UNIVERSITY OF PITTSBURGH LAW REVIEW
Vol. 85 ● Fall 2023

ARTICLES

"VOLUNTEER" SEARCHES

Christopher Slobogin

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.985
http://lawreview.law.pitt.edu

ARTICLES

"VOLUNTEER" SEARCHES

Christopher Slobogin*

ABSTRACT

In this age of digitization, law enforcement can obtain much of the information it used to seek through physical searches and seizures or subpoenas simply by asking or paying private companies for access to their databases. Unless the Fourth Amendment is broadly construed, much of this modern-day information gathering may be immune from the warrant requirement and other Fourth Amendment restrictions. While most of the discussion about the proper threshold of Fourth Amendment protection has focused on the definition of the word "search," of equal if not greater importance is the scope of the state action doctrine requiring government involvement in the search. This Article argues that, even when their actions are putatively "voluntary," private companies that act as government abettors, surrogates or informants should be brought within the ambit of the Fourth Amendment. Otherwise, law enforcement will often be able to work an end run around the burgeoning movement to expand the scope of search and seizure law.

* Milton Underwood Professor of Law, Vanderbilt University. Parts of this Article are from Chapter 8 of my book, CHRISTOPHER SLOBOGIN, VIRTUAL SEARCHES: REGULATING THE COVERT WORLD OF TECHNOLOGICAL POLICING (2022). I would like to thank workshop participants at the July, 2023 Crimfest conference, as well as Michael Mannheimer, Rudy Cooper, Paul Edelman and Wayne Logan for their comments on this Article.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.985
http://lawreview.law.pitt.edu

INTRODUCTION

To trigger Fourth Amendment protection, an action must be both a "search" or a "seizure" *and* the result of "state action."[1] Largely because of technology, the first component of the Fourth Amendment's scope has been in ferment for over two decades,[2] with the most prominent decision in this vein coming from the Supreme Court in its 2018 opinion in *Carpenter v. United States*.[3] There, the Court held that when police obtained the defendant's cell site location information ("CSLI") from his common carrier they conducted a "search" requiring a warrant,[4] despite caselaw from the 1970s adopting what came to be called the "third-party doctrine"—the idea that we do not have a reasonable expectation of privacy in information surrendered to a third party because we assume the risk the third party will turn it over to the government.[5] *Carpenter*'s conclusion that we do not assume that risk when it comes to CSLI could apply to many other government efforts to obtain records from private entities that obtain and store our personal information. Indeed, commentators have asserted that "*Carpenter* marks a sea change in Fourth Amendment analysis of privacy claims in digital data held in third-party hands, making viable a range of expectations of privacy that the law was ill-suited to recognize previously."[6]

A little noticed fact, however, is that *Carpenter*'s impact—and the impact of the Fourth Amendment more generally—might easily dissipate if the second component of the amendment's scope is defined narrowly. For an intrusion to trigger Fourth Amendment protection it must not only be a "search" or a "seizure"; it must also be carried out at the behest of the government. That is because the Fourth

[1] *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984).

[2] *See* Kyllo v. United States, 533 U.S. 27 (2001) (using a thermal imager to measure temperature in a house is a search); United States v. Jones, 565 U.S. 400 (2012) (using a GPS device to track a car is a search); Riley v. California, 569 U.S. 373 (2013) (search of cellphone incident to arrest requires warrant).

[3] Carpenter v. United States, 138 S. Ct. 2206 (2018).

[4] *Id.* at 2223 ("In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection.").

[5] *See* United States v. Miller, 425 U.S. 435, 443 (1976) (holding that obtaining Miller's bank records from his bank was not a search because Miller had "take[n] the risk, in revealing his affairs to another, that the information [would] be conveyed by that person to the Government."); Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (holding that the government's requisition of Smith's phone records from his phone company was not a search because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

[6] Natalie Ram, *Genetic Privacy After* Carpenter, 105 VA. L. REV. 1357, 1367 (2019).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.985
http://lawreview.law.pitt.edu

Amendment (and the other rights in the Bill of Rights) regulate actions only of the state, not of private individuals.[7] If one's privacy is invaded by another citizen, a claim in tort may exist. But one cannot make a constitutional claim unless the private party is "an agent or an instrument of the Government[.]"[8] This "state action" requirement is ironclad constitutional law.

At the same time, a private party does not have to be acting under police orders to be considered a state actor. Indeed, the Supreme Court has found state action even when there is no explicit direction by the government. *Skinner v. Railway Ass'n* involved a federal regulation governing drug testing by private railway companies.[9] One part of the law required testing of railway workers directly involved in a "major train accident," which was clearly state action.[10] But the regulation left to the companies' discretion whether to test workers who were involved in a "reportable accident or incident" and workers who violated speeding or other safety rules.[11] Despite the absence of a direct government command in the latter situations, the Court held that the Fourth Amendment applied to the *entire* drug-testing program.[12] The relevant regulations, the Court pointed out, provided that the testing was for the purpose of "promoting the public safety" and that railways could not act in a way that was inconsistent with that purpose by, for instance, foregoing testing on the basis of a collective bargaining agreement.[13] Furthermore, the regulations made clear that the Federal Railroad Administration was entitled to the results of any tests administered.[14] Thus, the Court stated, the government had "removed all legal barriers to testing" and "made plain not only its strong preference for testing, but also its desire to share the fruits of such intrusions[,]" factors the Court considered "clear

[7] Burdeau v. McDowell, 256 U.S. 465, 475 (1921) (holding that evidence obtained by private parties through a burglary did not implicate the Fourth Amendment because "whatever wrong was done was the act of individuals in taking the property of another."). *See* discussion of *Burdeau infra* notes 120–22.

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

[9] *Id.* at 606.

[10] *Id.* at 609.

[11] *Id.* at 611.

[12] *Id.* at 617.

[13] *Id.* at 603, 615.

[14] *Id.* at 615 (noting that the regulations "confer[red] upon the [federal government] the right to receive certain biological samples and test results procured by railroads").

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.985
http://lawreview.law.pitt.edu

indices of the Government's encouragement, endorsement and participation . . . suffic[ient] to implicate the Fourth Amendment."[15]

So, when a third party rather than a government agent is carrying out the search or seizure, after *Skinner* the scope of the Fourth Amendment depends on whether the government has expressed a "strong preference" that it be conducted and that its results be provided the government. More generally, the focus is on whether there are "clear indices" of the government's "encouragement, endorsement, and participation." The lower courts have added some gloss to *Skinner*'s language. For instance, the First Circuit Court of Appeals has held that whether a private actor becomes a state actor depends on "(1) the extent of the government's role in instigating or participating in the search; (2) its intent and the degree of control it exercises over the search and the private party; [and] (3) the extent to which the private party aims primarily to help the government or to serve its own interests."[16] The meaning of these various phrases is the topic of this Article.

In the age of digitization, this issue may now be the most consequential quandary in Fourth Amendment jurisprudence. If, as is currently the case, the government can obtain personal information simply by asking or paying for any data about wrongdoing that private actors can access, it could routinely resort to that ruse rather than worry about restrictions that cases like *Carpenter* might impose on state actors. The usefulness of this potential workaround is much greater than it was fifty or even twenty years ago because technology has greatly enhanced the ability of private companies to acquire mountains of information about each of us; indeed, many companies are set up solely or principally with that goal in mind.[17] Because law enforcement can acquire these detailed accounts of our personal activities from private companies without triggering state action, the Fourth Amendment is a nullity in an increasing number of cases. Ironically, *Carpenter* may exacerbate the situation, because the more courts restrict direct government searches through curtailing the third-party doctrine, the fewer compunctions law enforcement will have about relying on the private market to do its work.

