THE LOST NUANCE OF BIG DATA POLICING

94 TEX. L. REV. __ (forthcoming 2015)

Jane Bambauer[*]

The third party doctrine permits the government to collect consumer records without implicating the Fourth Amendment. The doctrine strains the reasoning of all possible conceptions of the Fourth Amendment and is destined for reform. So far, scholars and jurists have advanced proposals using a cramped analytical model that attempts to balance privacy and security. They fail to account for the filterability of data. Filtering can simultaneously expand law enforcement access to relevant information while reducing access to irrelevant information. Thus, existing proposals will distort criminal justice by denying police a resource that can cabin discretion, increase distributional fairness, and exculpate the wrongly accused.

This Article offers the first comprehensive analysis of third party data in police investigations by considering interests beyond privacy and security. First, it shows how existing proposals to require suspicion or a warrant will inadvertently conflict with other constitutional values, including equal protection, the First Amendment, and the due process rights of the innocent. Then it offers surgical reforms that address the most problematic applications of the doctrine: suspect-driven data collection, and bulk data collection. Well-designed reforms to the third party doctrine will shut down the data collection practices that most seriously offend civil liberties without impeding valuable, liberty-enhancing innovations in policing.

---

[*] Associate Professor of Law, University of Arizona James E. Rogers College of Law. B.S., Yale College; J.D., Yale Law School. The author is grateful for the thoughtful feedback from Derek Bambauer, Jeffrey Abramson, BJ Ard, Solon Barocas, Dan Barth-Jones, Marc Blitz, Oren Bracha, Tim Brennan, Kiel Brennan-Marquez, Dan Caprio, Jane Cohen, James Cooper, Bryan Choi, George Dix, Joshua Fairfield, Andrew Ferguson, Mary-Anne Franks, Daniel Gilman, David Gray, Rebecca Green, Brad Greenberg, Woodrow Hartzog, Stephen Henderson, Margaret Hu, Guz Hurwitz, Bruce Johnsen, Orin Kerr, Bruce Kobayashi, Jennifer Laurin, Tom Lenard, Geoffrey Manne, Richard Markovits, Deven McGraw, Alex Marthews, Kirsten Martin, David Rabban, John Robertson, Sasha Romanosky, Ira Rubenstein, Andrew Selbst, Berin Szoka, Alan Trammell, and Sean Williams. This research was generously supported by the Law and Economics Center at the George Mason University College of Law and by the University of Arizona James E. Rogers College of Law.

Contents

INTRODUCTION

In 2010, Quartavious Davis committed a series of armed robberies at a Little Caesar's, an Amerika Gas Station, a Walgreens, an Advance Auto Parts, a Wendy's, and a beauty salon in the Miami area.[1] During the criminal investigation, the government accessed sixty-seven days of cell site location data from Davis's service provider without a warrant. The data documented Davis's approximate location during the period and showed he was physically present at the various robbery scenes during the time the crimes were committed, corroborating the eyewitness testimony and other evidence used to convict him.[2] When Davis later challenged the government's warrantless access to the cell site data, the government relied on the third party doctrine—a constitutional rule that permits the state to access business records and transactional data about a company's consumers without constituting a Fourth Amendment "search."[3]

The Eleventh Circuit was not impressed with the government's theory. The facts of Davis's case drew out the great flaw in the third party doctrine. The doctrine relies on the untenable assumption that Americans should not have expectations of privacy in company records. Even if the courts have little sympathy for Davis's privacy expectations while he was robbing the Little Caesar's, the Wendy's, and the other places, Davis should be able to expect

[1] United States v. Davis, No. 12-12928, slip op. at *3-4 (11th Cir. 2014).
[2] Brief of *Amici Curiae* American Civil Liberties Union et al., United States v. Davis, No. 12-12928-EE 4, 7-9 (11th Cir. 2014).
[3] U.S. v. Miller, 425 U.S. 435, 443 (1976).

privacy in his location information during the sixty or so days that he was *not* robbing Miami businesses. On those other days, he might have been "near the home of a lover, or a dispensary of medication, or a place of worship, or a house of ill repute."[4]

Although the prosecutors had the better of the arguments based strictly on third party doctrine precedent, the Supreme Court has strongly signaled that it is ready to revisit the issue. Justice Sotomayor has denounced the logic of the third party doctrine[5], and all of the justices have openly criticized other well-established Fourth Amendment rules for being out of sync with today's technological realities.[6] And so, the Eleventh Circuit was emboldened to recognize Davis's expectation of privacy in his cell site location data. From now on, in that jurisdiction, the government must have a warrant to access third party records.[7]

The Eleventh Circuit got the outcome right but the rule wrong. The warrant requirement is sensible when police build their cases through focused attention on a particular suspect, as they did against Davis. When police seek long, detailed data histories about a specific individual, the target's civil liberties are best protected by guarantees that the data will only be accessed when police have sufficient individualized suspicion.[8] But the warrant requirement is not sensible if the police had conducted an altogether different type of investigation—one that takes advantage of the searchable nature of databases.

Suppose the Miami police department had requested all cell phone service providers to query their geolocation logs to identify any customers who were at three of the robbery locations within an hour of the respective robberies. This "crime-out" type of data request is markedly different from the suspect-driven request the police actually used to get Davis' records.[9] First, the privacy interests identified by the Eleventh Circuit are greatly reduced. The police would not know the long history of travel for Davis or anybody else whose identity was returned based on the search query criteria. The only thing the police would know about the pool of identified customers is that they were at three of the robbery locations near the times the robberies were committed. This sort of search constrains police discretion and limits the grip of confirmation bias.[10] Rather than selecting a suspect first and looking for evidence second, crime-out investigations reverse the order.

---

[4] Davis, No. 12-12928, slip op. at *21.
[5] U.S. v. Jones, 132 S.Ct. 945, 957 (2012) (Sotomayor, J., concurring).
[6] Riley v. California, 573 U.S. __ slip op. at 9 (2014).
[7] Davis, No. 12-12928, slip op. at *23.
[8] Jennifer Granick, *New Ruling Shows the NSA Can't Legally Justify Its Phone Spying Anymore,* WIRED, June 13, 2014.
[9] Crime-out investigations study clues from an already-committed crime. I explain why this category of investigations is special *infra* Part V.
[10] Raymond S. Nickerson, *Confirmation Bias: A Ubiquitous Phenomenon in Many Guises,* 2 REV. GEN. PSYCH. 175 (1998).

Moreover, if the police had been building a case against some other suspect—an innocent one—this crime-out mode of searching cell phone location data could unearth exculpating information. The query results could redirect police attention to the true culprit. Alternatively, the data could undermine the existing case. It could reveal that many people were at the sites of the three robberies around the same times for independent reasons so that the location evidence is less damning than it may initially seem.

This crime-out style of investigation could be considered a "search" on all cell phone customers if the Fourth Amendment expands to cover third party data in a superficially consistent way. But the illustration shows that, when data is used differently, and smartly, a warrant requirement will impede significant public safety interests while protecting only marginal privacy interests. Thus, when the Eleventh Circuit diligently followed the public outcry for a warrant requirement, it chased a civil rights mirage.

