DIGITIZING THE FOURTH AMENDMENT: PRIVACY IN THE AGE OF BIG DATA POLICING

Charles E. Volkwein

DIGITIZING THE FOURTH AMENDMENT: PRIVACY IN THE AGE OF BIG DATA POLICING

Charles E. Volkwein*

ABSTRACT

Today's availability of massive data sets, inexpensive data storage, and sophisticated analytical software has transformed the capabilities of law enforcement and created new forms of "Big Data Policing." While Big Data Policing may improve the administration of public safety, these methods endanger constitutional protections against warrantless searches and seizures. This Article explores the Fourth Amendment consequences of Big Data Policing in three parts. First, it provides an overview of Fourth Amendment jurisprudence and its evolution in light of new policing technologies. Next, the Article reviews the concept of "Big Data" and examines three forms of Big Data Policing: Predictive Policing Technology (PPT); data collected by third-parties and purchased by law enforcement; and geofence warrants. Finally, the Article concludes with proposed solutions to rebalance the protections afforded by the Fourth Amendment against these new forms of policing.

INTRODUCTION

We live in an era where digital information is ubiquitous. The ability to collect, store, process, and analyze large quantities of information yields a wealth of insight to the end user about individual and group behavior, thought and desire. This process, called "Big Data," is leveraged by law enforcement to enhance enforcement capabilities and maintain public safety.[1] Big Data policing on the one hand may be beneficial to the administration of public safety; however, it raises serious concerns about how these new methods impact existing Fourth Amendment protections against unwarranted searches and seizures. This paper examines how Big Data policing impacts the Fourth Amendment and endangers existing constitutional privacy protections. I argue that current interpretive doctrines of what constitutes a "search" under the Fourth Amendment must be adapted and implemented with additional legislative safeguards to ensure that Big Data policing methods do not erode constitutionally guaranteed protections against warrantless government searches.

To make this argument, I begin with an overview of Fourth Amendment jurisprudence. I describe the evolution of how the concept of a search is understood considering advancements in policing technology. Next, I turn to Big Data policing specifically. I provide a brief, technical definition of Big Data and then identify three examples of Big Data policing in practice. Each example will discuss how the technology or method interacts with the Fourth Amendment, illustrating how these

* J.D. candidate, University of Maine School of Law, class of 2023.

[1] *See, e.g.*, Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35, 38 (2014), https://digitalcommons.law.uw.edu/wlr/vol89/iss1/3.

tools are challenge constitutional protections against warrantless and arbitrary searches and seizures. In conclusion, I advocate for measures that rebalance protections afforded by the Fourth Amendment against unreasonable searches and seizures posed by Big Data policing. I propose potential legislative solutions designed to fill in the gaps where the Fourth Amendment may still fall short in mitigating the erosion of rights to individual rights and informational privacy caused by Big Data policing.

I. THE FOURTH AMENDMENT: AN OVERVIEW

The Fourth Amendment protects the "right of people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" and provides that "no [w]arrants shall issue, but upon probable cause . . . ."[2] A warrant issued upon probable cause must be "supported by [o]ath or affirmation, and particularly describe[] the place to be searched, and the persons or things to be seized."[3] Warrant applications must be submitted to a "neutral and detached" judge or magistrate.[4] That judge, in turn, makes an "informed and deliberate" decision regarding the warrant's showing of probable cause and particularity.[5] In some cases, law enforcement are permitted to conduct a search without a warrant. One exception to the warrant requirement is a law enforcement official's power to stop-and-frisk an individual based on "reasonable suspicion of criminal activity."[6] This power is uniquely augmented by Big Data policing capabilities and will be discussed in the context of predictive policing later in this paper.

Fourth Amendment jurisprudence is patchwork and fact- specific, with multiple competing doctrines informing the courts' decision-making as to what new policing methods and technology constitute searches or seizures.[7] The evolving interpretations of the Fourth Amendment reflect the push-and-pull relationship between the public's right to privacy and security in their persons, places, and things and the government's desire to ensure public safety. Courts initially interpreted the Fourth Amendment narrowly, limiting its scope as a right grounded in property protecting only against physical intrusion of private spaces.[8] In response

---

[2] U.S. Const. amend. IV.
[3] *Id*.
[4] *Johnson v. United States*, 333 U.S. 10, 14 (1948).
[5] *United States v. Lefkowitz*, 285 U.S. 452, 464 (1932).
[6] *Terry v. Ohio*, 392 U.S. 1, 30–31 (1968); *United States v. Sokolow*, 490 U.S. 1, 7 (1989) ("[P]olice 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,' even if the officer lacks probable cause.") (quoting *Terry*, 392 U.S. at 30).
[7] Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 480 (2011), https://harvardlawreview.org/2011/12/an-equilibrium-adjustment-theory-of-the-fourth-amendment/.
[8] *Olmstead v. United States*, 277 U.S. 438, 466 (1928), *overruled by Berger v. New York*, 388 U.S. 41 (1967), *and Katz v. United States*, 389 U.S. 347 (1967). This property-based approach is known as the trespass doctrine. *See also* Laura Hecht-Felella, *The Fourth Amendment in the Digital Age*: *How Carpenter Can Shape Privacy Protections for New Technologies*, BRENNAN CTR. FOR JUST. (Mar. 18, 2021), https://www.brennancenter.org/our-work/policy-solutions/fourth-amendment-digital-age.

to new policing technologies used in the absence of warrants, the interpretation expanded to "protect people and not simply areas," with the Supreme Court holding that the Fourth Amendment's applicability "cannot turn upon the presence or absence of a physical intrusion."[9] Trespass was no longer the controlling factor to assess whether a search occurred; rather, a person's reasonable expectation of privacy became part of the equation, so long as that reasonable expectation was still grounded in material things. Through its decision in *Katz v. United States*, 389 U.S. 347 (1967) the Supreme Court established a two-part doctrine to determine whether an individual has a reasonable expectation of privacy which, subject to some exceptions, cannot be violated without a warrant. The doctrine holds that if a person harbors a subjective expectation of privacy in a given place or toward a given thing, and society objectively accepts the reasonableness of that expectation then the individual maintains a reasonable expectation of privacy that cannot be invaded without a warrant.[10]