Expansion of the state action concept to cover these developments would not mean that every private action that is meant to help the government nab criminals is

[15] *Id.* at 615–16.

[16] United States v. D'Andrea, 648 F.3d 1, 10 (1st Cir. 2011).

[17] Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1338 (2012) (describing the "coming world" in which "police outsource [almost all] surveillance to private third parties").

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.985
http://lawreview.law.pitt.edu

governed by the Constitution. Private citizens should not be discouraged from bringing to the government evidence of crime they come upon; as the Supreme Court has stated, "it is no part of the policy underlying the Fourth and Fourteenth Amendments to discourage citizens from aiding to the utmost of their ability in the apprehension of criminals."[18] But a distinction should be made between commercial and individual informants. Government should not incentivize private companies to pry into people's lives. Corporate vigilantism not only differs from individual vigilantism in scope, but also breaches fiduciary duties, without the compensating justification for volunteering information that individuals, with more robust autonomy rights, can advance.

The following discussion is based on two assumptions. The first assumption (a big one) is that *Carpenter* eliminates the third-party doctrine in every case in which the government obtains records from a third-party recordholder, thus mooting the "search and seizure" issue. The second assumption is that state action occurs any time the government compels a third party to hand over information, either directly through court orders or indirectly by, for instance, abrogating immunity from liability if the third party does not carry out the searches the government wants.[19] Those assumptions allow us to focus on whether the Fourth Amendment is implicated by third-party conduct induced through more subtle means. The following discussion considers four scenarios—the first three focused on business entities and the fourth on private individuals—that involve descending levels of government "instigation" and "control."

The first scenario involves what I call "third-party abettors." These are private companies that, upon government request, willingly surrender data about their customers knowing it will facilitate government investigations of them. In this situation, the government seeks information already acquired by the third party in the course of its ordinary business. The Article then moves to "third-party surrogates," private parties that collect information for the government for profit. In this scenario the private party, at the government's bidding (literally), acquires data which it then voluntarily surrenders to the government. Finally, the Article looks at institutional and individual "informants" who, in the *absence* of a government request, relay information they believe incriminates a particular person. Here the Article makes a distinction between institutional and individual third parties.

[18] Coolidge v. New Hampshire, 403 U.S. 443, 488 (1971).

[19] *See* Joseph Zabel, *Public Surveillance Through Private Eyes: The Case of the Earn It Act and the Fourth Amendment*, 2020 U. ILL. L. REV. ONLINE 167 (analyzing whether state action is implicated by a federal statute withholding immunity from civil and criminal liability for internet service providers that do not adhere to "best practices" aimed at identifying the transfer of child sexual abuse material).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.985
http://lawreview.law.pitt.edu

The Article concludes that the first three of these scenarios implicate the Fourth Amendment, albeit with different consequences to be explored below. Government acceptance of data volunteered by *individual* informants is not state action unless the government has directed them to obtain it. But various characteristics of *institutions* should trigger Fourth Amendment oversight of their disclosures to the government even when unsolicited.

I. THIRD-PARTY ABETTORS: COMMUNICATIONS PROVIDERS

Third-party abettors collect information for their own purposes but willingly surrender it to the government upon request, even in the absence of a warrant or subpoena. Here the focus will be on institutional abettors; individual abettors are discussed in Part IV. The experience of common carriers—companies that maintain communications networks like AT&T, Verizon, and Quest—is a particularly interesting illustration of the institutional third-party abettor scenario. At one time these companies enthusiastically aided law enforcement efforts. Today, they are much more leery of government requests for aid.

Shortly after the assaults on 9/11, President George W. Bush issued a "highly classified presidential authorization" finding that the attacks constituted an "extraordinary emergency" that justified enhanced surveillance.[20] Specifically, the authorization allowed the National Security Agency to collect, without a warrant, the content and metadata of a wide range of communications between people outside and inside the country and between people inside the country who were not U.S. citizens.[21] Through Stellar Wind, the resulting program, the government leaned on AT&T, Verizon, and BellSouth—and eventually other companies as well—to forward routing information about the phone and email communications of their customers to the National Security Agency ("NSA").[22] In 2011, AT&T alone was sending to the NSA the metadata associated with about 1.1 billion domestic calls per

[20] *See* James Risen & Eric Lichtblau, *Bush Secretly Lifted Some Limits on Spying in U.S. After 9/11, Officials Say*, N.Y. TIMES (Dec. 15, 2005), http://www.nytimes.com/2005/12/15/politics/15cnd-program.html?pagewanted=all.

[21] *Id.*; *see also DNI Announces the Declassification of the Existence of Collection Activities Authorized by President George W. Bush Shortly After the Attacks of September 11, 2001*, IC ON THE RECORD (Dec. 21, 2013), http://icontherecord.tumblr.com/post/70683717031/dni-announces-the-declassification-of-the-existence.

[22] Barton Gellman, *U.S. Surveillance Architecture Includes Collection of Reveal Internet, Phone Metadata*, WASH. POST (June 15, 2013), https://www.washingtonpost.com/investigations/us-surveillance-architecture-includes-collection-of-revealing-internet-phone-metadata/2013/06/15/e9bf004a-d511-11e2-b05f-3ea3f0e7bb5a_story.html.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.985
http://lawreview.law.pitt.edu

day, supposedly after sifting through them to make sure they met the presidential guidelines (although the Office of the Inspector General later found the records were simply surrendered in bulk).[23]

Under Fourth Amendment jurisprudence at the time, the argument was strong that, despite its scope, this collection of metadata was not a search. In 1979, the Supreme Court had held, in *Smith v. Maryland*, that accessing a person's phone log from their phone company did not implicate the Fourth Amendment.[24] The Court asserted that people should know phone companies keep records of numbers dialed and also assume the risk the company will turn that information over to the government; therefore, the Court reasoned, any expectation of privacy in the phone numbers they dial is unreasonable.[25] Some lower courts relied on *Smith* in holding that the metadata program did not involve a Fourth Amendment search or seizure.[26]

But 40 years after *Smith*, the Court's decision in *Carpenter* repudiated its premise. *Carpenter* held that the government engaged in a Fourth Amendment search when it requisitioned several days of cell site location information from Carpenter's common carrier.[27] The decision did not overrule *Smith*, but rather distinguished it by noting that "[t]here is a world of difference between the limited types of personal information addressed in *Smith* . . . and the exhaustive chronicle of location information casually collected by wireless carriers today[,]"[28] a distinction that clearly applies to the all-encompassing NSA metadata program as well. Even more importantly (and even more difficult to square with *Smith*), the Court stated that "[c]ell phone location information is not truly 'shared'" as one normally understands the term because cell phones and the services they provide are "indispensable to participation in modern society."[29] In short, after *Carpenter*, one has a strong argument that the fact that people "knew" the metadata acquired through Stellar

[23] Julia Angwin, Jeff Larson, Charlie Savage & James Risen, *NSA's Spying Relies on AT & T's "Extreme Willingness to Help,"* PROPUBLICA (Aug. 15, 2015), https://www.propublica.org/article/nsa-spying-relies-on-atts-extreme-willingness-to-help.

[24] 442 U.S. 735 (1979).

[25] *Id.* at 743–44.

[26] *See* ACLU v. Clapper, 959 F. Supp. 2d 724, 749–52 (S.D.N.Y. 2013) (relying on Smith v. Maryland, 442 U.S. 735 (1979)).

[27] Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018).

[28] *Id.* at 2219.

[29] *Id.* at 2220.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.985
http://lawreview.law.pitt.edu

Wind was held by third-party common carriers should not diminish their expectation that their communication information is protected by the Fourth Amendment.