The third party doctrine will be dismantled soon, and for good reason. It always strained the logic and common sense of search and seizure law[11], and the National Security Administration's bulk collections of telephonic metadata have reinvigorated the demand for reform.[12] The law will shift to recognize a Fourth Amendment privacy interest in the business records that describe us, but the reformers are struggling to define the proper scope and strength of this new right.

So far, the literature on the third party doctrine has done an admirable job identifying the privacy interests at stake[13] and the practical consequences of the disruption to good police work if the doctrine is gutted.[14] Legal scholars have considered the third party doctrine and its alternatives using a cramped analytical model that balances privacy interests against general interests in crime-fighting, and nothing else.[15]

Consequently, the most popular proposals to reform the third party doctrine have looked backwards for solutions, embracing rules that simulate the slow and costly process of investigating crime with old tools, that restrict access to records based on the sensitivity of the information within them, and

---

[11] Jed Rubenfeld, *The End of Privacy,* 61 STAN. L. REV. 101, 113 (2008); Sherry Colb, *What Is a Search?: Two Conceptual Flaws in Fourth amendment Doctrine and Some Hints of a Remedy,* 55 STAN. L. REV. 119, 123 (2003); Andrew D. Selbst, *Contextual Expectations of Privacy*, 35 CARDOZO L. REV. 643, 669-77 (2013).

[12] *See, e.g.,* Ewen Macaskill & Gabriel Dance, *NSA Files: Decoded*, THE GUARDIAN, Nov. 1, 2013; John Villasenor, *What You Need to Know About the Third-Party Doctrine,* THE ATLANTIC, Dec. 30, 2013.

[13] Daniel J. Solove, *Data Mining and the Security-Liberty Debate,* 75 U. CHI. L. REV. 343, 344 (2008); DANIEL SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY (2011).

[14] Orin S. Kerr, *The Case for the Third-Party Doctrine,* 107 MICH. L. REV. 561, 580 (2009); Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too,* 34 PEPPERDINE L. REV. 975, 1008-1010 (2007).

[15] *See* the discussion *infra* Part III.

that reify traditional hierarchies of individualized suspicion.[16] These solutions revert law enforcement to an environment where they must begin their investigations with personal observations, witness testimony, and pure instinct, as they have historically done. They unwittingly promote an outdated criminal investigation system riddled with inequities and error. And they obscure the ultimate question: how do we want law enforcement to build cases?[17]

The scholarly debate has failed to appreciate how modern computing can promote justice in ways that were impossible a generation ago. Fast computers, cheap storage, and networked data allow criminal investigations to use automated searching, and this feature has unprecedented effects on government searches. Without computers, even the most legitimate searches conducted with a warrant based on probable cause required police to tromp through houses, flip through diaries, and sift through large amounts of personal information unrelated to the investigation. Automated searches, by contrast, can tailor information access so that most irrelevant data is filtered out.

Orin Kerr put his finger on this nearly ten years ago when he pointed out that the current Fourth Amendment rules "permit extraordinarily invasive government powers to go unregulated in some contexts, and yet allow phantom privacy threats to shut down legitimate investigations in others."[18] But even Kerr, the lone defender of the third party doctrine, justifies it on the grounds of maintaining clean rules, and encourages regulators to protect privacy using the legislative process however they please.[19] Whether reforms

---

[16] For example, The American Bar Association Standards for Criminal Justice recommends that courts categorize records based on their sensitivity, and then apply increasingly heightened procedural safeguards for increasingly sensitive information. ABA STANDARDS FOR CRIMINAL JUSTICE: LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS (3d ed. 2013) [hereinafter ABA Standards]. Christopher Slobogin's proposals, which I talk about at length later in the article, are a hybrid between the process hierarchy while still allowing for some pattern-driven investigation. Thus, we have the most common ground (although readers will see I disagree with aspects of his proposal as well.) Slobogin, *supra* note 17; Christopher Slobogin, *Government Data Mining and the Fourth Amendment,* 75 U. CHI. L. REV. 317, 321-22 (2008). *See also* Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations,* 37 HARV. J. L. & PUB. POL'Y 757 (2014); Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MARYLAND L. REV. 101 (2011); Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations,* 24 BERK. TECH. L. J. 1199 (2009).

[17] Christopher Slobogin acknowledges that police need to have reasonable means "to *develop* probable cause." Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory,* 8 DUKE J. CONST. L. & PUB. POL'Y 1, 14 (2012). *See also* William H. Simon, *In Defense of the Panopticon,* BOSTON REVIEW (2014) (critizing the "sentimental disposition toward past convention that obscures the potential contributions of new technologies to both order and justice").

[18] Orin Kerr, *Digital Evidence and the New Criminal Procedure,* 105 COLUM. L. REV. 279, 280 (2005).

[19] Kerr, *supra* note 14 at 565-66.

come from courts or legislatures, scholars have provided little guidance about how access to digital information can improve the criminal justice system.

This Article takes a wide-angle view of the third party doctrine. It analyzes societal interests *beyond* criminal deterrence that often run into conflict with privacy—specifically, due process, equal protection, and the right to free speech. Criminal justice has many interlocking parts. If they are not considered in a holistic way, courts will introduce new problems and paradoxes in their rush to solve old ones. When the full range of societal and constitutional interests are taken into account, it is clear that some warrantless uses of third party records positively promote civil rights. Third party records have the potential to dramatically change criminal investigations by providing new routes for suspects to prove their innocence. They can also increase distributional justice by ensuring that evidence of suspicious behavior is investigated evenly across race and class lines. And they can facilitate crime-out investigations of the sort described above. Each of these uses of data differs in important ways from the dragnet practices that have inspired so much hostility to the third party doctrine, and Fourth Amendment reforms should take care not to disrupt them. Otherwise, police will be consigned to traditional styles of investigation that rely much too heavily on eyewitness memory, police testimony, and intuition.[20]

That said, none of the innovations in criminal law enforcement endorsed in this Article can justify unfettered access to all third party records for any or no reason, which the current third party doctrine allows. Rather than defending the third party doctrine whole cloth, this Article will show how the doctrine should be revised to protect the subjects of criminal investigations without causing unnecessary conflicts with due process, equal protection, and First Amendment values.

Courts can do this by paying less attention to the technopanic that currently shapes privacy debates and paying more attention to the aspects of Fourth Amendment privacy that dovetail with other constitutional values: namely, government accountability and reduced discretion. When these priorities are kept at the center of reforms, two concrete insights emerge: First, the Fourth Amendment should not permit the government to engage in suspicionless suspect-driven data-gathering of the sort that occurred in the *Davis* case. Second, the Fourth Amendment should allow bulk data collection only if the law enforcement agency has designed protocols to ensure that the data is used in an accountable and evenhanded way. Other forms of collection—the sorts that take advantage of the filterability of data—should be left off limits from Fourth Amendment reforms.