The reasonable expectation of privacy doctrine is tempered, however, by yet another principle informing the analysis of a potential Fourth Amendment violation: the third-party doctrine. If an individual voluntarily shares information with a third-party, that individual's reasonable expectation of privacy to the information shared with the third-party is nullified; therefore, a warrant is not required for law enforcement to access the information.[11] The Supreme Court codified the third-party in two cases, *United States v. Miller* (1976) and *Smith v. Maryland* (1979). In *Miller*, the Supreme Court held that defendant Mitch Miller possessed no reasonable expectation of privacy to the contents of his checks and deposit slips which he had voluntarily shared with his bank. The Court reasoned that the Fourth Amendment was not violated because this information, was not a confidential communication, but instead, a voluntarily conveyed instrument used in routine commercial transactions by the bank and its employees.[12]

Three years later, in *Smith* the Court affirmed the third-party doctrine. In that case, the Supreme Court found no violation of the Fourth Amendment when police warrantlessly installed a pen register, which is an electronic device that records numbers dialed from a telephone, on defendant Michael Smith's telephone. The Court found that Mr. Smith possessed no reasonable expectation of privacy to the telephone numbers he dialed, because he voluntarily shared those numbers with the telephone company, who records them as part of its ordinary business practices.[13] Furthermore, the Court reasoned that Mr. Smith assumed the risk that the company might reveal the information he voluntarily conveyed to it, therefore

---

[9] *Katz*, 389 U.S. at 351, 353 (holding that an eavesdropping device placed on a public pay phone by law enforcement to listen to calls without a warrant constituted an unreasonable search).
[10] *Id*. at 361 ("[If the Fourth Amendment protects people not places], the question is what protection it affords those people. Generally, as here, the answer to that question requires reference to a 'place.'") (Harlan, J., concurring).
[11] *See United States v. Miller*, 425 U.S. 435 (1976); *see also Smith v. Maryland*, 442 U.S. 735 (1979).
[12] *Miller*, 425 U.S. at 437.
[13] *Smith*, 442 U.S. at 745.

the installation and use of a pen register collecting this same information is not a search within the meaning of the Fourth Amendment.[14]

The Supreme Court addressed both the reasonable expectations of privacy and third-party doctrines in *Carpenter v. United States* (2018). The Court's holding in *Carpenter* represents another stage in the evolution of Fourth Amendment interpretation, advancing the concept of reasonable expectations to privacy further to adapt the amendment to the digital age. In *Carpenter*, the Court held that a mobile phone user possesses a reasonable expectation of privacy in their historical cell-site location information (CSLI), which are records generated and retained by the user's cellular service provider (a third-party).[15] To access this information, law enforcement must get a traditional warrant.[16]

Prior to *Carpenter*, the reasonable expectation of privacy doctrine was limited to places and things. *Carpenter* shifts the inquiry from an individual's reasonable expectation of privacy concerning a place or thing to their reasonable expectation of what law enforcement can access and discover in the digital age.[17] This shift represents the Court's acknowledgment that "'[t]here is a world of difference' . . . 'between the limited types of personal information' at issue before the digital age and the 'exhaustive chronicle' of information . . . new technologies can provide."[18] To put it another way, *Carpenter* recenters the reasonable expectations inquiry on whether "a prior limit on government power has been lifted" that permits the Government to take investigative steps that "far exceed their powers in the past" and, therefore, "contravene[] expectations."[19] If technology enables surveillance that could not occur before, the new surveillance becomes a search.[20] The Court's ruling also declined to extend the third-party doctrine to CSLI, noting that "data generated by technologies that are integral to modern day life are [not voluntarily shared] when the production of this information is 'inescapable and automatic.'"[21] However, the Court did not categorically do away with the third-party doctrine as an avenue for interpretation, explicitly noting that its holding in *Carpenter* does not impact the precedent it set in *Smith* or *Miller*.[22]

The post-*Carpenter* Court has multiple avenues from which to approach the inquiry of whether a police activity is a search. In Part III of this analysis, I identify several methods of modern policing that the Court's new reasonable expectation of privacy doctrine will need to address. In Part IV, I argue that the Supreme Court will need to extend and clarify its new reasonable expectations of privacy test further to properly rebalance privacy rights considering the Big Data policing tactics explored in Part III.

---

[14] *Id*.
[15] *Carpenter v. United States*, 138 S. Ct. 2206 (2018).
[16] *Id*.
[17] Orin S. Kerr, "Implementing Carpenter," in *The Digital Fourth Amendment* (Oxford: Oxford University Press, forthcoming), 6, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3301257.
[18] *Id*. at 16 (quoting *Carpenter*, 138 S. Ct. at 2219).
[19] *Id.* at 10.
[20] *Id*.
[21] Hecht-Felella, *supra* note 8, at 10 (quoting *Carpenter*, 138 S. Ct. at 2223).
[22] *Carpenter*, 138 S. Ct. at 2220.

II. WHAT IS BIG DATA AND HOW DO LAW ENFORCEMENT AGENCIES USE IT

"Big Data" is a buzzword attributed to all sorts of digital activities in the public and private sectors. Although it seems that everyone in every industry, sector, and enterprise uses "Big Data," it can be difficult to attribute a single definition to the term. Is it a noun? Is it a verb? How "Big" is "Big"? Furthermore, what is "Data"? The next section will provide a brief overview and definition of the term before exploring its use by law enforcement.

a. *Big Data: A Brief Technical Overview*

Though it is a "generalized [and] imprecise term," Big Data is not impossible to concretely define.[23] To begin, the term itself refers to the collection of large quantities of data. There is no set amount of data that, once collected, defines a dataset as "Big." Rather, the adjective refers to the principle that "larger data sets generate results with greater truth, objectivity and accuracy."[24] Volume, variety, and velocity are the "common framework" through which data collection and analysis are viewed and classified as Big Data.[25] "Data," in this context, I define as digitally available information (regardless of source or input) about persons, whether they are acting as individuals or in groups. Because "nearly every piece of information . . . is capable of digitization and storage," the pervasiveness of Big Data will only increase.[26] At its core, Big Data's power "lies in capturing the massive reserves of data that are incidentally, as well as purposefully, generated through increasingly detailed electronic documentation of individuals' everyday lives.[27]

Large and diverse data sets containing intimate information are only half of the equation. The term "Big Data" also encapsulates how data is studied and analyzed to generate conclusions, namely correlative predictions, and insights into patterns of behavior concerning the individuals and groups whose data is collected. Big Data describes how tools that "maximize computational power and algorithmic

---

[23] Kate Crawford & Jason Schultz, *Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms*, 55 B.C. L. REV. 93, 96 (2014), https://lawdigitalcommons.bc.edu/bclr/vol55/iss1/4.