However, that conclusion by itself is not enough to bring Stellar Wind within the ambit of the Fourth Amendment. It would also need to be established that government efforts to obtain information from AT&T and the common carriers involved state action. The argument that it did not is twofold. First, the government did not "encourage" the common carriers to obtain the metadata; that data had already been obtained through their ordinary course of business. Second, while the government did request the metadata, the companies seemed glad to provide it under the circumstances. According to a *New York Times* article in 2015, the companies "voluntarily" provided foreign-to-foreign metadata, and even metadata involving a domestic party was proffered through a "partnership" arrangement that was "collaborative."[30]

That language notwithstanding, the government's request for information should have been considered state action. The presidential authorization for Stellar Wind made clear the government wanted metadata and specified the type of metadata it desired. Further, the government paid the companies handsomely for it.[31] Here, in the words of *Skinner*, the government clearly expressed a "strong preference" for the metadata; it also encouraged its retention, organization and transfer to the NSA in a way that would ensure its usefulness. Using the First Circuit's formulation, the government "instigated" and "controlled" the transfer of the metadata from the companies to the government.

If Stellar Wind were determined to involve state action (and a search and seizure), the implications could be significant. In other work, I have argued that special Fourth Amendment rules apply when—as occurred with Stellar Wind (and occurs with a wide array of other police techniques such as CCTV systems, border and traffic checkpoints, and drug testing)—the government sets up a program aimed at the general population rather than at specific persons.[32] A warrant is not required and in fact could not be issued in these settings, because at the time of the search or seizure no suspicion exists with respect to any particular individual. However, in such situations the Fourth Amendment still requires an "adequate substitute for a

[30] Julia Angwin, Charlie Savage, Jeff Larson, Henrik Moltke, Laura Poitras & James Risen, *AT&T Helped U.S. Spy on Internet on a Vast Scale*, N.Y. TIMES (Aug. 15, 2015), https://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html?_r=0.

[31] *Id.*

[32] Christopher Slobogin, *Policing as Administration*, 165 U. PA. L. REV. 91 (2016).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.985
http://lawreview.law.pitt.edu

warrant" that provides analogous protection against arbitrariness.[33] That substitute, I argue, can come (and, in fact, must come) from the restrictions set out in administrative procedure acts.[34] Under those acts, which exist in every jurisdiction,[35] an administrative agency proposing a policy of "general or particular applicability and future effect" that affects "the rights and obligations of citizens" must engage in a rulemaking process that establishes guidelines for how a legislative delegation is to be carried out.[36] These rules are subject to notice and comment from the general public and to hard-look review from the courts to ensure they rationally relate to the program's stated objectives and are implemented even-handedly.[37] Most importantly, the police agency should not be able to pursue the program at all in the absence of legislative authorization setting forth an "intelligible principle" governing the purpose and scope of the program.[38]

Under this legal regime, Congress should have authorized Stellar Wind's metadata program and either its statute or an NSA regulation should have identified the type of data sought and described its legitimate uses, how long it could be retained, and who could access it and when. Specific techniques that might help terrorists and others evade detection would not have to be revealed,[39] but there should

---

[33] *See* Donovan v. Dewey, 452 U.S. 594, 603–04 (1981) (holding that, although coal companies cannot demand that inspections be authorized by warrant, they are still entitled to demand "a constitutionally adequate substitute for a warrant," such as a statute that defines the scope and timing of the inspections and the precise standards by which the business owner must abide).

[34] Slobogin, *supra* note 32, at 97 (arguing that, under administrative law principles, policing programs are not legitimate in the absence of "authorizing legislation, policymaking procedures that involve community input, a written product with a written rationale, and strictures on implementation to ensure even application both across jurisdictions and within a particular application of the program.").

[35] Although many municipalities, in which most policing occurs, are not governed by administrative procedure acts, they enforce laws of the federal and state governments, which do have such acts. *See* Slobogin, *supra* note 32, at 135.

[36] 9 U.S.C. § 551(4); Davidson v. Glickman, 169 F.3d 996, 999 (5th Cir. 1999) ("Interpretive rules state what the administrative officer thinks the statute or regulation means . . . while legislative rules 'affect[] individual rights and obligations' and create law.").

[37] 5 U.S.C. § 553(b) (requiring publication of proposed rules and providing for notice and comment by "interested persons").

[38] BERNARD SCHWARTZ, ADMIN. L. § 4.4, at 171 (3d ed. 1991) ("The statute is the source of agency authority as well as of its limits. If an agency act is within the statutory limits (or vires), its action is valid; if it is outside them (or ultra vires), it is invalid.").

[39] *See* 5 U.S.C. § 552(b)(7)(E) (exempting from disclosure "techniques and procedures for law enforcement investigations or prosecutions, or . . . guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.").

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.985
http://lawreview.law.pitt.edu

have been democratic debate about the program through the legislative process and the notice and comment procedure. Further, courts should have ensured that the resulting regulations were consistent with the purpose and scope of Congress' delegation and that they were implemented in a neutral fashion.

In fact, something along these lines did occur when Congress passed the USA FREEDOM Act fourteen years *after* the metadata program began.[40] Rather than endorse the NSA's bulk collection program, the statute ended it, replacing it with a system that required that the records be maintained by the common carriers.[41] Today, under the statute and subsequently promulgated regulations the government may access only those records that satisfy a "specific selection term" that "specifically identifies a person, account, address, or personal device" and that limits, "to the greatest extent reasonably practicable, the scope of tangible things sought."[42] The NSA must convince the Foreign Intelligence Surveillance Court that there are reasonable grounds to believe the proposed search will obtain information relevant to an investigation that has been authorized by a high-level official and that there is a reasonable articulable suspicion that the specific selection term is associated with a foreign agent involved in international terrorism.[43]

Although Congress ultimately did the right thing, the USA Freedom Act should have preceded initiation of the metadata program, not the other way around. Furthermore, it is likely Congress acted less out of a desire to adhere to administrative law principles or the Fourth Amendment generally and more as a response to the revelations of Edward Snowden. In 2013, Snowden's release of classified documents exposed the scope of the bulk collection program as well as of a number of other national security programs, including PRISM, which compelled common carriers to send the NSA any communications sent to or from a specified selector such as an email address or a phone number.[44] Had his disclosures and the ensuing public uproar not occurred, the USA FREEDOM Act likely would never have been passed.

---

[40] 50 U.S.C. § 1861 *et seq.*

[41] *See id.*

[42] *Id.* at § 1861(4)(A).

[43] *Id.* § 1861(k)(4)(A)(i).

[44] Siobhan Gorman & Jennifer Valentino-DeVries, *New Details Show Broader NSA Surveillance Reach*, WALL ST. J. (Aug. 20, 2013), https://www.wsj.com/articles/SB10001424127887324108204579022874091732470.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.985
http://lawreview.law.pitt.edu

Fortunately, however, the Snowden affair has made it more likely that future Stellar Wind-type efforts, if they are to succeed, will *have* to involve state action—and thus, under the foregoing analysis, authorizing legislation as well. The reaction to Snowden's disclosures from an outraged public has changed the nature of government–private sector "collaboration" going forward. No longer are common carriers, concerned about consumer ire, as eager to assist the government in its investigative endeavors.[45] Other companies have become equally circumspect. These days entities such as Google, Apple, and Ancestry.com are likely to resist rather than comply with law enforcement requests for information.[46] Alan Rozenshtein has documented how communications enterprises are now more likely to engage in class action litigation about surveillance, publish "transparency reports" about the number of surveillance requests they receive, construct privacy-enhancing architecture (such as end-to-end encryption), lobby the government for more surveillance restrictions (as occurred with the FREEDOM Act), and lobby other government agencies such as the Federal Communications Commission and the Federal Trade Commission to battle their law enforcement counterparts over issues such as Department of Justice access to accounts held by privacy-conscious foreigners.[47] The type of "voluntary" cooperation between communications providers and the government that existed immediately after 9/11—and that characterized pre-9/11 programs such as SHAMROCK (which for decades until its exposure in the mid-1970s provided the government with all international telegraph communications)[48]—may be a thing of the past.