The Article proceeds as follows: Part I explains why the third party doctrine is unpopular and theoretically unstable. Parts II and III identify the Fourth Amendment interests that compete with the third party doctrine:

[20] *See infra* Part VII for a thorough discussion of the limitations of traditional police investigations.

privacy (Part II) and obstruction of the criminal law (Part III). Part IV considers the law enforcement interests that predictably run up against Fourth Amendment privacy interests and demonstrates why courts have extraordinary difficulty striking a balance between them. Parts V through VIII explore some of the other societal interests that can come into conflict with new constitutional restrictions on government access to third party records. They are (V) crime-out investigations; (VI) due process interests of criminal suspects; (VII) equal protection and distributional justice; and (VIII) the First Amendment speech interests of third parties. Each of these societal interests stands to suffer if a new Fourth Amendment rule creates overzealous privacy protections. But each can be maintained, even promoted, if the third party doctrine is revised to protect citizens from the harms of law enforcement discretion.

Building cases through unfettered, unaccounted access to personal data kept by private parties is no doubt unacceptable as a matter of constitutional policy and common sense. But cordoning off consumer data and forcing police to use conventional methods to build their cases will have equally repugnant consequences.

I. THE PROBLEM

In *U.S. v. Miller*[21] and again in *Smith v. Maryland*[22], the Supreme Court decided that government access to third party business records is not a search. Thus, the government could collect bank records (in *Miller*) or telephone metadata (in *Smith*) without a warrant, without probable cause, and without implicating the Fourth Amendment at all.

The Court reasoned in *Smith* that Americans do not and should not harbor any expectation of privacy in the phone numbers they dial because each caller knows that the telephone company uses this information to complete calls and logs it to facilitate billing.[23] Moreover, even if some callers do maintain an expectation of privacy, the expectation cannot be one that "society is prepared to recognize as 'reasonable'" since they voluntarily conveyed the information to a third party (the phone company.)[24] After all, the Court had already decided that Americans take the risk of disclosure when they confide in somebody who turns out to be cooperating with the government. In *U.S. v. White*[25], for example, the Court held that a criminal defendant had no privacy interest in a conversation he had with a snitch who was bugged and working with the

[21] 425 U.S. at 443.
[22] 442 U.S. 735, 745-46 (1979).
[23] *Id.* at 742.
[24] *Id.* at 743.
[25] 401 U.S. 745 (1971).

government.[26] *White* is emblematic of the Supreme Court's misplaced trust doctrine which had been firmly established by the time *Smith* came down. For the Court, *Smith* was just a corollary to the assumption-of-risk principle established in *White*. Personal information conveyed to a business or any other third party was no longer under the exclusive control of the customer. Any confidence they had that a business would not turn over the information to the government was misplaced and mistaken.[27]

In the wake of Edward Snowden's leaks about the NSA's telephonic metadata collection programs, *Smith*'s reasoning has come under fierce attack. In truth, the reasoning had serious flaws at inception. *Smith* badly overextended the reasoning from misplaced trust cases like *White.*[28] Although *White* prevents a criminal defendant from claiming a privacy interest in his conversation with a government informant, it is critical to the holding that White's confidant was working with the government knowingly and voluntarily. If the government had recorded White's conversation with another person without the knowledge and cooperation of a party to the conversation, *White* would have been indistinguishable from *Katz v. United States*, which had previously concluded that bugging a telephone constituted a search. *White* depended upon the voluntary cooperation of White's confidant. A theoretical possibility of snitching is not enough, on its own, to remove an expectation of privacy. To fit within the misplaced trust doctrine, the trust had to actually be misplaced.

The third party doctrine, by contrast, does not require the voluntary cooperation of the records-holder. In *Miller*, the FBI served a bank with a subpoena compelling the disclosure of Miller's bank records, whether the bank wanted to cooperate or not. In *Smith,* the telephone company did voluntarily cooperate with the police at the request of the investigating officers, but the Court did not tether its holding to that fact. Since *Smith,* the government has been able to compel the disclosure of telephonic metadata using orders sanctioned by the Pen Register Act[29], and the NSA telephonic metadata program relies on compulsion, too.[30] Verizon and other telecommunications companies have no choice but to hand their records over to the government.[31] In fact, in an ironic twist, telecommunications providers are obligated to keep the government's orders secret through the operation of gag orders that regularly accompany the disclosure orders.[32] Thus, the reasoning of *Smith* is

---

[26] *Id.* at 754.
[27] Smith, 442 U.S. at 745.
[28] Rubenfeld, *supra* note 11 at 113; Colb, *supra* note 11 at 123 (2003).
[29] 16 U.S.C. §§3121 et seq.
[30] In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from Verizon Business Network Services, Inc., available at http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order.
[31] *Id.*
[32] Jack Balkin, *Old School/New School Speech Regulation,* 127 HARV. L. REV. 1, 28 (2014).

strained: a user of a telephone "assumes the risk" that the metadata will be shared by the government, and then the government can exercise its subpoena power to ensure that the risk comes to pass.[33]

Smith was never popular among scholars[34], but the sweeping collection programs brought to light by Snowden's leaks have reinvigorated the push to abandon it. A reversal of the third party doctrine, or the very least a major overhaul, seems inevitable. Recently, *U.S. v. Jones,* which assessed the constitutionality of the warrantless use of a GPS device, all nine justices found that the use of the device constituted a Fourth Amendment search.[35] Five out of the nine believed the collection of 28 days of geolocation data constituted a search even without taking the physical trespass into account[36], and Justice Sotomayor's concurring opinion painted a target on the third party doctrine.[37] *Smith* is on death row.

It might be there for a while.[38] Most scholars know that recognizing access to third party records as a full-fledged search requiring a warrant and probable cause is an unworkable solution. Police need some way to build up suspicion about a suspect, and keeping every last third party record off limits until the case progresses to probable cause would unacceptably frustrate investigations.[39] Thus, scholars have tinkered with compromises to the Warrant Clause to find a solution to the incoherence of the third party doctrine.[40] Some have suggested varying the amount of process required

---

[33] Orin Kerr agrees that the Court never explained why we should believe people "assume the risk" when they disclose information to a third party. As he puts it, "assumption of risk is a result rather than a rationale." Orin Kerr, *supra* note 19 at 564 (2009).

[34] Scott E. Sundby, *"Everyman"'s Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1757–58 (1994); Matthew Toskin, *Automation and the Fourth Amendment,* 96 IOWA L. REV. 581 (2011).

[35] Jones, 132 S. Ct. at 948, 954, 958.

[36] *Id.* at 956, 964 (Sotomayor, J. and Alito, J., concurring).

[37] *Id.* at 957 (Sotomayor, J., concurring).

[38] As Andrew Ferguson cleverly put it to me in conversation, this may be California's death row.

[39] Indeed, this is why federal privacy legislation designed to bolster consumer privacy rights almost always permits law enforcement to access records as long as the records have some relevance to an investigation. Erin Murphy, *The Politics of Privacy in the Criminal Justice System: Information Disclosure, the Fourth Amendment, and Statutory Law Enforcement Exemptions,* 111 MICH. L. REV. 485 (2013); 18 U.S.C. §2703(d) (allowing law enforcement to access telephone and Internet communications metadata as long as they have "specific and articulable facts" to show that the data is "relevant and material" to an investigation).