[24] *Id*.

[25] Amir Gandomi & Murtaza Haider, *Beyond the Hype: Big Data Concepts, Methods, and Analytics*, 35 Int'l. J. Of Info. Mgmt. 137, 138 (2015), https://www.sciencedirect.com/science/article/pii/S0268401214001066; *see also*, Timothy A. Asta, Guardians of the Galaxy of Personal Data: Assessing the Threat of Big Data and Examining Potential Corporate and Governmental Solutions, 45 Fla. St. U. L. Rev. 261, 267 (2019), https://ir.law.fsu.edu/lr/vol45/iss1/6 ("[t]he 3 Vs . . . can be used to identify datasets that are so large in volume, so diverse in variety or moving with such velocity, that traditional modes of data capture and analysis are insufficient.").

[26] Joh, *supra* note 1, at 38.

[27] Carey Devens et al., *The Law and Big Data*, 27 Cornell L. Rev. 357, 363 (2017), https://scholarship.law.cornell.edu/cjlpp/vol27/iss2/3/.

accuracy" magnify and manipulate vast troves of information.[28] Likewise, when drawing conclusions, Big Data is "empirical, algorithmic, and deterministic."[29] In sum, Big Data refers to the operation by which large amounts of digital information are amassed and subjected to analysis by algorithms or other analytical methods, which revealing correlations of value to the end user of the data. These algorithms are crafted to provide any number of desired insights or outcomes to the end user.[30]

Despite the perceived objectivity of Big Data and its widespread adoption by police departments of all sizes, it is crucial to highlight its limitations. Decisions made by police about what data is collected and how it is collected reflect human biases, impacting the efficacy, accuracy and quality of the data collected.[31] Furthermore, Big Data's capacity to accurately and completely create an image of who a person is or whether they are more prone to commit a certain act is limited. Once the information is collected, analytical models and algorithms cannot "innovate beyond the paradigm of [their] creators" and are only as good as the data provided to them.[32] Accurate insights cannot be extrapolated from poor data. Finally, decisions about how to interpret conclusions rendered from Big Data raise further vulnerabilities, particularly in the criminal justice context, where stakes are high. Data may indicate one reality, but the complexities of human nature often cannot be boiled down to a few data points. In sum as the next section details, while the benefits are clear to law enforcement, poor data and faulty analysis in Big Data policing risks increasing the likelihood of arbitrary surveillance, warrantless searches and seizures, and even illegitimate detentions of innocent individuals.[33]

b. Big Data Policing: What It Looks Like

Law enforcement agencies have historically relied on data collection and analysis to inform their administration of public safety.[34] However, now, because of the eruption and demands of the modern information economy, law enforcement agencies have access to massive amounts of consumer data, historical and real-time, that allow them to "essentially pluck a suspect out of thin air."[35] Big Data

---

[28] Crawford & Schultz, *supra* note 23, at 96.
[29] Devens et al., *supra* note 27, at 360.
[30] *Id.*
[31] *See* Rashida Richardson et al., *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 N.Y.U. L. REV. 192, 208 (2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3333423.
[32] Crawford & Schultz, *supra* note 23, at 96.
[33] *See, e.g.*, Kashmir Hill, *Wrongfully Accused by an Algorithm*, N.Y. TIMES (Aug. 3, 2020), nytimes.com/2020/06/24/technology/facial-recognition-arrest.html.
[34] *See* Jennifer Bachner, *Predictive Policing: Preventing Crime with Data and Analytics*, IBM Center for the Business of Government (2013), https://www.businessofgovernment.org/sites/default/files/Management%20Predictive%20Policing.pdf.
[35] Jennifer Lynch, *Modern-Day General Warrants and the Challenge of Protecting Third Party Privacy Rights in Mass Suspicion-less Searches of Consumer Databases*, Hoover Working Group. on National Security, Technology and Law, Aegis Series Paper No. 2104, 1, https://www.lawfareblog.com/modern-day-general-warrants-and- challenge-protecting-third-party-privacy-rights-mass-suspicionless.

amplifies the potency and scope of traditional police activities dramatically. Indeed, "the surveillance capacities of police today far exceed what armies of police officers could accomplish without access to [B]ig [D]ata" in the past.[36] Law enforcement "now ha[s] relatively easy and inexpensive access to data that can identify and track all of us."[37] At what point do surveillance, data collection and predictive technologies, employed without warrants, become searches and seizures that violate the Fourth Amendment? Should a computer program decide whether "reasonable suspicion exists" as a pretext to stop and frisk someone on the street?

To illustrate how law enforcement agencies' leveraging of Big Data imperils Fourth Amendment protections, I provide an overview of three examples of Big Data techniques used by police: (1) predictive policing; (2) the purchasing of third-party harvested consumer data; and (3) geofencing.

i. Predictive Policing Technology ("PPT")

"Predictive policing refers to any policing strategy or tactic that develops and uses information and advanced analysis to inform forward-thinking crime prevention."[38] The idea of predictive policing is not new, but how it is currently employed is markedly more potent than its early roots.[39] Traditionally, predictive policing relied on crime-mapping with historical crime data collected and analyzed to produce a physical map of where such crime is occurring, which would then be used to deploy resources.[40] Modern predictive policing attempts to be proactive, building on this information to, in theory, prevent crime before it happens. PPT "predicts" crimes or suspicious targets using artificial intelligence and algorithms to visualize correlations and patterns within large quantities of data about a given geographical area.[41] Police departments' access to cheap and voluminous data storage combined with powerful analytical processing capabilities make PPT a potent crime prevention technique.[42]

There are two primary forms of PPT: place-based and person-based.[43] Place-based PPT, which has been more widely adopted than person-based, still relies on historical crime data to produce detailed spatial and temporal maps that