---

[45] *See* Yan Zhu, *Security Experts Call on Tech Companies to Defend Against Surveillance*, ELEC. FRONTIER FOUND. (Feb. 26, 2014), https://www.eff.org/deeplinks/2014/02/open-letter-to-tech-companies (noting that "trust in technology companies has been badly shaken" in the wake of the Snowden disclosures); *see also* Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, N.Y. TIMES (Mar. 21, 2014), https://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html.

[46] *See, e.g.*, Tom Brant, *Google Resists Warrant for Data in Minnesota Fraud Case*, ENTREPRENEUR (Mar. 20, 2017), https://www.entrepreneur.com/business-news/google-resists-warrant-for-data-in-minnesota-fraud-case/290863 (reporting that Google resisted a warrant seeking information on people who search for victim's name); Peter Aldhous, *A Court Tried To Force Ancestry.com to Open Up Its DNA Databased to Police. The Company Said No*, BUZZFEED NEWS (Feb. 3, 2020), https://www.buzzfeednews.com/article/peteraldhous/ancestry-dna-database-search-warrant (reporting Ancestry.com's resistance to police use of DNA databases).

[47] Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99 (2018).

[48] S. REP. NO. 94-755S. Rep. No. 94–755, bk. 3, at 765, 767–69, 771, 776 (1976).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.985
http://lawreview.law.pitt.edu

That does not mean, however, that there are not plenty of other companies willing to lend a helping hand to law enforcement—if they can make a profit.

II. THIRD-PARTY SURROGATES: DATA BROKERS

The information government obtains from communications providers such as Google and AT&T is already collected by those companies as part of their business model. In contrast, many other companies aim to acquire information for the precise purpose of selling it to law enforcement. For instance, at one time a company called Geofeedia, using information it obtained from scraping Instagram, Facebook, and Twitter posts and the locations from which they originated, claimed to help over 500 police departments predict and monitor "events" ranging from gang activities to political and union protests.[49] After this surveillance was exposed by the American Civil Liberties Union ("ACLU") in 2016, Instagram and Facebook purportedly stopped providing Geofeedia their content.[50] But other companies such as Palantir,[51] Dataminr,[52] Fusus,[53] Fog Reveal,[54] and Hunchlab,[55] claim to provide similar types of information about hot spots, hot people, or hot events to the police. Dataminr, for instance, relayed tweets about the George Floyd and Black Lives Matter protests to the police,[56] and Fog Reveal allows police to browse cellphone data.[57]

---

[49] Ali Winston, *Oakland Cops Quietly Acquired Social Media Surveillance Tool*, E. BAY EXPRESS (Apr. 13, 2016), https://eastbayexpress.com/oakland-cops-quietly-acquired-social-media-surveillance-tool-2-1.

[50] Matt Cagle, *Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color*, ACLU N. CALIF (Oct. 11, 2016), https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target.

[51] PALANTIR, https://www.palantir.com (last visited Oct. 10, 2023).

[52] DATAMINR, https://www.dataminr.com (last visited Oct. 10, 2023).

[53] FUSUS, https://www.fusus.com (last visited Oct. 10, 2023).

[54] Will Greenberg, *Fog Revealed: A Guided Tour of How Cops Can Browse Your Location Data*, ELEC. FRONTIER FOUND. (Aug. 31, 2022), https://www.eff.org/deeplinks/2022/08/fog-revealed-guided-tour-how-cops-can-browse-your-location-data#:~:text=Conclusions,went%20during%20other%20time%20periods.

[55] SHOTSPOTTER, https://www.shotspotter.com/law-enforcement/patrol-management/?src=hunchlab.com (last visited Oct. 11, 2023).

[56] Sam Biddle, *Police Surveilled George Floyd Protest with Help From Twitter-Affiliated Startup Dataminr*, THE INTERCEPT (July 9, 2020), https://theintercept.com/2020/07/09/twitter-dataminr-police-spy-surveillance-black-lives-matter-protests.

[57] Greenberg, *supra* note 54.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.985
http://lawreview.law.pitt.edu

While these companies cater primarily to the police, companies such as Acxiom,[58] LexisNexis,[59] and Oracle,[60] seek a wider consumer base and aggregate a much larger array of records—including data generated from retail purchases, internet surfing, and financial transactions, as well as from "smart" devices in cars, medical apps, and home appliances that are sometimes referred to as the "Internet of Things."[61] Acxiom, for instance, claims to have acquired, on each of more than 700 million people, over 1,500 data points, which can provide "insight into your psychological makeup to fit you into hundreds of refined consumer categories, estimating, for example, how likely you are to pay cash for a new Korean vehicle."[62] Information this granular can be very useful to law enforcement, which is why these companies have multi-million contracts with numerous government agencies.[63] The practice has become so common at the federal level that even the agencies themselves think more restrictions are necessary.[64]

The huge increase in government reliance on private data brings several dangers. First, of course, the potential for unnecessary privacy invasions increases dramatically; the specter of "digital dossiers" on everyone is more real than ever

[58] ACXIOM, https://www.acxiom.com (last visited Oct. 11, 2023).

[59] LEXISNEXIS, https://risk.lexisnexis.com (last visited Oct. 11, 2023).

[60] ORACLE, https://www.oracle.com (last visited Oct. 11, 2023).

[61] *See* Jamie Lee Williams, *Privacy in the Age of the Internet of Things*, 41 HUM. RTS. 14, 14 (2016) (stating that "[t]he 'Internet of Things' is a loosely defined term referring to a future in which everyday objects have built-in sensors and network connectivity, allowing them to send and receive data on their own—i.e., without human-to-human or human-to-computer interaction.").

[62] Alex Kozinski & Mihailis E. Diamantis, *An Eerie Feeling of Déjà Vu: From Soviet Snitches to Angry Birds*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 420, 423 (David Gray & Stephen Henderson eds., 2017) [hereinafter CAMBRIDGE BOOK OF SURVEILLANCE].

[63] *Id.* at 424 (reporting a $56 billion contract between the U.S. government and Acxiom). *See also* Garance Burke & Jason Dearen, *Tech Tool Offers Police "Mass Surveillance on a Budget*," AP NEWS (Sept. 2, 2022), https://apnews.com/article/technology-police-government-surveillance-d395409ef5a8c6c3f6 cdab5b1d0e27ef; Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, WALL ST. J. (Feb. 7, 2020), https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600.

[64] The report can be found in a link provided in Andrew Crocker, *Even the Government Thinks It Should Stop Buying Corporate Surveillance Data*, ELEC. FRONTIER FOUND. (July 14, 2023), https://lawprofessors.typepad.com/crimprof_blog/2023/07/even-the-government-thinks-it-should-stop-buying-corporate-surveillance-data.html.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.985
http://lawreview.law.pitt.edu

before.[65] Less obviously, as Andrew Ferguson has detailed, police departments can become dependent on private companies to do their jobs, which in turn can mean the companies will come to dominate decisions about the types of information to collect and the way it is inputted, organized, analyzed, and corrected.[66] Concomitantly, departments might have great difficulty changing vendors once they invest money and organizational resources integrating them into departmental decision-making.[67] Unless oversight is extensive, data error, data bias, and data incompatibility with existing government databases could become more difficult to correct.[68]

Ferguson points out that, although the Federal Trade Commission has made some effort to restrict aspects of private data collection, no overarching statutory scheme provides a basis for regulating the situation. As he summarizes it, "federal laws targeting the national problem of data collection, aggregation and use remain weak. . . . The current reality is wide-scale, growing big data collection without commensurate legal regulation."[69] And there is even less law regarding police use of collected information. Although a bill entitled The Fourth Amendment Is Not For Sale Act has languished in Congress for some time,[70] existing federal statutes exempt

[65] The phrase "digital dossier" comes from Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1086 (2002).

