viewing the entire twenty-eight-day surveillance as a single act that at some point crosses the threshold into a search?

Conversely, to determine whether a *Terry* stop has taken place, it is often necessary to aggregate a series of acts (or what might be described as distinct

---

209 *Id.* at 318 n.41.

210 *Cf.* Levinson, *supra* note 56, at 1313–14 (suggesting that "the 'frames' that define constitutional law transactions" are constructed, rather than cutting along "natural joints"); RICHARD RORTY, *Texts and Lumps*, *in* 1 PHILOSOPHICAL PAPERS: OBJECTIVITY, RELATIVISM, AND TRUTH 78, 80 (1991) (suggesting that "[t]he notion that some one among the languages mankind has used to deal with the universe is the one the universe prefers—the one which cuts things at the joints . . . . has become too shopworn to serve any purpose"). This Article, like Levinson's *Framing Transactions*, attempts to draw attention to the ways in which legal transactions, such as a "seizure" or a "*Terry* stop," can be seen as historical (and political) constructions, rather than fixed and natural features of the landscape.

211 *Cf.* United States v. Jones, 565 U.S. 400, 403 (2012). In fact, the government replaced the battery in Jones's vehicle once during the twenty-eight-day surveillance period. *Id.*

acts) by a police officer or officers and then to decide whether the acts, as a whole, would have left a reasonable person feeling that she was not "free to leave," or, more abstractly, "free to terminate the encounter."[212] The Supreme Court's 1991 decision in *Florida v. Bostick* directs courts to look to "whether, taking into account all of the circumstances surrounding the encounter, the police conduct would 'have communicated to a reasonable person that he was not at liberty to ignore the police presence and go about his business.'"[213] In more abstract terms, we might interpret *Bostick* as requiring courts to conduct a "totality of the circumstances" analysis involving the aggregation of the coercive and permissive signals communicated by the police's conduct in light of the surrounding circumstances, where coercive signals increase and permissive signals decrease the sum total of coercion in the encounter. At some point along a continuum, the resulting "quantity" of coercion becomes high enough that a reasonable person would not feel free to terminate the encounter. At that point, the legal "quality" of the encounter changes from a non-seizure to a seizure, specifically a *Terry* stop.

In practice, courts attempting to determine whether a police encounter rose to the level of a *Terry* stop often conduct precisely this sort of analysis. They describe various facts about the encounter that would tend to be relevant to a reasonable person[214] attempting to decide whether he or she is

---

212 The "free to leave" test originated in *United States v. Mendenhall*, 446 U.S. 554 (1980), and was adopted by a majority of the Court in *Florida v. Royer*, 460 U.S. 491, 502, 514 (1983). The "free to terminate the encounter" test comes from *Florida v. Bostick*, 501 U.S. 429, 436 (1991). *See* LAFAVE, *supra* note 68, § 9.4(a).

213 *Bostick*, 501 U.S. at 437 (quoting Michigan v. Chesternut, 486 U.S. 567, 569 (1988)).

214 More precisely, "the 'reasonable person' test presupposes an *innocent* person." *Bostick*, 501 U.S. at 438. Or perhaps even more precisely, the test may presuppose an innocent *adult* who is *white*. *See* LAFAVE, *supra* note 68, § 9.4(a) n.42 (quoting Maclin, *supra* note 81, at 250) (noting, among other scholarship and cases, Tracey Maclin's proposal that "[w]hen assessing the coercive nature of an encounter, the Court should consider the race of the person confronted by the police, and how that person's race might have influenced his attitude toward the encounter"). Surely there can be even less doubt in 2020 than in 1991 that young African American men, in particular, face police with a very different set of reasonable assumptions than many other demographic groups. *See, e.g.*, Jemar Tisby, *The Heavy Burden of Teaching My Son About American Racism*, ATLANTIC, Mar. 20, 2018 ("Every black parent has to have 'the talk,' about how to survive an encounter with the police.").