---

[36] Joh, *supra* note 1, at 60.
[37] Lynch, *supra* note 35, at 1.
[38] Andrew G. Ferguson, *Predictive Policing and Reasonable Suspicion*, 62 Emory L. J. 259, 265 (2012), https://scholarlycommons.law.emory.edu/elj/vol62/iss2/1 (quoting, Craig D. Uchida, *A National Discussion on Predictive Policing: Defining Our Terms and Mapping Successful Implementation Strategies*, Nat'l Inst. Of Just., No. NCJ 230404 (2009)).
[39] *See* Bachner, *supra* note 34, at 86 (describing early forms of crime mapping in the 19th century).
[40] *Id*.
[41] Ferguson, *supra* note 38, at 266 ("A simple predictive policing model might take historical data about a particular type of crime, the location and the time of that crime and plot those past crimes . . . . A more complex predictive policing model might involve event-based concerns—such as arrests, calls for services or incident reports.").
[42] Bachner, *supra* note 34, at 86.
[43] *See* Tim Lau, *Predictive Policing Explained*, BRENNAN CTR. FOR JUST. (Apr. 1, 2021), https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained.

identify places and times that have a high risk of crime.[44] So- called "hotspot" detection enables law enforcement to forecast where crime is more likely to occur and, with targeted resource deployment, proactively reduce the likelihood of that occurrence.[45] The New York City Police Department ("NYPD"), for example, uses a Domain Awareness System ("DAS") that stores and processes information obtained from a network of information collection inputs around the city (e.g., cameras, databases, radiation sensors, and automatic license plate readers).[46] With predictive algorithms for several different categories of crime, the NYPD deploys officers based on the insights DAS provides.[47]

Person-based PPT is used to detect persons of interest or individuals likely to be involved in a crime. One method of person-based PPT is employed through social network analysis ("SNA"), where "a target's numerous interpersonal relationships are mapped and mine[ed] for actionable information."[48] Another method employed uses the collection and review of crime databases in combination with third-party data to identify individuals who are at risk of being a party to a criminal act.[49]

The widespread adoption of PPT by law enforcement agencies raises two primary concerns. First, PPT allows law enforcement to outsource the prerequisite of establishing reasonable suspicion prior to a search, to an algorithm. Because PPT's data-backed insights appear objective and unbiased, police may over rely on those insights to establish reasonable suspicion and initiate a search.[50] Experience shows that PPT programs suffer from lack of accuracy and objectivity in their data.[51] Historical crime data informing PPT systems often comes from "documented periods of flawed, racially biased, and sometimes unlawful practices and policies."[52] Simply put, "dirty" data cannot produce accurate results because the data itself is fundamentally flawed.[53] Compounding this flaw is the fact that individuals with prior interactions with law enforcement, even if those interactions were the product of illegitimate policing practices, will have that information

---

[44] *Id. See also* Bachner, *supra* note 34, at 87 ("It is important to keep in mind that a hot spot is a perceptual construct. Because geographical space is inherently continuous, the placement of a boundary to delineate a hot spot is somewhat arbitrary.").
[45] Bachner, *supra* note 34, at 87.
[46] *See* City of New York Police Department, *Domain Awareness System: Impact and Use Policy* (Apr. 11, 2021), https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/post-final/domain-awareness-system-das-nypd-impact-and-use-policy_4.9.21_final.pdf.
[47] *Id.*
[48] Bachner, *supra* note 34, at 88.
[49] Richardson et al., *supra* note 31, at 208.
[50] *See* Ferguson, *supra* note 38, at 304; *see also* Emily Berman, *Individualized Suspicion in the Age of Big Data*, 105 IOWA L. REV. 463 (2020), https://ilr.law.uiowa.edu/print/volume-105-issue-2/individualized-suspicion-in-the-age- of-big-data/.
[51] *See* Richardson et al., *supra* note 31.
[52] *Id*. *See also* William K. Rashbaum, *Retired Officers Raise Questions on Crime Data*, N.Y. TIMES (Feb. 6, 2010), https://www.nytimes.com/2010/02/07/nyregion/07crime.html; John Marzulli, *We Fabricated Drug Charges Against Innocent People to Meet Arrest Quotas, Former Detective Testifies*, N.Y. DAILY NEWS (Oct. 13, 2011), https://www.nydailynews.com/news/crime/fabricated-drug-charges-innocent-people-meet-arrest-quotas- detective- testifies-article-1.963021.
[53] *See* Richardson et al., *supra* note 31.

weaponized against them by a PPT system. This means that "those with lengthy criminal records. . . [will be] stopped because of who they are and not what they are doing."[54] Notably, the lack of unbiased, independently certifiable data has caused several departments to abandon their programs.[55]

Second, there is a likelihood that preemptive monitoring of crime hotspots will lead to higher numbers of searches of otherwise innocent persons because of their proximity to a PPT- designated crime hot spot. The use of PPT technology without sufficient data transparency makes it difficult to challenge the validity of a stop. A suspect might be completely innocent and stopped regardless, on account of their proximity to a PPT-designated hotspot. "To mount a coherent challenge to a particular decision, we must know how that decision is made."[56] However, there is little transparency into how police departments' PPT programs weigh each factor that goes into their analyses. The risk of arbitrary searches is high if police rely on PPT to generate the reasonable suspicion that permits them to make a stop but cannot identify how the PPT actually came to its conclusion that reasonable suspicion exists.[57] So far, there is one clear example of PPT causing this type of situation to occur in an instance where someone was in the wrong place at the wrong time. In 2020, the Fourth Circuit Court of Appeals upheld a motion to suppress firearm evidence acquired after police officers stopped and frisked an individual in close proximity to a PPT- designated hotspot.[58] The court maintained that a person's physical presence, even within a PPT-designated high-crime area, cannot alone create a reasonable suspicion.[59] Concurring opinions also noted the dangers that PPT poses to those living near high-crime areas, and the risk that such technology perpetuates bias and illegitimate profiling.[60]

PPT programs are a form of Big Data policing that have the potential to enhance public safety, especially when it comes to the effective distribution of resources in a large jurisdiction. However, until these programs can be sufficiently

---

[54] Ferguson, *supra* note 38, at 401; *see also* The Verge, *Chicago PD automated policing program got this man shot twice* (May 24, 2021), https://www.theverge.com/c/22444020/chicago-pd-predictive-policing-heat-list.

[55] The Santa Cruz Police Department, Los Angeles Police Department and Chicago Police Department all abandoned their PPT programs because of problematic outcomes reflecting biased data. *See*, *e.g.*, Kristi Sturgill, *Santa Cruz becomes the first U.S. city to ban predictive policing*, LOS ANGELES TIMES (June 26, 2020), https://www.latimes.com/california/story/2020-06-26/santa-cruz-becomes-first-u-s-city-to-ban-predictive-policing; Kathleen Foody, *Chicago police end effort to predict gun offenders, victims*, THE ASSOCIATED PRESS (Jan. 23, 2020), https://apnews.com/article/41f75b783d796b80815609e737211cc6; Johana Bhuiyan, *LAPD ended predictive policing programs amid public outcry. A new effort shares many of their flaws*, THE GUARDIAN (Nov. 8, 2021), https://www.theguardian.com/us-news/2021/nov/07/lapd-predictive-policing-surveillance-reform (noting that in 2019 the LAPD Inspector General found the criteria used in the program to be inconsistent).