[66] Andrew Ferguson, *Big Data Surveillance: The Convergence of Big Data and Law Enforcement*, *in* THE CAMBRIDGE BOOK OF SURVEILLANCE LAW 171, 193.

[67] *Id.*; *see also* Elizabeth Joh & Thomas Joo, *The Harms of Police Surveillance Technology Monopolies*, 99 DEN. L. REV. F. 1, 2–3 (Apr. 27, 2021) (pointing out that once police departments have decided to buy technology from a private company, they tend to stick with the company because of the sunk costs and noting that "if a single company should come to dominate the market for [policing] platforms . . . [it will] effectively control the design, access, and availability of multiple police surveillance technologies" and thus "gain enormous power over basic questions in democratic policing.").

[68] Ferguson, *supra* note 66, at 191.

[69] *Compare id.* at 181, *with* Hannah Ruschemeier, *Data Brokers and European Digital Legislation*, EUR. DATA PROT. L. REV. 9 (2023), https://ssrn.com/abstract=4521470.

[70] *See Coalition Calls for Congressional Hearings on the Fourth Amendment is Not For Sale Act*, ACLU (Jan. 26, 2022), www.aclu.org/letter/coalition-calls-congressional-hearings-fourth-amendment-not-sale-act. The bill would prohibit law enforcement and national security agencies from buying the "contents of communications" or "geolocation information." *Id.* In July, 2023, a similar bill made it out of the House Judiciary Committee. Tim Cushing, *Bill Limiting Data Broker Sales to Law Enforcement Moves Forward*, TECHDIRT (July 21, 2022), https://www.techdirt.com/2023/07/21/wyden-bill-targeting-data-broker-sales-to-law-enforcement-passes-in-the-house.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.985
http://lawreview.law.pitt.edu

police from their purview, and state statutes regulating collection and use are few and far between.[71]

Here the state-action requirement becomes especially important. As explained above, if police vacuum up personal data from common carriers and the like, they would be engaging in searches that should be subject to administrative law restrictions on programmatic actions.[72] And, as now occurs with the National Security Agency's metadata program under the FREEDOM Act, if they want to access the data collected to zero in on a particular person they should have to obtain a court order authorizing that access.[73] But if police can get a private company to do the collecting or searching of the data and then simply purchase the information without abiding by those rules, they could engage in what has been called "data laundering."[74] Data brokers become a "fourth party" that can collect and aggregate information from third parties and deliver it to law enforcement without concern about the Fourth Amendment.

That would be the wrong result. Admittedly, in these situations no presidential authorization lurks in the background, as it did with the post 9/11 metadata collection program. But the fact that the government pays for the data that data brokers provide should, by itself, be evidence of law enforcement's strong preference for the information and its desire to encourage its collection. As Kiel Brennan-Marquez has noted, data brokers are repeat players, their existence depends in part on government largesse, and their technological capabilities enable them to access information much

[71] Ferguson, *supra* note 66, at 188.

[72] *See supra* text accompanying notes 34–38.

[73] Although they may not always need a warrant. *See* Christopher Slobogin, *Equality in the Streets: Using Proportionality Analysis to Regulate Street Policing*, 2 AM. J.L. & EQUAL. 36, 40–46 (2022) (arguing that the Fourth Amendment should be interpreted to endorse a "proportionality principle" that modulates the cause required for a search or seizure based on the degree of intrusion involved).

[74] Joshua L. Simmons, Note, *Buying You: The Government's Use of Fourth-Parties to Launder Data About "The People,"* 2009 COLUM. BUS. L. REV. 950, 976. This phrase is particularly apt when police use companies that go to extreme lengths to avoid disclosure of *any* information about their services to the public. *See* Tau & Hackman, *supra* note 63.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.985
http://lawreview.law.pitt.edu

more easily than either individuals or the government acting on its own.[75] In effect, data brokers are agents of the state, not simply abettors of government efforts.[76]

It has been argued that payments to data brokers should not be considered state action because doing so would mean that "*every time* a private party contracts with the government, they would become a state actor."[77] But in the typical contractual situation the government is not seeking—here quoting a leading Supreme Court case on the state action doctrine—"to induce, encourage or promote private persons to accomplish what it is constitutionally forbidden to accomplish."[78] In the data broker context, in contrast, assuming (as we are) that the third-party doctrine does not apply, the government could not collect what it wants data brokers to collect without legislative authorization or a warrant. While the Supreme Court has made clear that acceptance of government money, by itself, does not make the recipient a state actor,[79] doing so when it allows the state to avoid constitutional dictates does.

For the same reason, the argument that a search/state action does not occur if the government merely replicates what a private party (here the data broker) has already discovered should not prevail.[80] This argument is based on the Supreme Court's decision in *United States v. Jacobsen*, which relied on this rationale in holding that a federal agent's search of a FedEx package and seizure of cocaine found inside did not constitute state action because FedEx agents had already searched the package when they saw it was damaged.[81] But *Jacobsen* is *sui generis* and should not be broadly applied; the cocaine discovered in that case could be seen in plain view, was the only item in the package, and was an illegal substance in which a

[75] *See* Kiel Brennan-Marquez, *The Constitutional Limits of Private Surveillance*, 66 KAN. L. REV. 584 (2018).

[76] *See* Cooper v. Hutcheson, 472 F. Supp. 3d 509, 512 (E.D. Mo. 2020) (holding that a company from which sheriff's office purchased cellphone data was a state actor, albeit largely because the company dealt exclusively with law enforcement).

[77] Aaron X. Sobel, *End-Running Warrants: Purchasing Data Under the Fourth Amendment and the State Action Problem*, 42 YALE L. & POL'Y REV. (forthcoming 2023) (emphasis in original).

[78] Norwood v. Harrison, 413 U.S. 455, 465 (1973) (stating that, in such a situation, it is "axiomatic" that constitutional protection is triggered).

[79] *See* Rendell-Baker v. Kohn, 457 U.S. 830, 840–41 (1982) (holding that private actions "do not become acts of the government by reason of their significant or even total engagement in performing public contracts").

[80] *See* Sobel, *supra* note 77, at 29–30.

[81] 466 U.S. 109, 115–16 (1984).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.985
http://lawreview.law.pitt.edu

person can have no "legitimate interest in privacy."[82] Carrying the majority's reasoning to its otherwise logical conclusion, even searches of houses would not implicate the Fourth Amendment when they merely replicate what an informant has already seen.[83] More importantly, under this logic *Carpenter* would likely become a dead letter. Instead of needing a warrant when seeking CSLI about a specific individual, as that case required,[84] government could simply get "consent" from the dataholder, which will usually be forthcoming from a data broker either explicitly or through voluntary acquiescence to a "lawful order," a term that could easily encompass the type of subpoena found insufficient in *Carpenter*.[85]

The implications of the conclusion that government use of data broker information constitutes state action are even more significant than in the third-party abettor setting. It requires not only that, before acquiring information from these companies, the government have the requisite justification for accessing the type of information it wants.[86] It also requires that the collection of the data *by the data broker* meet the same legislative authorization, notice-and-comment, and judicial review requirements that should be imposed on government-run programs. Specifically, before government can access the data of these quasi-governmental "private" companies, a statute would have to identify the types of data they can collect, specify the purposes for which law enforcement can use it, and set out guidelines for retention and security; further, regulations would have to be

[82] *Id.* at 123.