[40] Colb, *supra* note 11 at 189 (identifying Fourth Amendment incoherence as a critical problem for the privacy and security of the people).

depending on the sensitivity of the records.[41] Others suggest increasing procedural safeguards when the police seek greater quantities of information.[42]

The constitutional soundness of these proposals is open to interpretation because the existing Fourth Amendment rules on information-gathering have no clear guiding principles.[43] At a high level of abstraction, the Fourth Amendment constrains the government's investigatory powers so that its opportunities to abuse its other powers—especially its penal powers—are limited. For the last fifty years, the balance between privacy and law enforcement interests was struck by defining a Fourth Amendment search through the "reasonable expectations of privacy" test from *Katz v. United States*.[44] If government conduct interferes with a person's reasonable expectations of privacy, then that conduct is treated as a search, and the warrant requirement presumptively applies.[45] Prior to the information revolution, the courts bumped along one new technology at a time, working out a bargain between privacy intrusions and the government's interests in enforcing the law. Occasionally new technologies like heat-sensing cameras[46] or aerial surveillance[47] would challenge the bargain and force it to adapt, but none of the early surveillance technologies fundamentally changed how law enforcement investigated. They merely enhanced the senses and observations that police were already accustomed to using. They worked at the pace of individual police officers, who had to listen in on bugs and wiretaps, observe from the helicopter, or take the thermal image. They did not and could not cause the system-wide disruption that cheap, fast computers do.

Computing power and the accretion of third party records have challenged the entire framework. The *Katz* test causes problems by setting a strong presumption for a warrant requirement when investigatory conduct is treated as a "search."[48] With stakes that high, courts were naturally hesitant to call something that would colloquially be called a search a "search" for Fourth Amendment purposes.[49] If courts open the definition of "search" to cover more things, they must have the latitude to work exclusively within the

---

[41] Stephen Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULLETIN 39, 44 (2011). Henderson's work was greatly influential for the ABA standards.

[42] Deven Desai, *Constitutional Limits on Surveillance: Associational Freedom in the Age of Data Hoarding,* 90 NOTRE DAME L. REV. 579 (2014); Slobogin, *supra* note 17 at 24.

[43] AKHIL AMAR, THE CONSTITUTION AND CRIMINAL PROCEDURE: FIRST PRINCIPLES 1 (1997) ("The Fourth Amendment today is an embarrassment."); John D. Castiglione, *Human Dignity Under the Fourth Amendment,* 2008 WIS. L. REV. 655, 657 ("reasonableness as an analytical concept is maddeningly frustrating").

[44] 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[45] *Id.* at 362 (Harlan, J., concurring).

[46] Kyllo v. United States, 533 U.S. 27 (2001).

[47] Florida v. Riley, 488 U.S. 445 (1989).

[48] AKHIL AMAR, THE BILL OF RIGHTS 68-77 (2006).

[49] United States v. White, 401 U.S. 745, 753 ("Nor should we be too ready to erect constitutional barriers to relevant and probative evidence which is also accurate and reliable.").

Reasonableness Clause of the Fourth Amendment, and to avoid the Warrant Clause.[50] Reasonableness will be the touchstone. But of course, "reasonableness" isn't stone at all. It is a soup of competing interests.[51] Courts must ensure that the harms caused by government intrusion are proportional to the government's interests. Mass computing affects both sides of the ledger.

Computing does three things very well. It facilitates aggregation, persistence, and searchability. Scholars have grasped the negative potential of aggregated and persistent data.[52] A Fourth Amendment rule that gives the state easy access to large amounts of personal data can cause catastrophic distortions in the balance of power between the government and the governed. However, criminal procedure scholarship has not yet acknowledged how automated searching and filtering can dramatically change criminal investigations, largely (though not exclusively) for the better.[53]

Traditional searches of homes and effects rely on physical intrusions and human observations. By contrast, automated searches and computer-run filters can permit government access to potentially relevant information without risking observation and use of extraneous details. This difference has profound consequences for policing and for the Fourth Amendment. Without automated searchability, even the most legitimate searches performed with a warrant and based on probable cause require police to rifle through an abundance of irrelevant personal items. With automated searchability, most of the private, irrelevant information can be filtered out from police observation. If done well, automated searching can open up access to data for legitimate law enforcement purposes while simultaneously constraining illegitimate searches. This is an unprecedented technological development. The evolving Fourth Amendment can and should take advantage of this special quality of databases.[54]

---

[50] Akhil Reed Amar, Terry *and Fourth Amendment First Principles,* 72 ST. JOHN'S L. REV. 1097, 1098 (1998); Daniel Solove, *Fourth Amendment Pragmatism,* 51 B. C. L. REV. 1511, 1514 (2010) (encouraging Fourth Amendment law to recognize greater coverage and to regulate police conduct by looking for unreasonable practices).

[51] This problem is on naked display in the Supreme Court's consideration of *California v. Riley*, a case in which the Court had to decide whether police could search the contents of a smart phone automatically pursuant to an arrest. In oral argument, the justices were groping for a middle ground between a rule that protects cell phone privacy and a rule that allows law enforcement access. Amy Howe, *A Whole New World: Today's Oral Arguments In Plain English*, SCOTUSBLOG (April 29, 2014) (describing *Riley v. California* and *United States v. Wurie*).

[52] *See* the discussion and accompanying cites *infra* Part II.

[53] For example, Laura Donohue argues that data collection should always be treated as a Fourth Amendment search without regard to whether the collection and processing is done through automation. Donohue, *supra* note 16 at 765. *But see* Erin Murphy, *Databases, Doctrine, and Constitutional Criminal Procedure,* 37 FORDHAM URB. L. J. (Fordham Urb) 803, 834 (2010) ("In short, rather than follow an industrial age model reliant upon physical acquisition, constitutional doctrine would transition to an information age approach based on knowledge, creation, and dissemination.").

[54] In many ways, this article is doing the work invited by Orin Kerr. "Digital evidence exposes the contingency of the existing rules. It reveals how the rules generated to implement

The next seven Parts will show how this can be done by considering the costs and benefits of law enforcement access to third party records one at a time.

II. FOURTH AMENDMENT PRIVACY

The reasoning of *Smith* is undoubtedly on shaky ground. However, articulating the privacy interests in third party records is not an easy task, either. Privacy advocates must explain why third party data, even when collected in bulk, implicate the same level of privacy concern as the search as listening to a private conversation or physically searching a home.

Privacy objections can be organized into four categories of harm: collection (the government acquires, maintains, and has ready access to sensitive information about the subject); risk of misuse (the government uses or discloses this information in inappropriate ways); aggregation (the accumulation of sensitive information adds an additional layer of risk); and hassle (even legitimate exercises of criminal investigation will cause a number of downstream intrusive searches and seizures.)

A. Collection

The collection interest in third party records stems from unconsented and unwanted exposure to the government about the details of our lives. Moreover, data collected by the government is usually stored and maintained indefinitely. As Jack Balkin has put it, "the rise of the National Surveillance State portends the death of amnesia."[55] Some of the problems raised by collection and persistence of data are more accurately categorized as problems of risk of abuse. That is, if the state collects the details about what we purchase, where we go, and when, where, and whom we call, it will have a lot of granular information at the ready for harassment or vindictive prosecution. But I will hold off discussing the harms that come from the potential of abuse for now. They will be discussed in the next subsection. This section explores the harms immediately and independently imposed by the act of collection. Even apart from the potential for abuse, collection *at all* causes public unease due to the subject's lack of control.