[56] Berman, *supra* note 50, at 502.

[57] *Id*. "A computer model cannot necessarily reveal what exactly is included in the model, how each factor is weighed, or whether there are factors included in the model that perhaps should *not* be taken into account." *Id.*

[58] *United States v. Curry*, 965 F.3d 313 (4th Cir. 2020) (en banc) (8-6 decision).

[59] *Id*. at 331.

[60] *Id.* at 344-45 (Thacker, J., concurring); *id.* at 334 (Gregory, J., concurring); *id.* at 336-37 (Wynn, J., concurring).

vetted to demonstrate that the information and methods used by the systems are accurate and unbiased, these programs will continue to produce arbitrary searches without proper, individualized reasonable suspicion, raising various concerns under the Fourth Amendment.

ii. Data Collected by Third-Parties and Purchased by Law Enforcement

Ordinarily, law enforcement seeking access to personal electronic information from an entity that retains it must obtain a warrant based on probable cause with sufficient particularity or a court order following the procedures established by the Electronic Communications Privacy Act (1986) ("ECPA").[61] Now, however, state and local police, federal law enforcement entities, and domestic intelligence agencies are able to purchase bulk, packaged sets of consumer data collected and categorized by private data brokers for further downstream analysis.[62] Data brokers are for-profit companies, typically operating in obscurity to consumers, who collect personal information about individual consumers from a variety of online sources, combine it in a multitude of ways and then sell it to buyers who, in turn, use that information for their own commercial purposes.[63] There is little transparency or oversight into how much personal information is purchased by law enforcement and the purposes for which it is used.[64]

There are recorded instances of law enforcement entities on record purchasing "aggregated app-generated location data."[65] This data concerns precise location data, including "patterns of travel," which are generated as a byproduct of a user engagement with a networked device or application. This information is purportedly de-identified, aggregated, and then sold to data brokers, either directly from the mobile application, website, or via another broker. The information is then resold by the data broker to law enforcement. Using this information, law enforcement entities are able to conduct "suspicion-less searches," that is, searches

[61] *See* 18 U.S.C. § 2703(a)-(d). Covered entities under the ECPA are precluded from voluntarily sharing stored information with the government. *Id*.

[62] *See* Lynch, *supra* note 35; *see also* Carey Shenkman et al., *Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers*, Ctr. For Dem. & Tech. (Dec. 2021), https://cdt.org/wp-content/uploads/2021/12/2021-12-08-Legal-Loopholes-and-Data-for-Dollars-Report-final.pdf; Lauren Sarkesian & Spandana Sigh, *How Data Brokers and Phone Apps Are Helping Police Surveil Citizens Without Warrants*, ISSUES IN SCI. AND TECH. (Jan. 6, 2021), https://issues.org/data-brokers-police- surveillance/.

[63] Shenkman et al., *supra* note 62, at 9 ("[A] data broker [is] any business that knowingly collects, purchases, analyses, or aggregates data used or intended to be used to identify individuals or their devices without having a direct relationship with those individuals, for the purpose of selling that data.").

[64] *Id*. at 22. Publicly available documents indicate that data obtained from brokers are used for "pre-investigative inquiries, intelligence gathering, crime prevention, or criminal investigations." *Id.*

[65] Lynch, *supra* note 35, at 6; Shenkman et al., *supra* note 62, at 24 (highlighting contracts between the FBI and data brokers for location data).

within these databases that are not based on a particularized suspicion.[66] Though all the information is de-identified when aggregated by data brokers, is de-identified, re-identification is typically part of the law enforcement processing of that information.[67] Re-identification is made easier when location information is combined with another type of consumer information known as "advertising identifier data" ("AdID"), which is also available for purchase by law enforcement.[68] AdID provides information about "where a person is located, what device they are using, what language they use, which websites they're visiting and for how long, and which websites they buy things from."[69] Details about the extent to which law enforcement (primarily federal agencies) leverage AdID are scarce; however, law enforcement agencies have acknowledged that they are able to use this information to re-identify individual users from location data.[70]

This practice circumvents Fourth Amendment protections and is problematic for two primary reasons. First, the practice exploits a blind spot in ECPA's scope of coverage. ECPA prevents "Remote Computing Services" ("RCS") and "Electronic Communications Services" ("ECS") from voluntarily disclosing non-content information retained about their customers or users to government entities.[71] However, "ECPA permits RCS and ECS providers to voluntarily share non-content information to non-governmental third parties. If those third parties are not RCS or ECS providers . . . [,] ECPA does not apply."[72] Because data brokers are neither RCS nor ECS providers under ECPA, they are not prohibited from sharing or selling geolocation data with the Government.

Second, the type of information sold by data brokers to law enforcement is akin to the CSLI at issue in *Carpenter*: in that it is location information that "provides an intimate window into a person's life."[73] Because the Supreme Court recognized the sensitivity of location information in *Carpenter*, it should follow that sensitive information sold by data brokers to law enforcement is afforded the same protection as CSLI. However, "internal legal justifications of government purchases . . . are explicit in referencing *Carpenter* and stating that . . . the case does not apply to their practice."[74]

---

[66] *Id*.
[67] *See, e.g.*, Yves-Alexandre de Montjoye et al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, 3 NATURE SCI. REPS., no. 1376 (2013), http//www.nature.com/articles/srep01376; Jennifer Valentino- DeVries et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), http://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.
[68] Lynch, *supra* note 35, at 6.
[69] *Id*.
[70] Hamed Aleaziz & Caroline Haskins, *DHS Authorities Are Buying Moment-by-Moment Geolocation Cell Phone Data to Track People*, Buzzfeed (Oct. 30, 2020, 6:19 PM), http://www.buzzfeednews.com/article/hamedaleaziz/ice- dhs-cell-phone-data-tracking-geolocation.
[71] 18 U.S.C. §§§ 2510(15), 2711(22), 2702(a).
[72] Shenkman et al., *supra* note 62, at 16. Notably, "in most cases where devices and apps record location information, it has been considered to be 'non-content' information." *Id*.
[73] *Carpenter*, 138 S. Ct. at 2217.
[74] Shenkman et al., *supra* note 62, at 18.