[*Author's Note*: This Article was largely written in spring 2019 and revised in December 2019. During the final copyediting of the Article, mass protests erupted in the United States in response to the digitally filmed killing of an African-American man, George Floyd, by a Minneapolis police officer. *See* Amy Harmon & Sabrina Tavernise, *One Big Difference About George Floyd Protests: Many White Faces*, N.Y. TIMES (June 12, 2020), https://nyti.ms/3dYnkZJ. The protests suggest a growing public

free to leave. LaFave provides a survey of some of the recurring facts courts have considered relevant:

> [A]n officer has not made a seizure if, for example, he interrogated "in a conversational manner," "did not order the defendant" to do something or "demand that he" do it, did not ask questions "overbearing or harassing in nature," and did not "make any threats or draw a weapon." As for "an officer's asking for identification," such action "alone does not amount to a seizure under the Fourth Amendment." (On the other hand, "repeated questioning" regarding identification, "especially when combined with . . . computer databases searches, would convey to a reasonable person that the police were unsatisfied with his answers—to the point that he would not be free to leave until the computer database returned a positive result.") . . . [A]n encounter becomes a seizure if the officer engages in . . . . such tactics as pursuing a person who has attempted to terminate the contact by departing, continuing to interrogate a person who has clearly expressed a desire not to cooperate, renewing an encounter with a person who earlier responded fully to police inquiries, calling to such a person to halt, holding a person's identification papers or other property, conducting a consensual search of the person in an "authoritative manner," bringing a drug-sniffing dog toward the person or his property, intercepting a phone call for the suspect, blocking the path of the suspect, physically grabbing and moving the suspect, drawing a weapon, calling for backup, and encircling the suspect by many officers, in addition to the more obvious ones.[215]

In other words, it would be difficult to defend the notion that a "stop" by a police officer is a single, naturally delineated act, as Kerr's presentation of the mosaic theory assumes. To the contrary, a *Terry* stop is a legal construction that is often defined through the aggregation of multiple acts taking place over time, like a *Maynard/Jones*-type search as presented by Kerr. Just as the court in *Maynard* aggregated a number of acts that were not searches into a search, so courts attempting to determine whether a *Terry* stop has taken place routinely aggregate a number of acts that were not seizures into a seizure. Something similar could be said of other legal categories and definitions in the Fourth Amendment doctrine governing the seizure of

---

acceptance of the racial critiques of American policing and criminal procedure that scholars such as Maclin have been making for decades. Other than this footnote, however, I have not revised the Article to address developments since December 2019, including the COVID-19 pandemic. The pandemic, and the technological reactions to it, have obviously demonstrated the urgency of developing constitutionally reasonable restrictions on digital mass surveillance in the United States.]

215 LAFAVE, *supra* note 68, § 9.4(a) (citations omitted).

persons, including the definition of various types of arrest and the definition of consent to stop.[216]

If a *Terry* stop seems to many of us today to be a naturally discrete act, while prolonged location-tracking using a GPS device seems to consist of a series of separate acts—at least for those attuned to the reasoning of *Knotts*—this may in large part be an illusion resulting from the fact that we have become habituated to *Terry* stops as a legal category, while the coalescing of prolonged electronic surveillance as a recognizable legal category is far more recent and unsettled. In fact, if *Jones* had established a bright-line rule that continuous GPS surveillance of a vehicle for up to seven days is a non-search, while the continuation of the surveillance after the start of day seven is a search and requires a warrant,[217] it would be easy to imagine courts in the future referring to a "*Jones* search" just as they refer to a "*Terry* stop" today. In time, it might have come to seem intuitive to think of *Jones* searches—continuous digital location tracking of vehicles lasting seven days or longer—as discrete, naturally defined acts, rather than as artificial aggregations of smaller acts. As often happens with legal categories, and with concepts in general, the process of construction that resulted in the intuitive sense of a stable entity would have gradually faded from view.

---

216 *Cf. Id.* § 5.1(a) (quoting United States v. Corral-Franco, 848 F.2d 536 (5th Cir. 1988) (defining an arrest as a seizure in which "a reasonable person in the suspect's position would have understood the situation to constitute a restraint on freedom of movement of the degree which the law associates with formal arrest")). Similarly, LaFave notes that courts determine whether a consent to be seized was "voluntary" by looking to the "totality of the circumstances," potentially including:

> the time, place and purpose of the encounter; the words used by the officer, his tone of voice and general demeanor in requesting the defendant to accompany him to the police station; the officer's statements to others who were present during the encounter; the manner in which the defendant was escorted out of the house and transported to the stationhouse; the officer's response to any questions by the defendant or his parents regarding the defendant's right to refuse to go to the stationhouse; and the defendant's verbal or non-verbal responses to any directions given to him by the officer.