[83] *See id.* at 132–33 (White, J., concurring in part) (making this point and supporting the majority only because the cocaine was in plain view when the federal agents arrived).

[84] Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

[85] *Id.* (finding insufficient an order authorized by 18 U.S.C. § 2703(d), which issues upon "'specific and articulable facts showing that there are reasonable grounds to believe' [the sought-after wire and electronic communications records] are relevant and material to an ongoing criminal investigation"). *See generally* Christopher Slobogin & James W. Hazel, *Who Knows What, and When: A Survey of the Privacy Policies Proffered by U.S. Direct-to-Consumer Genetic Testing Companies*, 28 CORNELL J.L. & PUB. POL'Y 35–66, 60–63 (2018) (describing types of orders, most of which do not require probable cause). For the same reason, the argument that such a transaction is not a "search" when the data broker has control over the property and agrees to its disclosure should not prevail. *See* Orin Kerr, *Buying Data and the Fourth Amendment*, HOOVER INST. AEGIS SERIES PAPER NO. 2109 (2021), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3880130 (making this argument, based on the holding in *United States v. Matlock*, 415 U.S. 164 (1974), that a third party may consent to search of property over which they have mutual control).

[86] If the information is about a particular person, I have argued that the justification should be roughly proportionate to the amount and type of information sought, which means that a warrant would not always be required. SLOBOGIN, *supra* note *, at 38–77.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.985
http://lawreview.law.pitt.edu

promulgated implementing the statute. This regime is necessary because, unlike the common carriers that helped the government post-9/11, data brokers are collecting the information as government surrogates; they are collecting information from those very common carriers, as well as from other private and public databases. To the extent a company like Acxiom or Fog Reveal conducts its business as an agent of the government, it should be treated like the government. If it does not want to be subject to this type of regulation, it has the option of dropping the government as a client.

III. INFORMANTS: INSTITUTIONAL V. INDIVIDUAL

What if the police do not cajole transfer of data through executive or legislative action—as with abettors—or by contracting for it—as with surrogates? Instead, a third party comes across incriminating information and gives it to the police. Can there be state action in this situation?

There is some caselaw suggesting that state action occurs if a third party usurps a function traditionally reserved "exclusively" for the government.[87] While at a stretch that rationale might make state actors of private police who patrol a locale to the exclusion of government agents, it would not apply to the typical business or individual that happens to have information the government has not traditionally collected.[88] Nonetheless, in the specific context of obtaining information from third parties for investigative purposes, there are good reasons for concluding that unsolicited surrender of material to the government involves state action, at least when the third party is a commercial entity rather than an individual.

To understand why, it helps to revisit the origins of the third-party doctrine (briefly mentioned in connection with the discussion of *Carpenter v. United States*[89]). That doctrine interacts with the state action requirement in interesting ways. One of the first Supreme Court cases to recognize the third-party exception to the Fourth Amendment involved Jimmy Hoffa (the famed labor leader) and an acquaintance of his named Edward Partin; Partin agreed to pass on to the government any information about jury tampering that came to his attention, which he

[87] Jackson v. Metro. Edison Co., 419 U.S. 345, 352 (1974).

[88] *See* Flagg Bros. v. Brooks, 436 U.S. 149, 160 (1978) (holding that this type of state action occurs only when the state has "delegated [to the private actor] an exclusive prerogative of the sovereign").

[89] *See supra* text accompanying notes 3–6, 27–29.

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.985
http://lawreview.law.pitt.edu

subsequently did.[90] Hoffa challenged the admission of Partin's testimony on the ground that Partin betrayed his confidence when he posed as an ally. The Court rejected that argument because Partin "was not a surreptitious eavesdropper" but rather was privy to Hoffa's statements "by invitation."[91] Other informant cases before and after *Hoffa v. United States* repeated this reasoning.[92] It was this line of cases on which the Supreme Court relied in *Smith*, the decision that, along with *United States v. Miller*[93] (involving account information obtained from the defendant's bank) established that the Fourth Amendment does not apply to government requests for information from corporate entities. Like Hoffa, the Court reasoned, Smith and Miller assumed the risk that the information they surrendered to a third party would end up in the government's hands.[94]

However, this Article takes as a given that *Miller* and *Smith* are wrong. The question then arises as to how the state action requirement applies when an individual like Partin or an entity like a bank or phone company decides to hand over incriminating information to the government. I have argued in other work that, when the government requests the information, state action exists even when the informant is an individual like Partin.[95] But even if that argument fails, individual informants should be distinguished from institutional informants on at least three grounds, grounds that could lead to the conclusion that when companies become informants there is often state action even in the *absence* of a government request.

The first distinction is that businesses, in contrast to individuals, are commercial entities driven primarily by the profit motive. As both Chris Hoofnagle and Aidan Cover have documented, even "volunteered" disclosures that are not motivated by a government request will often be driven by the hope of cultivating government favor, in all sorts of ways, ranging from beneficial regulatory decisions to direct sales.[96] Reinforcing these incentives through nullifying Fourth Amendment

[90] Hoffa v. United States, 385 U.S. 293 (1966).

[91] *Id.* at 302.

[92] Lopez v. United States, 373 U.S. 427 (1963); Lewis v. United States, 385 U.S. 206 (1966); United States v. White, 401 U.S. 745 (1971).

[93] 425 U.S. 435 (1976).

[94] *Id.* at 443.

[95] Christopher Slobogin, *The World Without a Fourth Amendment*, 39 UCLA L. REV. 1, 103–06 (1991).

[96] Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REGUL. 595, 617–18 (2004); Avidan Y. Cover, *Corporate Avatars and the Erosion of the Populist Fourth Amendment*,

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.985
http://lawreview.law.pitt.edu

protections could lead to surreptitious surrogate surveillance—for instance, the development of algorithms to detect criminal activity—that ought to be regulated programmatically but cannot be because it is undiscovered.

It is possible that, on a much smaller scale, something analogous could happen with individuals hoping to garner favor with the government. But the second distinction explains why individual informants might still be allowed to volunteer information that companies cannot. That distinction has to do with autonomy. Establishing a rule that the government must ignore disclosures from individual citizens such as Partin denigrates their autonomous choice to make the disclosures.[97] In contrast, impersonal corporate bodies have historically not been granted the same rights as natural persons; while "corporations are people" in some contexts,[98] the Supreme Court has declined to so hold in the Fourth and Fifth Amendment settings.[99] Individual actors should be able to do what they want with information in their possession. But no autonomy interest is insulted by a government refusal to accept or use volunteered information from state-created entities like those involved in *Miller* and *Smith*.

Third, and most important, unlike human confidantes, commercial institutions can be said to owe either formal or quasi-formal fiduciary duties to their customers. These companies are only able to obtain personal facts because they purport to

100 IOWA L. REV. 1441, 1445 (2015) (describing the economic and legal incentives that technology companies have to "cooperate" with the authorities).

[97] Mary Irene Coombs, *Shared Privacy and the Fourth Amendment, or the Rights of Relationships*, 75 CAL. L. REV. 1593, 1643–44 (1987) ("To deny even the possibility of such a decision [to cooperate] is to turn a freely chosen relationship into a status, denying one person's full personhood to protect another's interests.").