The constitutionality of this current arrangement where multiple forms of sensitive data are sold by data brokers to law enforcement is suspect. The lack of transparency, regulatory oversight and judicial scrutiny of this practice means that it will continue to grow unchecked, with "multiple agencies spending upwards of tens of millions of dollars on multi-year contracts" lacking any concern for the erosion of constitutionally guaranteed protections against unreasonable search and seizure.[75]

iii. Geofence Warrants

Geofence warrants, or "reverse location searches," are instances where law enforcement uses a warrant to acquire data directly from the entity that retains the data.[76] Geofencing allows police to "identify all devices that were in a given area during a given time period in the past."[77] After law enforcement receives judicial approval, a three-step process occurs. First, a geofence warrant is submitted to the entity holding the location data. The warrant provides a search radius expressed in location coordinates and a set duration of time, though it does not name a specific person, device, or account. For example, a request for "all implicated users [within the search parameters], their phone numbers and IP addresses" is sufficient.[78]

Second, once received, the subjected entity executes an indiscriminate search of *all* its databases that house user-account location information. The entity subject to the warrant then extracts the data specified with the given parameters and provides it to law enforcement. This means that in response to the initial request, detailed location information of individuals with no connection to the underlying criminal investigation is provided to law enforcement for analysis.

Third, in response to this initial dragnet, law enforcement returns with a narrowed request for information about particular users in that search radius.[79]

Geofence warrants are a potent example of how Big Data policing, in the absence of clearly defined judicial and legislative oversight, erodes constitutional protections from arbitrary and expansive searches.[80] In many cases, these warrants permit overly broad searches lacking the particularity or probable cause required for traditional warrants. Rather, they are "fishing expeditions" that involve "the very sort of general exploratory rummaging that the Fourth Amendment was intended to prohibit."[81] Additionally, the scale and frequency of the requests raises questions about the effectiveness of judicial oversight in the warrant approval process.

---

[75] *Id.* at 7.
[76] *See* Note, *Geofence Warrants and the Fourth* Amendment, 134 HARV. L. REV. 2508 (2021), https://harvardlawreview.org/2021/05/geofence-warrants-and-the-fourth-amendment. Google, for example, is a popular recipient of these requests, from June to Jan 2020 it received approximately 19,000 search warrants. *Id.*
[77] Lynch, *supra* note 35, at 3.
[78] Note, *supra* note 76, at 2515.
[79] *Id.*
[80] According to Google, from 2018 to 2020, 95.6 percent of requests came from state and local police. Lynch, *supra* note 35.
[81] Note, *supra* note 76, at 2513-14.

Judges have been known to approve multiple warrants in "a few minutes" and, often without "realizing the technical details or broad scope of the searches they are authorizing" because the warrant application consists of coordinates, not a visual map of the area to be searched.[82] Moreover, geofence warrants are an evolving practice, and police are using them to acquire more and more detailed information about users and their networked devices, beyond their location. For example, police are also requesting "keyword search history."[83]

No court has held that geofence warrants are categorically unconstitutional, and the use of these warrants by law enforcement is increasing.[84] Therefore, while it is possible to draft a geofence warrant with probable cause and sufficient particularity, there is recognition that without careful scrutiny "it is easy for a geofence warrant . . . to cross the threshold into unconstitutionality."[85] Recent case law indicates that the judiciary is split with regard to the dangers of geofencing. For example, the United States District Court for the Eastern District of Virginia held that the scope of a geofence warrant used to identify all devices in the area of a bank robbery, including the defendant's, "plainly violates the rights enshrined in the [Fourth] Amendment."[86] The judgment made clear that the three-step process of these warrants was not adequate and that even "anonymized location data—from innocent people—can reveal astonishing glimpses into individuals' private lives."[87]

This ruling marks an important step in adapting the Fourth Amendment to counterbalance Big Data policing more effectively. Still, the lack of judicial clarity and legislative oversight regarding geofence warrants, which are only increasing in their scope and sophistication, threatens constitutional protections against indiscriminate searches.

III. REORIENTING THE FOURTH AMENDMENT AND OTHER LEGISLATIVE SOLUTIONS TO BIG DATA POLICING

Fourth Amendment jurisprudence is "patchwork" and is "cobbled together" from inconsistent doctrines.[88] However, this characterization reflects the dynamic nature of the right to be free from unreasonable search and seizure, which is an important feature given the protections that it explicitly provides. The flexibility of Fourth Amendment jurisprudence regarding what constitutes a search or seizure is

---

[82] *See* Alfred Ng, *Google Is Giving Data to Police Based on Search Keywords, Court Docs Show*, CNET (Oct. 8, 2020, 4:21 PM), http://www.cnet.com/new/google-is-giving-data-to-police-based-on-search-keywords-court-docs- show (noting that Google provides ISP addresses to police requesting information on who searched for an arson victim's address).

[83] *Id.*

[84] Note, *supra* note 76, at 2529.

[85] *In re Search Warrant Application for Geofence Location Data Stored at Google Concerning An Arson Investigation*, 497 F. Supp. 3d 345 (N.D. Ill. 2020) (holding that geofence warrant satisfied Fourth Amendment probable cause and particularity requirements).

[86] *United States v. Chatrie*, 590 F. Supp. 3d 901, 905 (E.D. Va. Mar. 2022). *But see In the Matter of the Search of Information That is Stored At the Premises Controlled by Google LLC*, 579 F. Supp 3d 62, 82 (D.D.C. 2021) (holding that a geofence warrant sought by the government was not constitutionally overbroad in its scope).

[87] *Chatrie*, 590 F. Supp. 3d at 931 n.39.