Id. § 5.1 & nn.22–50 (quoting People v. Pancoast, 659 P.2d 1348 (Colo. 1982)).

217 Because Justice Scalia's opinion for the majority in *Jones* was based on a theory of trespass, it did not address the issue of how long, under a mosaic theory, the GPS tracking would have had to be in order to constitute a Fourth Amendment search. *See* United States v. Jones, 565 U.S. 400, 404–411 (2012). Justice Alito noted, however, in a concurrence joined by Justices Ginsburg, Breyer, and Kagan, that "[w]e need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark." *Id.* at 418, 430 (Alito, J., concurring in the judgment). Based on the holding in *Carpenter v. United States* that "accessing seven days of CSLI constitutes a Fourth Amendment search," 138 S. Ct. 2206, 2217 n.3 (2018), it does not seem implausible that future courts might also hold that the collection of digital location tracking data for a vehicle for seven days or longer constitutes a Fourth Amendment search. For the possible treatment of digital location tracking lasting less than seven days, see Part III.B above.

Similarly, the application of various evidentiary standards under the Fourth Amendment such as "reasonable suspicion" or "probable cause" frequently involves the aggregation of multiple acts over time—in those cases, the acts of the suspect.[218] Reasonable suspicion analysis often involves the aggregation of a number of pieces of evidence that would not provide a basis for reasonable suspicion by themselves into a totality of evidence that does provide such a basis.[219] The Supreme Court has even referred to such an aggregation using the mosaic-like metaphor of "the whole picture":

> Terms like "articulable reasons" and "founded suspicion" are not self-defining . . . . But the essence of all that has been written is that the totality of the circumstances—the whole picture—must be taken into account. Based upon that whole picture the detaining officers must have a particularized and objective basis for suspecting the particular person stopped of criminal activity.[220]

In the words of the Court in *Terry*, police officers may observe "a series of acts, each of them perhaps innocent in itself, but which taken together warrant[ ] further investigation."[221] Or as the Second Circuit has stated, "the proper inquiry is not whether each fact considered in isolation denotes unlawful behavior, but whether all the facts taken together support a reasonable suspicion of wrongdoing."[222] Just as it is necessary to view the pieces of a mosaic together in order to perceive a picture, so it is often necessary in reasonable suspicion analysis to view a series of acts in combination in order to perceive the grounds for suspicion.

To be clear, Kerr's argument is that the mosaic theory has not been used until recently to distinguish between conduct governed by the Fourth Amendment, and conduct that is not—and his primary focus is the distinction between a non-search and a search. He says nothing about the use of aggregative reasoning in the analysis of reasonable suspicion or probable cause. But the fact that mosaic-like reasoning also appears in the context of the application of evidentiary standards adds to the sense that the Court's recent invocation of such reasoning in digital search cases did not

---

218 *See generally* LAFAVE, *supra* note 68, §§ 3.1–7, 9.5.

219 *See* LAFAVE, *supra* note 68, § 9.5(b) ("The essential point, the *Sokolow* Court said (quoting *Terry*), is that "a series of acts, each of them perhaps innocent" if viewed separately, sometimes "warranted further investigation" when taken together.").

220 United States v. Cortez, 449 U.S. 411, 417–18 (1981).

221 Terry v. Ohio, 392 U.S. 1, 22 (1968).

222 United States v. Lee, 916 F.2d 814, 820 (2d Cir. 1990).

represent a radical departure within Fourth Amendment jurisprudence. With regard to both the definition of stops (and, for that matter, arrests), and the definition of reasonable suspicion (and, for that matter, probable cause), Fourth Amendment doctrine has long recognized that a series of acts that do not fit a legal category in isolation may fit the category "when considered as a group."[223] Even if it is true that courts have not applied this type of aggregative analysis until recently to the specific question of what rises to the level of a search, the use of such an analysis in other core areas of Fourth Amendment law suggests that it is neither as much of a methodological innovation nor as problematic as recent scholarship may suggest.