[98] *See* Kent Greenfield, *If Corporations Are People, They Should Act Like It*, THE ATL. (Feb. 1, 2015) [https://perma.cc/GK82-P74B] (alluding to the Citizens United v. Fed. Elections Comm., 558 U.S. 310 (2010) granting corporations First Amendment rights).

[99] *See* United States v. White, 322 U.S. 694, 698 (1944) ("The constitutional privilege against self-incrimination is essentially a personal one, applying only to natural individuals."); United States v. Morton Salt Co., 338 U.S. 632, 652 (1950) ("[C]orporations can claim no equality with individuals in the enjoyment of a right to privacy. They are endowed with public attributes. They have a collective impact upon society, from which they derive the privilege of acting as artificial entities."). Some sole proprietors might escape this categorization. The Court's Fifth Amendment jurisprudence helps determine whether a company should be treated as an individual or an entity. *See* Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 841–44 (2005).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.985
http://lawreview.law.pitt.edu

provide a particular service.[100] In that sense, they offer professional services like lawyers, doctors, social workers and accountants who normally must maintain confidentiality. The companies themselves recognize this fact; the typical commercial privacy policy guarantees that the personal information they obtain will not be surrendered to the government without a lawful order.[101] Those policies exist, in large part, because companies realize that if people thought banks, phone companies, and other businesses that they routinely patronize searched through their data looking for evidence of tax fraud, unusual call patterns or other anomalies they would be perceived as conduits to—and agents of—the government.

All of this suggests that, even if the Fourth Amendment does not govern individual informants like Partin, it should discourage institutional vigilantes. Congress may well agree: the way the Electronic Communications Privacy Act, passed by Congress in 1986, accomplishes this goal is through prohibiting common carriers from disclosing information to police unless its discovery was "inadvertent."[102] This prohibition, which captures the notion that a discovery becomes a state-encouraged search when premeditated, should usually be rigorously enforced. That would mean that information a company looked for with the purpose of giving it to the government, even if unprompted, should generally not be admissible in evidence.

At the same time, even well-established fiduciary obligations do not always trump concerns about public safety. For instance, both the legal and treating professions recognize a duty to reveal information that would prevent a crime.[103]

---

[100] *See id.* at 836 (discussing a "'fiduciary duty of allegiance,' which obligates the recordholder to use information for the purpose for which it is acquired"); Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611 (2015) (discussing the concept of information fiduciaries).

[101] *See* Jim Harper, *The Fourth Amendment and Data: Put Privacy Policies in the Record*, THE CHAMPION 32 (July, 2019) (noting that "[t]he heart of the typical privacy policy" promises not to sell, license or share information that individually identifies customers except when necessary to carry out the agreed upon service and to comply with valid legal process); Sobel, *supra* note 77, at 20 (noting that "few, if any" Terms of Service "specifically provide that user data may be sold to government bodies").

[102] 18 U.S.C. § 2702(b)(7). An example of an "inadvertent" discovery comes from *United States v. Jacobsen*, 466 U.S. 109 (1984), where Fed Ex agents came across a damaged Fed Ex package and found cocaine inside. Admittedly, in deciding that the subsequent search by federal agents did not constitute state action, the Court focused on whether the government exceeded the scope of the private search rather than whether the employees' search was premeditated. *Id.* at 115–16. But, as argued earlier, see *supra* text accompanying notes 80–85, *Jacobsen* is *sui generis* on this score. The better rationale for the decision is that the discovery by the private party was inadvertent.

[103] MODEL RULES OF PRO. CONDUCT r. 1.6(b)(1)(2) ("A lawyer may reveal information relating to the representation of a client to the extent the lawyer reasonably believes necessary (1) to prevent reasonably

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.985
http://lawreview.law.pitt.edu

Explicitly applied to the search setting, that norm might permit third-party institutions to disclose even "advertently" discovered information that a crime is occurring or is about to occur (as distinguished from information about a completed crime). Another exception to a lawyer's fiduciary duties arises when confidentiality would prevent discovery of crimes involving use of the lawyer's services.[104] By analogy, if a company-created algorithm discovered that the company's services were deployed to defraud others it should be able to report that crime to the authorities.

Finally, a duly enacted statute requiring disclosures about a customer's transactions could override fiduciary obligations. Examples include the federal "anti-Smurf" legislation mandating that banks report deposits of $10,000 or more,[105] mandatory reporting laws,[106] and laws providing that pawn shops must report receipt of tangible property or evidence of stolen items to the police.[107] Note, however, in contrast to statutes that compel third parties to look through their databases or files for evidence, this type of legislature does not (or at least should not) require that third parties actively search for the relevant information, but rather merely mandates disclosure of material inadvertently discovered in the normal course of business.

Arguably, this should be the extent to which the law bows to the volunteer notion when third-party institutions are involved. Traditional fiduciary rules permit disclosure for serious emergencies, self-protection and statutory obligations, but otherwise prohibit it. That prohibition is presumably based on the recognition that

certain death or substantial bodily harm (2) to reveal the client's intention to commit a crime and the information necessary to prevent the crime"); American Psychological Association Ethical Standard 4.05(3) ("Psychologists disclose confidential information without the consent of the individual . . . to . . . protect the client/patient, psychologist, or others from harm").

[104] MODEL RULES OF PRO. CONDUCT r. 1.6(b)(3) ("A lawyer may reveal information relating to the representation of a client . . . to prevent, mitigate or rectify substantial injury to the financial interests or property of another that is reasonably certain to result or has resulted from the client's commission of a crime or fraud in furtherance of which the client has used the lawyer's services.").

[105] 31 U.S.C. § 5313(a).

[106] *See, e.g.*, Jonathan Todres, *Can Mandatory Reporting Laws Help Child Survivors of Human Trafficking?*, 2016 WIS. L. REV. FORWARD 69, 70 (citing mandatory reporting statutes in all 50 states).

[107] *See, e.g.*, CAL. BUS. & PRO. CODE § 21625 ("It is the intent of the Legislature in enacting this article to curtail the dissemination of stolen property and to facilitate the recovery of stolen property by means of a uniform, statewide, state-administered program of regulation of persons whose principal business is the buying, selling, trading, auctioning, or taking in pawn of tangible personal property . . . .).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.985
http://lawreview.law.pitt.edu

people should be able to trust that institutions on which they depend will not be tempted to betray them by government largesse.

IV. CROWDSOURCING: WEB SLEUTHING AND TORT LAW

Still left unresolved is when, if ever, *individuals* who "voluntarily" help the police should be governed by the Fourth Amendment. An easy answer is that the state action issue need not be addressed in this scenario because, after *Hoffa*, people have no reasonable expectation of privacy in information they knowingly provide an acquaintance. *Carpenter* arguably does not affect that conclusion because, in contrast to the cell site location information collected by the common carrier in that case, the information that individual informants like Partin obtain is "truly shared" and, in contrast to common carriers, such individuals are not "indispensable to participation in modern society."[108] Further, relevant to both search and state action analysis, compared to a commercial entity there is no formal fiduciary relationship between the individual informant and the target, and individual informants possess full autonomy rights that should enable them to control the information they have. Nor is there usually a profit motive incentivizing the individual to ferret out information for the government.

But sometimes there is, and in those situations the Fourth Amendment might be implicated. Most obviously, the government might offer a potential informant money or some other type of compensation to go after a specified target.[109] Whether a person who acts on the offer engages in a search depends on one's interpretation of *Hoffa* and whether *Carpenter* has or should change the law in this area. But the application of state action doctrine is clear: such an informant is no different than the post-9/11 common carriers or data brokers providing information for cash and is clearly a state actor.[110]

What if, instead of soliciting a particular informant, the government offers a reward to the general public? Again, putting the search issue to the side and focusing

[108] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

[109] *See, e.g.*, United States v. Hullaby, 736 F.3d 1260, 1263 (9th Cir. 2013) ("[I]t is 'common practice for the government to reduce or drop charges against persons who cooperate with law enforcement officials in the prosecution of others.'").