The problems of collection (apart from abuse) are difficult to solve unless Fourth Amendment doctrine is willing to differentiate law enforcement-related government collections from other government collections. Instead, the Supreme Court has gone to great pains to *avoid* that differentiation by insisting

constitutional limits on evidence collection are contingent rules, premised in large part on the dynamics of physical crimes and traditional forms of physical evidence and eyewitness testimony." Kerr, *supra* note 18 at 306. (Columbia piece)

[55] Jack Balkin, *The Constitution in the National Surveillance State,* 93 MINN. L. REV. 1, 13 (2008).

government employers, schools, and housing inspectors must comply with Fourth Amendment rules.[56] This puts third party doctrine reforms in a bind. If the third party doctrine were altered to forbid the government (in any form) from collecting data on a large scale, the repercussions would be severe. The government has been intimately involved in our personal data for decades, and the sensitivity and detail of data held by government actors is breathtaking.[57] The federal government is the nation's largest employer, and the combined employment at all levels of government accounts for 7% of American jobs.[58] 30% of Americans share their health information with their public health insurers (Medicare or Medicaid.)[59] And all of us share the intimate details of our financial lives with the IRS. Government-run libraries know what we've read, public schools know what we've written, and in cities with publicly-provided Internet service, the government maintains ISP records.[60]

Each of these examples theoretically can be distinguished from compelled disclosure of records to the government since they involve some amount of *quid pro quo* bargaining between the government and the employee, patient, and other recipients of service. But a lot of government information-collection does not involve even the barest fig leaf of choice. Households randomly selected to complete the U.S. Census Bureau's long form face criminal sanctions if they refuse to provide the detailed information asked. The Center for Disease Control compels the release of medical records for public health research. One of the FDA's innovative programs requires pharmacies and doctors' offices to report data on every prescription and every adverse reaction to look for side effects that went unnoticed in smaller scale clinical trials.[61]

---

[56] Camara v. Mun. Ct. of the City and Cty of San Francisco, 387 U.S. 523 (1967); O'Connor v. Ortega, 480 U.S. 709 (1987); New Jersey v. T.L.O., 469 U.S. 325 (1985).

[57] Bill Stuntz has made these same observations. "There is a lot to argue about in Fourth and Fifth Amendment law, but the arguments seem to have no effect on debates about the scope of the government's power *outside* traditionally criminal areas… Yet much of what the modern state does *outside* of ordinary criminal investigation intrudes on privacy just as much as the kinds of police conduct that Fourth and Fifth Amendment law forbid." William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure,* 93 MICH. L. REV. 1016, 1017 (1995). "Privacy is a poor separating mechanism: it does not distinguish what the police do from what the rest of government does." *Id.* at 1047. Stuntz suggests reorienting debate to focus on "what makes the police different from, and more threatening than, the government in its other guises." *Id.* at 1019. But ultimately he focuses on force and coercion rather than information gathering. *Id.* at 1020, 1034. Stuntz ignored some of the differences between police power that I identify here (specifically, the potential for aggregation, the discretion of police in directing charges and prosecutions for vindictive or inappropriate reasons.)

[58] Henry Blodget, *Guess What Percentage of Americans Work for the Government Now Versus the Late 1970s?,* BUSINESS INSIDER, July 24, 2012.

[59] Daniel B. Wood, *Census Report: More Americans Relying on Medicare, Medicaid,* CHRISTIAN SCIENCE MONITOR, September 13, 2011.

[60] As is the case in Culver City, California, and Chattanooga, Tennessee. Derek Bambauer, *Orwell's Armchair,* 79 U. CHI. L. REV. 863, 876 (2012).

[61] Barbara J. Evans, *Authority of the Food and Drug Administration to Require Data Access and Control Use Rights in the Sentinel Data Network,* 65 FOOD & DRUG L. J. 67 (2010).

Abortion facilities in many states must make their patient-identified records available for inspection by a government official, and pornography studios are under similar record-keeping requirements under federal law. For the last twelve years, NASA has mapped the ocean floor using a satellite with a lens so strong that, as one researcher boasted, you could zoom in on a person on an intersection in Washington, D.C., and be able to tell whether his toes were hanging off the sidewalk.[62] Cities considering congestion taxes for environmental reasons could force taxpayers to transmit detailed geolocation data to the government.[63] Even the Federal Trade Commission, the self-appointed privacy enforcer, uses its subpoena power to collect consumer data and investigate fraudulent practices.[64] Thus, although many have criticized the third party doctrine for allowing the government to circuitously collect from private industry what it couldn't collect itself[65], the observation is incomplete. The government, in non-law enforcement forms, collects just about everything.

All of these programs are valuable and repay data subjects with direct or indirect benefits. A prohibition or significant procedural barrier to government collection of sensitive personal information is simply not workable. I do not mean to imply that a privacy interest in government non-collection is wrong or morally flawed, necessarily, but it might ask too much of the Fourth Amendment to roll back these practices now that our governments are as thoroughly data-dependent as private companies.

The better approach is to recognize that we have very often permitted the government to collect highly sensitive information in non-criminal contexts that would trouble us in criminal contexts. In other words, if law enforcement data collection is a problem, it is because law enforcement is special.

First, law enforcement collection of third party records presents *more* risk of inappropriate observation, disclosure, and abuse than similar types of collections by other agencies. Law enforcement has a much closer connection to the executive or the controlling political party, both of which might have illegitimate interest in directing investigations to harass their rivals and dissenters. But I will account for this heightened potential for abuse of discretion in the next subsection.

Law enforcement is special in other ways, too, because of its unique power to interfere in the most profound ways with individual liberties. But these powers are wielded after the point of collection. They are incorporated into the upcoming discussions on misuse, hassle, and obstruction.

---

[62] NOVA, EARTH FROM SPACE (aired June 26, 2013).

[63] *The Success of Stockholm's Congestion Pricing Solution,* THISBIGCITY (August 23, 2011).

[64] 15 U.S.C. §49 (authorizing the FTC to "require by subpoena the attendance and testimony of witnesses and the production of all such documentary evidence relating to any matter under investigation").

[65] TERMS AND CONDITIONS MAY APPLY (2013) (documentary film).

After those special features of law enforcement are accounted for, not much is left of the collection harm. Nevertheless, it would be premature to dismiss collection harms outright since there is evidence that, rationally or not, Americans are more bothered by, and more chilled by, NSA and law enforcement collection practices than they are by other significant government collections of sensitive information.[66] Thus, even if other arms of the government collect information similar to the data that could be collected by law enforcement through the third party doctrine, the public has exhibited a different relationship with law enforcement, and that difference deserves recognition.

B. Risk of Misuse

The risk of government misuse, both intentional and accidental, is a more concrete privacy interest than the abstract problems from collection. Misuses come in three forms: observation, abuse of discretion, and disclosure.