CONCLUSION

A sophisticated observer of the role that the Supreme Court and its interpretations of constitutional law have played in American history might object that the focus of this Article on Fourth Amendment doctrine is misplaced. If Americans are willing to surround themselves with digital sensors whose data may ultimately be transmitted to the government for storage, analysis, and querying, the argument would go, it is hopeless to expect courts to stop the gradual slide toward an ever-more intrusive and oppressive digital surveillance state.[224]

After all, it might be argued, the Supreme Court rarely departs too far from popular preferences; it has been especially ineffective as a check on executive power wielded in the name of national security; and its current composition suggests that future displays of countermajoritarianism will likely be in favor of, rather than against, law enforcement, executive power, and national security interests. It was always misguided for progressives and civil libertarians to dedicate so much energy and attention to the project of attempting to win the votes of largely unsympathetic swing Justices over the last four decades. Now that the Court has been stocked with youthful, conservative appointees, the argument might conclude, it is almost laughable

---

223 *Cf.* Kerr, *The Mosaic Theory of the Fourth Amendment*, *supra* note 190, at 320.

224 In the frequently quoted words of Learned Hand: "I often wonder whether we do not rest our hopes too much upon constitutions, upon laws and upon courts. These are false hopes . . . . Liberty lies in the hearts of men and women; when it dies there, no constitution, no law, no court can save it . . . ." LEARNED HAND, THE SPIRIT OF LIBERTY: PAPERS AND ADDRESSES OF LEARNED HAND 189–90 (Irving Dillard ed., 1952).

for progressives and civil libertarians to maintain hope for salvation through the Supreme Court.[225]

Indeed, a strong case could be made that the greatest and most urgent threats in the contemporary United States to the privacy values enshrined in the Fourth Amendment lie categorically outside the reach of Fourth Amendment doctrine.[226] Privacy is likely more threatened by the abuses of private parties, from social media platforms and credit card companies to Internet and cell phone service providers, than by state action.[227] Unless and until the Supreme Court begins carving out limitations to the state action doctrine, attempts to regulate the privacy practices of private businesses through legislation, administrative action, and democratic activism will almost certainly remain the most important fronts in the struggle for privacy in the digital age.

But even if the preceding critiques show that the reform of Fourth Amendment doctrine should not be the primary focus of efforts to defend digital privacy, the critiques do not suggest that the shape of Fourth Amendment doctrine makes no difference at all. Government invasions of privacy obviously continue to have a special importance because of the powers of government, including through the punitive enforcement of criminal laws. In closing, I would emphasize three reasons why those who are concerned about digital privacy should remain engaged in debates over the future shape of Fourth Amendment digital search doctrine.

First, and most importantly, whatever the relative efficacy of protecting digital privacy through courts and other means, it remains the fact that judges will continue to be confronted with litigants challenging the

---

225 *Cf.* Samuel Moyn, *Resisting the Juristocracy*, BOSTON REV. (Oct. 5, 2018), http://bostonreview.net/law-justice/samuel-moyn-resisting-juristocracy (criticizing the inevitable prospect that many progressives "will look hopefully to Chief Justice John Roberts as the new swing vote and treat him, as they did Anthony Kennedy, as the new 'centrist' to lure").

226 *See, e.g.*, Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 19–21 (2008).

227 An example that arose during the writing of this Article, one of countless examples that could be offered, involves medical information: "[P]owerful companies such as LexisNexis have begun hoovering up the data from insurance claims, digital health records, housing records, and even information about a patient's friends, family and roommates, without telling the patient they are accessing the information, and creating risk scores for health care providers and insurers." Mohana Ravindranath, *How Your Health Information Is Sold and Turned into 'Risk Scores*,' POLITICO (Feb. 3, 2019, 6:56 AM), https://www.politico.com/story/2019/02/03/health-risk-scores-opioid-abuse-1139978.

constitutionality under the Fourth Amendment of the government's collection and use of digital data. These judges will be forced to make rulings. As appealing as counterintuitive arguments based on futility, perversity, and jeopardy may be in an academic setting, it is hardly the case that when courts hold a practice to be an unconstitutional violation of some constitutional right, the result is always a political backlash that ultimately leads to greater violations of the right or the sacrifice of some other interest.

To the contrary, as the stop-and-frisk litigation in New York shows, a judicial declaration that a practice violates the Constitution can at least sometimes focus public and official attention on the practice in a way that ultimately undermines popular support for it and encourages the practice's abandonment by public officials.[228] The stop-and-frisk litigation also offers a reminder that not all constitutional decisions are made by the Supreme Court, or ever reach the Court.[229] There is no reason for privacy advocates to unilaterally abandon the courts as one potential lever for promoting digital privacy—especially considering that digital privacy may be one of the only disputed areas on which the current Supreme Court's remaining liberals are sometimes, at the moment, capable of achieving a majority.