[88] Kerr, *supra* note 7, at 481.

necessary in the face of constantly evolving government methods for executing searches and seizures. As "[n]ew [policing] practices arise . . . and begin to threaten the Fourth Amendment equilibrium, [they are] then addressed by judicial decisions that make the necessary adjustment."[89] Big data policing is the new practice to which the courts and legislatures must respond. Below I present three measures that the courts and legislatures can take in connection to halt the erosion of Fourth Amendment rights facilitated by Big Data policing.

a. Eliminating the Third-Party Doctrine

In *Carpenter*, Chief Justice Roberts's majority opinion, in dicta, expressed concern about the limited applicability of the third-party doctrine in light of modern information sharing practices.[90] However, the Court explicitly declined to abandon the doctrine beyond declaring that it did not apply to a customer's historical CSLI retained by a telecommunications provider.[91] The Court could have been more assertive and used *Carpenter* as the case to close the book on the third-party doctrine.[92] As it stands, the third-party doctrine remains an ill-suited method for assessing an individual's reasonable expectation of privacy over their digital information during a time "in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[93]

The third-party doctrine is anachronistic. Its rigid approach to information transfers does not take into consideration the reasonable expectations of privacy held by the public regarding their online activity and fails to acknowledge the reality that the voluntariness of this sharing is not a meaningful assumption of risk, especially "given how omnipresent and necessary technological disclosures are."[94] The mere fact that much of daily life is conducted digitally has not necessarily changed the public's attitude toward the privacy of their intimate digital information. Studies show that "a majority of people do not knowingly convey their locations information to cell phone providers and expect law enforcement to obtain a warrant before gathering information."[95] As stated, the Fourth Amendment is flexible in response to technological progress and changing societal attitudes about what information, activities, and behaviors the public holds a reasonable expectation of privacy.

---

[89] *Id.*
[90] *Carpenter*, 138 S. Ct. at 2219 ("There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers.").
[91] *Id.* at 2217.
[92] *See* Daniel Solove, Carpenter v. United States, *Cell Phone Location Records and the Third-Party Doctrine*, TEACHPRIVACY (July 1, 2018), https://teachprivacy.com/carpenter-v-united-states-cell-phone-location-records- and-the-third-party-doctrine/.
[93] *United States v. Jones*, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).
[94] Cristina Del Rosso & Carol M. Bast, *Protecting Online Privacy in the Digital Age:* Carpenter v. United States *and the Fourth Amendment's Third-Party Doctrine*, 28 CATH. U. J. L. & TECH. 89, 104 (2020), https://scholarship.law.edu/jlt/vol28/iss2/5.
[95] Harvey Gee, *Last Call for the Third-Party Doctrine In the Age After* Carpenter*?*, 26 B.U. J. SCI & TECH. L. 286, 299 (2020), https://www.bu.edu/jostl/files/2020/08/2-Gee.pdf.

The amount of granular information that is collected by third parties about an individual because of that individual's participation in modern society is immense.[96] Therefore, it is unreasonable to expect an individual to waive their expectation of privacy consciously, knowingly, intentionally, and voluntarily in every instance of digital interaction during which their information is collected. To the contrary, because of the information economy, individuals are pushed, prodded, incentivized, encouraged, and cajoled into sharing even more information in exchange for participation in the most basics of online activities. This information then becomes the source of warrantless Big Data policing, and law enforcement will continue to leverage such data unless told otherwise. While *Carpenter* might have narrowly limited the third-party doctrine, the Court needs to take a bold step toward rebalancing Fourth Amendment protections by abolishing the view that the "voluntary" sharing of information with a third-party in the digital context defeats the sharer's reasonable expectation of privacy in that information.

b. Adopting a Source-Based Test for When a Search Occurs

The Court should build on its reasonable expectation of police capabilities inquiry introduced in *Carpenter* and adopt a bright- line rule to establish when a search of digital information occurs. A bright-line rule supports the sound policy that police have clear knowledge about what activities they are permitted to engage in without a warrant and when a warrant is required. This bright-line rule would ask "whether any information revealed to the government was dependent or relied on use of a technology that *Carpenter* covers."[97] If so, then a warrant is needed.

While Fourth Amendment cases are fact and context specific, the courts should not rely on "difficult line drawing exercises" that attempt to assess, in a given context, whether so much information has been transferred from the individual to the government that a search has occurred.[98] Rather, Big Data policing methods should be treated as searches because their "fruits" (i.e., the digital information acquired) are categorically different from those of analogous pre-digital search methods.[99] In other words, digital records are different, and when they are created without meaningful voluntary choice while simultaneously revealing personal information, they should be covered under the Fourth Amendment. Under this framework, there are three steps that a court may take to assess whether a search has occurred.

First, determine whether the record subject to a search is a new type of record meaning that had it is not previously been available through pre-digital or conventional surveillance methods (e.g., website search history). This step underscores the intent of the Court in *Carpenter*, which is that Fourth Amendment protections extend to digital records and that digital records are different than their

[96] *See, e.g.*, Aliza Vigderman & Gabe Turner, *The Data Big Tech Companies Have on You*, security.org (Mar. 23, 2022), https://www.security.org/resources/data-tech-companies-have/.
[97] *Kerr*, *supra* note 17, at 28.
[98] *Id.* at 40.
[99] *Id*. at 42.

pre-digital analogues.[100] Because of this difference, a new approach is necessary to "best maintain the original balance [between Fourth Amendment rights and public safety goals] before the Internet age."[101]

Second, if the record is "new," its creation must not be voluntary. As argued in Part IV.A above, the digital age frustrates the logic of the third-party doctrine when so much important information is created as a by-product of daily life. Where in *Carpenter*, the Court found CSLI inescapable, so too are a variety of other automatically created non-content records.

Take, for example, email and its pre-digital analog of mail sent via the post office ("snail mail"). The exterior of an envelope in the mail, containing the "to" and "from" information, is considered publicly available metadata. The same applies for an email message with the added inclusion of the "subject" line at the top of the message. Collectively, this information is considered "envelope" data and is unprotected against warrantless searches for both mediums of communication, while the contents of both forms remain protected. However, because "digital is different," the metadata generated by an email message is more detailed and novel than that of a traditional envelope, and much of this metadata is created involuntarily.[102] Additionally, the government's capacity to use Big Data policing techniques to surveil communications metadata is significantly different than its pre-digital surveillance capabilities for snail mail. This capacity is amplified by the frequency with which individuals send email or internet messages and the length of time with which message information is stored by third parties.[103]

Third, if a record is "new" and involuntarily created, it is only protected if it reveals sufficiently private information. Involuntary or automatically generated records that reveal an intimate portrait of a person should be protected from warrantless searches. Therefore, whether it is autogenerated, real-time location information created by an individual's physical mobile telephone, or the detailed metadata of an internet message, both reveal intimate details to which individuals hold reasonable expectations of privacy.[104]

Adopting a test that provides a bright-line framework for Fourth Amendment searches would bring much needed clarity to law enforcement as they deploy rapidly evolving Big Data policing methods. Although the test would establish an expanded presumption of privacy in many digital records and could, thus, provide a safe harbor for illicit activities to be free from surveillance and investigation, such presumption is necessary to counterbalance the already pervasive surveillance capacities enabled by Big Data policing.