Any government agent with access to sensitive information might make an inappropriate query and observe something he shouldn't. This was the harm uncovered when an internal audit of NSA employees and contractors found that some of the agents with access to sensitive records had looked up their friends and ex-girlfriends.[67] The government could also use third party records to map social networks and associations. The victim's associations could be exploited either by inferring something about the victim or by abusing his social and political associations.[68]

Far more troubling, and more specific to the criminal investigation process, is the abuse of discretion problem. Whether or not collection is legitimate when made, a government agent might use the information strategically to pester political dissidents or personal foes. A police officer could search for criminal violations out of eagerness to bring charges. Recent scandals along these lines include prosecutions of journalists who facilitated the leaks of government information for unrelated crimes[69], and the IRS's ideologically tilted treatment of non-profit tax treatment.[70]

---

[66] Alex Marthews & Catherine Tucker, *Government Surveillance and Internet Search Behavior*, available at ssrn.com/abstract=2412564 (2014).

[67] Evan Perez, *NSA: Some Used Spying power to Snoop on Lovers,* CNN.COM, September 27, 2013.

[68] The problem of associational inference is not unique to the law enforcement context (the IRS, public hospitals, and public universities have some of this information as well), but because First Amendment case law specifically honors a freedom of association, this problem merits deliberate consideration. Desai, *supra* note 42.

[69] Emily Bazelon, *Obama's War on Journalists,* SLATE, May 14, 2013.

[70] Lois G. Lerner, *Emails Show IRS' Lois Lerner Specifically Targeted Tea Party,* WASH. TIMES (September 12, 2013); *Judge Orders IRS to Explain Lost Tea Party Emails,* ASSOCIATED PRESS, July 10, 2014. *But see New Records: IRS Targeted Progressive Groups More Extensively Than Tea Party,* HUFFINGTON POST (April 23, 2014).

If those tactics fail, the officer could deliberately disclose embarrassing details or use sensitive information to harass the victim.[71] Disclosures can also occur unintentionally if the agency has a data breach or spill and exposes the information to others.

C. Aggregation

Even if governments at various levels regularly collect sensitive data about its constituents, the aggregation of *all* data presents additional privacy aggravations.[72] Each agency may collect some category of sensitive data that relates to the agency's particular charge, but as long as agencies keep their data siloed, the risk posed by rogue employees is constrained. So, too, is the harm caused by data breaches. If, by contrast, a law enforcement agency is able to collect data of the same sort maintained by all the various agencies, the risks from inappropriate observation and use are bound to grow non-linearly.[73] First, the combination of different types of information might be more revealing because of relationships between the information.[74] In fact, even rich collections of just one type of data can reveal, through inferences, other non-collected attributes about the subject, as when geolocation data is used to determine where a person lives, eats, and works, or when telephonic metadata is used to create a detailed map of social networks.[75] And regardless of what types of inferences can or cannot be made, a variety of sensitive data offers more opportunities to discover something embarrassing about a target. An aggregated database might be an irresistible honeypot for government employees.

D. Hassle

A final privacy harm comes in the form of fruitless searches, seizures, and prosecutions of individuals who turn out to be innocent. These experiences

---

[71] President Obama's Privacy Review Group held out the risk of abuse as one of the two major threats posed by the NSA's metadata collection program. The other was repurposing the information for ordinary criminal law enforcement. LIBERTY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES (2013).

[72] Andrew Guthrie Ferguson, *Big Data Distortions: Exploring the Limits of the ABA LEATPR Standards,* 66 OK. L. REV. 1, 7 (2014).

[73] "[T]he information held by different merchants, insurers, and government agencies can readily be pooled, opening the way to assembling all the recorded information concerning an individual in a single digital file that can easily be retrieved and searched." Richard A. Posner, *Privacy, Surveillance, and Law,* 75 U. CHI. L. REV. 245, 248 (2008).

[74] For example, if the data subject is known to be married and known to make multiple phone calls a week to a cell phone number registered to a woman who is not a work colleague.

[75] Donohue, *supra* note 16 at 873; Steven M. Bellovin et al., *When Enough Is Enough: Location Tracking, Mosaic Theory, and Machine Learning,* 8 N.Y.U. J. L. LIBERTY 556 (2014).

impose significant costs in terms of time, humiliation, and insecurity. I have called these costs "hassle" in other work.[76]

Some amount of hassle is inevitable in any criminal enforcement system, but it will become increasingly common if the police start to use data more aggressively to generate and follow up on predictive profiles.[77] Data-driven profiles operating on third party records offer many benefits, including increased accuracy and equitable application. But there can be significant hassle costs, even when the profiling program meets or exceeds the relevant suspicion standards for a search, if it is applied to large quantities of data *en masse*. After all, we all pass through short-term phases or circumstances that seem suspicious. (We get lost and drive around the block in a "casing" fashion, or we purchase brownie mix and Bob Marley CDs on the same day.) If police had data and resources to act on all suspicious patterns, we would experience a drastic increase in the number of fruitless stops and searches for common crimes such as theft or the possession of marijuana.[78]

Out of these four privacy interests—collection, risk of abuse, aggregation, and hassle—only collection directly and inevitably clashes with the third party doctrine. The others could potentially be managed and mitigated after third party documents are collected. However, there is one more conception of the Fourth Amendment that comes into inescapable conflict with the third party doctrine. Indeed, it conflicts with the whole of the law enforcement enterprise. The interest in obstruction is considered next.

III. FOURTH AMENDMENT OBSTRUCTION

The dominant conception of privacy argues that because we all engage in sensitive yet perfectly legal activities (health decisions, political dissent, sexual behavior, and so forth), privacy is important even if we have nothing to hide.[79] But there is another conception of privacy that seeks to dull the effects of overzealous criminal legislation. Because the substantive criminal law is so broad and complex, Fourth Amendment privacy might be called to service to ensure that we do not suffer disproportionate penalties for minor infractions.[80]

---

[76] Jane Bambauer, *Hassle,* 113 MICH. L. REV. 461 (2015).

[77] Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion,* 163 U. PENN. L. REV. 327 (2015).

[78] For low base rate crimes like murder, the suspicion standard will guarantee that the number of fruitless searches stays low. If the police must have a high enough hit rate (chance of recovery of evidence) for low base rate crimes, they will not be able to cause much hassle.

[79] Daniel Solove, *'I've Got Nothing to Hide' and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745 (2007).

[80] ALAN WESTIN, PRIVACY AND FREEDOM (1967) ("Some norms are formally adopted—perhaps as law—which society really expects many persons to break."); Glenn Harlan Reynolds, *Ham Sandwich Nation: Due Process When Everything Is a Crime,* 113 COLUM. L. REV. SIDEBAR 102 (2013).