Second, promoting digital privacy through social movements, legislation, and administrative action generally requires that the public be aware of the government's use of digital surveillance, so that the public can organize in opposition to excesses, and advocate for legislative and regulatory change. But much of the government's use of digital surveillance, across all levels and areas of government, has been and remains clouded in secrecy. Constitutional litigation can sometimes help expose, document, and draw attention to government practices that would otherwise remain unknown.[230]

---

228 As Harmon and Manns note:

> In the presence of intense public and media debate following the *Floyd* decision, Bill de Blasio, a long-shot candidate, bet his political future on opposing the SQF policy, and won that bet. After he took office, he withdrew the appeal, ending further litigation of the merits; agreed to the City's participation in the court-run remedial process; and has substantially changed NYPD's practices with respect to stops and frisks in New York City.

Harmon & Manns, *supra* note 64, at 68 (footnotes omitted).

229 *See id.*

230 *See, e.g.*, Klayman v. Obama, 957 F. Supp. 2d 1, 40 (D.D.C. 2013) (noting that "the Government does *not* cite a single instance in which analysis of the NSA's bulk metadata collection actually stopped an imminent attack, or otherwise aided the Government in achieving any objective that was time-sensitive in nature"), *vacated*, 800 F.3d 559 (D.C. Cir. 2015).

Third, even if some parts of the public are aware of constitutionally problematic digital surveillance practices, such awareness may be insufficient to bring about change if the most negatively affected parts of the public lack sufficient political power. In the words of Justice Robert Jackson, "[c]ourts can take no better measure to assure that laws will be just than to require that laws be equal in operation."[231] Where laws are unequal in their operation, as policing and surveillance have been throughout American history,[232] judicial intervention may be a worthwhile, perhaps even essential, part of a larger, coordinated political effort to protect the privacy of marginalized groups from digital threats. Although it might seem at first glance that digital surveillance would mostly affect the affluent, because they own and use the most digital devices, in reality the usual subjects of disproportionate government surveillance—such as racial and religious minorities, and those living in poverty[233]—are likely to bear a disproportionate burden of digital surveillance as well. They will have more contacts with bodycam-wearing police, their neighborhoods will be the focus of anti-crime surveillance technologies such as surveillance cameras, stingrays, and gunfire locators, and their interactions with often invasive government programs will result in greater accumulations of government records, which may then be digitally stored, aggregated, and queried.

Indeed, when this Article has referred to mass or large-scale surveillance, it has often left unspecified which community or communities might be subject to such surveillance. But surely one of the things that makes unchecked digital mass surveillance so troubling is the likelihood that it will be focused on politically subordinated groups. In the context of digital mass surveillance, as in so many other contexts, the concerns of the Fourth Amendment ultimately cannot be separated from the concerns of the Equal Protection Clause of the Fourteenth Amendment.[234] It is true that the judiciary may not be able, by itself, to prevent the rise of an era of discriminatory digital mass surveillance, if the political will for such programs exists. But, if nothing else, courts can attempt to draw democratic attention

---

231 Ry. Express Agency v. New York, 336 U.S. 106, 113 (1949) (Jackson, J., concurring).

232 *See generally* LAWRENCE M. FRIEDMAN, CRIME AND PUNISHMENT IN AMERICAN HISTORY (1993).

233 *See, e.g.*, KHIARA BRIDGES, THE POVERTY OF PRIVACY RIGHTS (2017).

234 In a future work, I hope to explore the equal protection implications of discriminatory mass surveillance in greater depth.

to the constitutional threats posed by such programs, and can avoid complicity in their undermining of the Constitution.[235]

235 *Cf.* Korematsu v. United States, 323 U.S. 214, 244 (1944) (Jackson, J., dissenting) (suggesting that in times when constitutional values are threatened, even if the Supreme Court cannot confine the executive's expedients by the Constitution, neither should the Court "distort the Constitution to approve" all that the executive deems expedient), *overruled by* Trump v. Hawaii, 138 S. Ct. 2392 (2018); ROBERT M. COVER, JUSTICE ACCUSED: ANTISLAVERY AND THE JUDICIAL PROCESS (1975).