[110] *See, e.g.*, Kuhlman v. Wilson, 477 U.S. 436, 459–69 (1986) (assuming the Sixth Amendment was implicated solely by the government's request of a jail cell informant to "listen to" the defendant, allegedly for nothing in return).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.985
http://lawreview.law.pitt.edu

solely on the question of when state action occurs for Fourth Amendment purposes, is this form of incentive enough to trigger constitutional regulation?

Rewards have long been offered for information that helps solve a crime.[111] Similarly, whistleblower statutes incentivize government employees to expose corruption and other types of malfeasance.[112] Further, just as digitization has vastly expanded the personal information held by commercial third parties, it has dramatically changed the scope of what has come to be called "crowdsourcing." Today there is a website, Websleuths, that asks "[o]dinary people from all walks of life [to] come together . . . to dissect clues to crimes and unravel real-life mysteries.[113] A Georgia police department has a mobile app that allows community members, through Facebook and Twitter, to learn about and assist in investigations.[114] Amazon's Ring has developed a Request for Assistance app that police can use.[115] Vizsafe offers digital blockchain rewards for providing tips and video about "incidents," through a private enterprise that could easily be converted to law enforcement use.[116] As Wayne Logan notes, digital crowdsourcing "[has] promise as an investigative force multiplier for governments."[117]

Applying *Skinner*, one might argue that crowdsourcing methods both express a preference for and encourage private pursuit of personal information about others. But even if such pursuits were deemed searches under the Fourth Amendment and were prompted by a reward, individuals who engage in them should not be

[111] For an interesting account of how often rewards are offered and how often they are successful, see Cheryl Corley, *Do Cash Rewards for Crime Tips Work?*, NPR (Sept. 17, 2019), https://www.npr.org/2019/ 09/17/761183202/do-cash-rewards-for-crime-tips-work.

[112] *See Compilation of Federal Whistleblower Statutes* (Feb. 26, 2023), https://crsreports.congress.gov/product/pdf/R/R46979.

[113] Tamara Gane, *Should Police Turn to Crowdsourced Online Sleuthing?*, OZY (Aug. 14, 2018), https://perma.cc/YVS7-GZKV.

[114] Sara E. Wilson, *Cops Increasingly Use Social Media to Connect, Crowdsource*, GOV'T TECH. (Apr. 29, 2015), https://www.govtech.com/gov-experience/cops-increasingly-use-social-media-to-connect-crowdsource.html.

[115] *See, e.g.*, *Ring Launches Requests for Assistance Posts on the Neighbors App* (June 3, 2021), https://blog.ring.com/products-innovation/ring-launches-request-for-assistance-posts-on-the-neighbors-app.

[116] *See Vizsafe, Inc.*, EQUITYNET, www.equitynet.com/c/vizsafe-inc (last visited Oct 11, 2023); Jon Glasco, *How Crowdsourcing and Incentives Improve Public Safety*, BEE SMART CITY (Mar. 10, 2019), https://perma.cc/2VX5-MPWS.

[117] Wayne Logan, *Crowdsourcing Crime Control*, 99 TEX. L. REV. 137, 163 (2020).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.985
http://lawreview.law.pitt.edu

considered state actors. Unlike a government request directed at a specific third party, as occurs with surveillance abettors or surrogates, any disclosure prompted by a reward announcement aimed at the general public is truly voluntary; individuals can decide, free of government pressure, whether to come forward. On that view, providing the public with detailed information about a crime or a crime problem and asking for help—as usually occurs with Websleuths, the Georgia police app, Vizsafe, or Ring's Request for Assistance app—would not trigger the Constitution.

At the same time, vigilantism can be carried too far. One can imagine over-eager sleuths, acting on a hunch or triggered by a law enforcement bulletin, hacking into computers, stalking "suspects" with cell phone cameras, and attempting amateur online stings.[118] Without some sort of specific police direction, none of this implicates the Fourth Amendment.[119] But it could still have repercussions for the vigilante.

In *Burdeau v. McDowell*,[120] the first Supreme Court decision to consider the state action requirement in a Fourth Amendment case, the Court found that, given the absence of police direction, the Constitution was not applicable even though the private individuals from whom the government received the defendant's papers committed a burglary to get them. However, the Court also stated: "We assume that the petitioner has an unquestionable right of redress against those who illegally and wrongfully took his private property."[121] The common law has long recognized a tort of intrusion, which, as the *Second Restatement of Torts* describes it, occurs when a person "intentionally intrudes . . . upon the . . . seclusion of another [and] the intrusion would be highly offensive to a reasonable person."[122] In effect, this tort

[118] *See, e.g.*, United States v. Jarrett, 338 F.3d 339, 345–46 (4th Cir. 2003), *cert. denied*, 540 U.S. 1185 (2004) (finding that a hacker who repeatedly searched private computers for child pornography with the purpose of assisting law enforcement was not a state actor); United States v. Koenig, 856 F.2d 843, 848–50 (7th Cir. 1988) (holding that FedEx employee who repeatedly searched packages and reported discoveries to the police was not a state actor).

[119] It should also be noted that most courts have held that bounty hunters are private contractors not governed by the Constitution, because their contract is with a bondsperson, not the government. *See* Andrew DeForest Patrick, *Running from the Law: Should Bounty Hunters Be Considered State Actors and Thus Subject to Constitutional Restraints*, 52 VAND. L. REV. 171, 172 (1999) ("Bounty hunters have long been recognized by the courts as private actors, and thus immune from constitutional restraints."). Patrick's article goes on to argue, as this Article does, that common law criminal and civil statutes can provide sufficient protection against misconduct. *Id.* at 195–99.

[120] 256 U.S. 465 (1921).

[121] *Id.*

[122] RESTATEMENT (SECOND) OF TORTS, § 652B (1977).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.985
http://lawreview.law.pitt.edu

prohibits private individuals from engaging in the same type of conduct the Fourth Amendment forbids police and police agents to undertake in the absence of adequate authorization.

Much rides, of course, on the definition of "offensive." But here Fourth Amendment law can be useful, if only analogically. For instance, survey results, which I have long argued should inform analysis of the Amendment's "search" threshold,[123] might also be the best way to decide when an intrusion "would be highly offensive to a reasonable person." If so, civil liability should result.

V. FINE-TUNING THE STATE ACTION REQUIREMENT

There can be a very fine line between government encouragement that amounts to state action and government importuning that does not. Given the often-close financial relationship between governments and corporations, the fiduciary duties of the companies that seek and obtain our personal information and their lack of a strong autonomy interest, that line should be drawn in a different place depending on whether the "volunteer" is an entity or an individual. Private entities can easily become willing government appendages and will often need to be treated as such for constitutional purposes, even when they "volunteer" incriminating information. Most importantly, companies whose business model contemplates collecting data for the government should be regulated as if they were the government, subject to both administrative principles and Fourth Amendment access rules. While individual volunteers are less likely to be financially dependent repeat players and thus usually should not be considered state agents, they still should be liable in tort if they obtain their incriminating information through egregious privacy invasions.

[123] *See, e.g.*, SLOBOGIN, *supra* note *, at 53–58 (defending the use of polling to determine which expectations of privacy vis-à-vis the police are reasonable); Christopher Slobogin & Joseph Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society,"* 42 DUKE L.J. 727 (1993).

ISSN 0041-9915 (print) 1942-8405 (online) ● DOI 10.5195/lawreview.2023.985
http://lawreview.law.pitt.edu