In other words, we *all* have something incriminating to hide. These conceptions are not mutually exclusive, and in fact coexist without much conflict in the privacy literature.[81]

The obstructionist view of privacy protects people from facing criminal charges for crimes they actually committed. It assumes that the modern criminal code is hazardous.[82] Some criminal statutes are overly complex and easy to break on a technicality (the tax code, or Sarbanes-Oxley), some are too vague and wide-sweeping, inviting vindictive prosecution (the Computer Fraud and Abuse Act), and some harshly penalize behavior that many (even most) do not consider objectionable (possession of marijuana, immigration violations, or copyright infringement). Obstructionist privacy instincts explain why the public reacts strongly to highly accurate means of criminal detection, such as red light cameras, speed traps, and record-linking exercises to find "deadbeat dads".[83] My own survey research has uncovered evidence that Americans may disapprove of narcotics-sniffing dogs because they have grown weary of the War on Drugs.[84]

The Fourth Amendment provides a convenient surface to wage a counterattack against unjust laws, but using it in this way is likely to be counterproductive. If a criminal law is unjust, the best solution is to modify the substantive law. Fourth Amendment privacy rules may look like a second best solution if fixing the substantive law is politically infeasible, but that appearance does not hold up upon closer inspection. When a poorly conceived

---

[81] Sometimes they coexist in the same article. *See, e.g.,* Gregory Conti et al., *Conservation Theory for Automated Law Enforcement,* available at http://robots.law.miami.edu/2014/wp-content/uploads/2013/06/Shay-etal-TheoryofConservation_final.pdf (2014).

[82] There are a couple other theoretical defenses of obstruction, as well. One rests on the idea that people must be gin a "sporting chance" of getting away with crime. David M. Obrien, *Fifth Amendment: Fox Hunters, Old Women, Hermits, and the Burger Court,* 54 NOTRE DAME L. REV. 26 (1978). Another is what Lawrence Rosenthal has called a libertarian model that holds certain places, mainly the home, so critical to liberty and autonomy that it is practically sovereign even against the detection of crime. Lawrence Rosenthal, *Binary Searches and the Central Meaning of the Fourth Amendment,* 22 WM. & MARY BILL OF RT.S J. 881, 887 (2014). Neither of these theories is particularly rational or well-supported once their core assumptions are exposed, as O'Brien and Rosenthal nicely demonstrate.

[83] Ilya Somin, *Speed Limits, Immigration, and the Duty to Obey the Law,* THE VOLOKH CONSPIRACY (April 17, 2014); MARY DEROSA, CTR. FOR STRATEGIC AND INT'L STUDIES, DATA MINING AND DATA ANLYSIS FOR COUNTERTERRORISM 16 (2004).

[84] Jane Bambauer, *Defending the Dog,* 91 OR. L. REV. 1203, 1205 (2013). This is consistent with the findings of Frank Bowman and Michael Heise, who have demonstrated a drastic decline in federal drug sentences during the 1990s. Frank O. Bowman, III & Michael Heise, *Quiet Rebellion? Explaining Nearly a Decade of Declining Federal Drug Sentences,* 86 IOWA L. REV. 1043 (2001); Frank O. Bowman & Michael Heise, *Quiet Rebellion II: An Empirical Analysis of Declining Federal Drug Sentences Including Data from the District Level,* 87 IOWA L. REV. 477 (2002) [hereinafter Bowman & Heise, *Rebellion II*]. This trend in reduced prosecutions has occurred even while the drug quantity per defendant and the recidivism rate increased, meaning that more serious offenses were receiving shorter sentences. Frank O. Bowman & Michael Heise, *Quiet Rebellion II: An Empirical Analysis of Declining Federal Drug Sentences Including Data from the District Level,* 87 IOWA L. REV. at 505, 511.

criminal law is left on the books, and its enforcement is constrained through privacy rights instead of substantive revisions, the result is less frequent but less fair enforcement.

The interests of political dissidents, whistle-blowers, and relatively powerless individuals may not be served when government access to third party records is greatly restricted. After all, a highly motivated investigator can build an individualized case of suspicion against his chosen target, and he will succeed if he focuses on his target long enough. A vindictive investigator might even prefer to avoid facing hard evidence that his target looks indistinguishable from others who were not investigated. A warrant requirement (or something like it) will prevent the target or the public from having the data to show the police willfully ignored similar, allegedly suspicious behaviors when they were performed by other people.

The best way to test whether a criminal statute is appropriately defined and conscribed, and that its penalty is fair, is to aim for more evenly distributed detection so that the costs of a law are felt by the elite and politically powerful.[85] If the entire electorate runs the risk of feeling the pain of enforcement, the punishment is more likely to be proportional to the crime. I have used a senator's daughter test as a rough rule of thumb: if the senator's daughter has a the same chance of getting caught committing a crime as a relative nobody, an irrational law or unjust penalty will be revisited.[86]

Two vignettes from Harvard help illustrate the link between evenhanded enforcement and changes to the substantive law. In 2011, Aaron Swartz, a Harvard fellow and Larry Lessig protégé, was indicted for violations of federal wire fraud and hacking laws.[87] The details of his case are complex[88], but at the heart of the charges was a scheme to circumvent security measures of MIT and JSTOR in order to download the entire library of articles hosted by JSTOR. The indictment was instantly scandalous to the technorati. Many believed the prosecution was irresponsible given that JSTOR had disclaimed any interest in legal process.[89] But when Aaron Swartz later committed suicide partly due to the stress from his criminal defense, his prosecution opened a national debate about the propriety of the crimes he was charged with. Earlier this year, a bill called "Aaron's Law" was introduced to Congress to amend the

---

[85] Elizabeth Joh has recognized the potential for technology to create a check on police discretion where law has failed to do so in the context of traffic enforcement. Elizabeth Joh, *Discretionless Policing: Technology and the Fourth Amendment,* 95 CAL. L. REV. 199, 204 (2007).

[86] Bambauer, *supra* note 84 at 1209-10 (using the chance that the senator's daughter will get caught as a gauge for evenhanded enforcement).

[87] John Schwartz, *Internet Activist, a Creator of RSS, Is Dead at 26, Apparently a Suicide,* N. Y. TIMES, January 12, 2013; Superseding Indictment, United States v. Swartz, Crim. No. 11-CR-10260-NMG (2012).

[88] I recommend Orin Kerr's summary. Orin Kerr, *Criminal Charges Against Aaron Swartz (Part 1: The Law),* VOLKH CONSPIRACY, January 14, 2013.

[89] Richard Adams, *Harvard's Aaron Swartz Indicted on MIT Hacking Charges,* THE GUARDIAN, July 21, 2011.

Computer Fraud and Abuse Act so that they do not cover mere violations of a website's terms of service.[90] The CFAA was badly in need of these reforms before Aaron Swartz's indictment. Federal prosecutors had successfully prosecuted many computer users for accessing computer information under facts much more sympathetic than Swartz's.[91] In fact, it is by no means clear that Swartz's conduct would fall outside the scope of the CFAA even if the "Aaron's Law" amendments are adopted since he circumvented technological, and not merely contractual, barriers.[92] But Swartz's prosecution and subsequent death finally mobilized the powerful and politically connected to demand reform.

Contrast the prosecution of Aaron Swartz with the non-prosecution of Harvard law professor Charles Nesson, who has regularly identified himself as an avid marijuana and LSD user to news outlets.[93] In an interview with Forbes, Nesson explained that he preferred not to keep secrets, and relied on tenure to protect him from the consequences that most employees would have to face.[94] Nesson's unabashed admissions, without any subsequent criminal investigation, serve as a rather sad reminder that the criminal law informally exempts the privileged. Nesson's blatant drug use sends a shallow signal[95] that drug laws are not enforced in Massachusetts. That signal is incorrect. And it is more incorrect for some than others; during the period that Nesson began to talk openly about his drug use, Massachusetts' marijuana-users were twice as likely to be arrested if they were black than if they were white.[96] The experience leaves one to wonder if the process to decriminalize personal marijuana use would have been hastened by the arrests of Nesson and other politically powerful drug-users.