---

[100] *Id.* In *Carpenter*, the difference was between physical law enforcement surveillance and cell site location information.

[101] *Id*. at 19.

[102] For example, the specific accounts engaged in the communication, the platform used, the precise time when the messages were sent, non-content attachments, the size of communication etc.

[103] Kerr, *supra* note 17, at 43.

[104] This information may be used to "invade and chill associational freedoms." *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring); *see also* Kerr, *supra* note 17, at 45 ("This kind of transactional information would allow the government to gain a comprehensive picture of the persons associations and contacts akin to knowing their precise location.").

c. Legislative Solutions to Big Data Policing

Taking steps to shore-up protections against unreasonable, arbitrary, and expansive search and seizure practices does not have to wait for judicial action. Federal and state legislatures have enacted and should continue to enact laws that establish oversight mechanisms for Big Data policing techniques and methods. Developing regulations for Big Data policing must include the public's perspective, that the lawmaking process provides. Legislative efforts to tackle Big Data policing can be grouped into three categories: (1) moratoriums, bans, and restrictions on certain Big Data technologies and methods; (2) regulations for transparency and efficacy in law enforcement collection and use of Big Data; and (3) specific laws closing gaps in Fourth Amendment coverage that are currently exploited by Big Data policing.

The most aggressive regulatory action that, many municipalities and states have already taken, is to categorically ban the use of certain technologies by police.[105] The benefit of a moratorium or ban is clear: the erosion of civil liberties that results from the widespread adoption of Big Data policing methods with little judicial or legislative oversight is instantly halted. Predictive Policing Technology is particularly ripe for this ban. With a checkered history of accuracy in the major metropolitan areas in which it has been adopted, PPT is shown to cause the arbitrary surveillance of, and even detention of, innocent individuals. The risk to civil liberties is too high to adopt this technology, especially when the effectiveness of PPT is not entirely clear as there is limited transparency into the frequency of its use. As such, the technology should be banned until its trustworthiness can be proven. The burden of proof in such instances should be on law enforcement; there should not be a presumption of objectivity or reasonableness unless and until the technology is demonstrated to be unbiased.

Citizens have the right to know about the nature of the Big Data policing methods to which they are subjected. The current complexity and obscurity of many such methods undermines the legitimacy of their application. Without sufficient transparency and efficacy controls, citizens and lawmakers cannot know whether the Big Data methods are accurate or even whether they work as advertised. Therefore, lawmakers should institute robust transparency regulations for Big Data policing. Such regulations should include provisions to illuminate the contractual relationships of law enforcement entities with third parties who provide the technology or from whom police acquire information. Information transparency is critical as well. If Big Data policing tools are only as good as the information they analyze, it is imperative that this information be publicly scrutinized and vetted. Any application of Big Data policing must make clear the specific information that technology uses and how it uses it to generate insights. In turn, the sources of information and the information itself should be independently audited prior to deployment to ensure accuracy and non-bias. Finally, law enforcement agencies

[105] Facial recognition technology is currently banned in at least 13 municipalities, with bills in many state legislatures advocating for additional restrictions or bans. *See* Ban Facial Recognition, https://www.banfacialrecognition.com/map/ (last visited April 29, 2022).

who use Big Data policing methods should be required to provide routine reports about their effectiveness and frequency of use. If the technology does not produce effective results, or is infrequently used, that should be communicated to lawmakers who can then address these deficiencies.

Certain Big Data policing practices, like the purchasing of third-party collected data for down-stream analysis or geofence warrants, reside in a Fourth Amendment gray zone. They are currently considered lawful activities, despite the concerns they raise about particularity and reasonable suspicion in the context of a search. Lawmakers should pass legislation that either bans transactions between third-party data brokers and law enforcement or severely restricts and regulates such transactions. There should not be a scenario where the government is able to purchase data that it would otherwise need a warrant to acquire. At the federal level, for example, bills such as "The Fourth Amendment is Not for Sale Act" are an important step in building a stronger federal regulatory apparatus for Big Data policing practices.[106] At the state level, measures such as requiring data brokers to register with the Secretary of State provide much needed transparency.[107] Similarly, with regard to geofence warrants, steps can be taken to formalize the shadowy process of dragnet law enforcement search requests to companies like Google. As a private entity, Google has taken steps to challenge the expansiveness of geofence requests, but it cannot be expected to shoulder the burden of protecting this information unilaterally. Individual states can act to require law enforcement to be more particular with their initial search requests or ban the practice entirely. However, because of the interstate nature of location data, a comprehensive federal regulatory scheme should be prioritized. Rather than relying on court challenges to geofence warrants to provide clarity on this practice, legislatures must be proactive in developing geofence warrant guidelines.

CONCLUSION

Each time a new technology expanded law enforcement capabilities, the Fourth Amendment readjusts to counterbalance those enhanced capabilities and affirm the rights of people. In the face of Big Data policing, the Fourth Amendment must once again be reinterpreted to effectively protect individuals in the modern information economy. Big Data provides immense opportunities for law enforcement to better serve and ensure public safety; but, the risks to individual privacy are equally high. To counterbalance this danger, three things must happen. First, our understanding of the reasonable expectation of privacy over certain information under the Fourth Amendment must expand through the removal of the third-party doctrine, because the doctrine is anachronistic considering modern information collection practices.

Second, the courts must adopt a clearer test for determining when a search has occurred. This test should be a bright-line framework that assesses: (1) the novelty of the information subject to a search; (2) the voluntariness of that

[106] Sarkesian & Singh, *supra* note 62, at 3.
[107] For example, Vermont requires data brokers to annually register. *See* Vermont Data Broker Regulation Act, 9 V.S.A. §§ 2430, 2433, 2446 (2021).

information sharing; and (3) the intimacy of the information shared. Third and finally, legislatures must address the areas where Fourth Amendment protection remains weak. through legislation Where appropriate, the adoption of Big Data policing techniques should be halted or, alternatively, stringently regulated to maximize transparency, accountability, and trust by the public. Taken together, these efforts will allow the potential of Big Data to be realized without it costing us our privacy rights.