More generally, testing the legitimacy of a criminal law could require more, rather than less, enforcement because half-hearted enforcement will skew

---

[90] H.R. 2454, 113th Cong. (2013); S. 1196, 113th Cong. (2013).

[91] United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009) (overturning conviction based on violating the Facebook terms of service); United States v. Auernheimer, No. 13-1816 (3d Cir. 2014) ("Weev") (overturning conviction of gray hat hacker who demonstrated a bug in the iPad by downloading several other customers' email addresses on the grounds of venue).

[92] Kerr, *supra* note 88.

[93] Lloyd Grove, *Distinguished Harvard Law Prof. Speaks Openly About His Use of Marijuana and LSD,* WASHINGTON POST, March 5, 2002; Tamar Lewin, *Comments Concerning Race Divide Harvard Law School,* N. Y. TIMES, April 20, 2002.

[94] Adam Tanner, *Dean of Cyberspace Charles Nesson Says It's No Use Trying to Hide Secrets,* FORBES, June 28, 2013.

[95] I am borrowing this term from Bert Huang's excellent article of the same name. However, Huang writes about official licenses to engage in conduct that is otherwise illegal, whereas I am using the term here to explore the signal sent by non-enforcement of conduct that is not formally sanctioned in any way. Bert I. Huang, *Shallow Signals,* 126 HARV. L. REV. 2227 (2013).

[96] ACLU, THE WAR ON MARIJUANA IN BLACK AND WHITE 52 (2013). The statistics from 2001 are the most relevant. In 2008, Massachusetts decriminalized the possession of small amounts of marijuana. Massachusetts Sensible Marijuana Policy Initiative, Massachusetts Ballot Question 2 (2008).

toward the underclass. Consider this snapshot from drug enforcement: In 1999, the US Attorney for San Diego chose not to charge a single person with possession or sale of crack cocaine even though police were catching them.[97] Instead the US Attorney's office focused on the sale of marijuana. The US Attorney for the Eastern District of North Carolina did precisely the opposite—he chose to prosecute crack cases and ignore marijuana.[98] This information arms the public with some evidence of racially-motivated prosecutorial choices since the larger minority population in San Diego (Latinos) were more likely to distribute marijuana while the larger minority population in North Carolina (African-Americans) were more likely to distribute crack.[99]

Since the Fourth Amendment's doctrines have the effect of offering greater protections to the educated and wealthy[100], Fourth Amendment obstruction may have the counterintuitive effect of keeping bad laws on the books for *longer*.

Moreover, since expanded Fourth Amendment rights make the detection of other more serious, less controversial crimes harder, prosecutors and lawmakers are prone to respond by increasing the length of the sentences in order to make the most out of the cases they manage to put together. Alternatively, legislators may pass a greater number of criminal statutes, or pass laws with greater breadth, to give police more opportunities to make arrests.[101] Fourth Amendment obstructions unwittingly contribute to the arms race.[102]

The interests in obstruction cannot play a great role in the design of Fourth Amendment doctrine. Obstruction for its own sake is a direct assault on law enforcement, yet law enforcement is one of the government's "most basic tasks."[103] Thus, while obstruction instincts will no doubt continue to be in the fabric of American culture, and will therefore find its way in Fourth Amendment law in some form, this Article will focus most of its analytical attention on the privacy interests identified in the last Part.

The next Part moves to the other side of the leger and explores the interests that run against Fourth Amendment values. The first is the most

---

[97] Bowman & Heise, *Rebellion II, supra* note 84 at 537.

[98] *Id.*

[99] This is one of the few instances in which we have enough information to *know* how the government chose to exercise leniency. If the public, or at least criminal defendants, had more information about what the government knows and systematically chooses to ignore, the consequences could have a checking effect on discretion. Mass collection of third party data could help in this regard. *See infra* Part VII(c).

[100] Christopher Slobogin, *The Poverty Exception to the Fourth Amendment,* 55 FLA. L. REV. 391 (2003).

[101] Stuntz, *supra* note 57 at 1058 (describing how legislatures could regulate junk yards to the point where every junk yard is guaranteed to have a violation, thus PC established always).

[102] The consequences are significant. As criminal statutes multiply, police discretion to pull over or arrest anybody under the authority of *some* statute grows in step.

[103] Gregg v. Georgia, 428 U.S. 153, 226 (1976) (White, J., concurring).

often frequently invoked: security. The Parts that follow will consider other interests that are more often overlooked in the course of striking a Fourth Amendment balance. Many of the privacy themes will reemerge, and reveal themselves to be more compatible with third party data-collection than they initially seemed. This is because, while some Fourth Amendment interests are significant at the collection stage, others dissolve into concerns about unchecked discretion and abuse.[104] The collection of third party records are sometimes orthogonal, and sometimes antithetical, to police discretion. With the right set of rules, the collection of third party records can help constrain government abuses of power.

IV. THE FOURTH AMENDMENT V. PERSONAL SECURITY

The decline of the third party doctrine's legitimacy offers courts or proactive legislators a rare opportunity to reflect on the larger purpose of the Fourth Amendment. Whatever comes to replace the third party doctrine should curb the risks of state power without impeding the government's basic obligation to enforce its laws, and to enforce them fairly. Crafting the right rule will require a complex balancing of competing interests. The most obvious countervailing interest that regularly conflicts with the Fourth Amendment is the societal interest in law enforcement to prevent and deter crime. Usually this is as far as the balancing goes. Other countervailing interests are ignored by courts and scholars alike.[105] Even if we restrict ourselves to this age-old tension and ignore, for now, all of the other interests identified later in this Article, the balancing act is extremely challenging.

First, estimating privacy harm is a wearisome task. No matter which conception of privacy one measures (sensitivity, aggregation, obstructionism, or hassle), the subjective experience of harm varies widely. Research shows that opinions about data sensitivity and aggregation follow a bimodal distribution.[106] Some people care deeply about control of their personal information, others don't, and the two camps do not understand each other.

---

[104] *See* William J. Mertens, *The Fourth Amendment and the Control of Police Discretion,* 17 U. MICH. J. L. REFORM 551 (1983).

[105] Jones, 132 S. Ct. at 964 (Alito, J., concurring) (balancing "privacy and public safety in a comprehensive way"); Solove, *supra* note 13 at 344 (2008); Epstein, *supra* note 13 at 1202. Christopher Slobogin has considered interests other than privacy that often run against the government's desire to search or seize a person (interests such as freedom from harassment and from false accusations), but he analyzes these other interests as supports to privacy rather than in opposition to it. Christopher Slobogin, *A World Without a Fourth Amendment,* 39 UCLA L. REV. 1, 6-7 (1991).

[106] Alessandro Acquisti et al., *What Is Privacy Worth?,* 42 J. LEG. STUD. 249 (2013); Jacob T. Biehl et al., *When Privacy and Utility Are in Harmony: Towards Better Design of Presence Technologies,* 17 PERS UBIQUIT COMPUT 503, 504 (2013).

Even if we did have a consistent and generally accepted measure of privacy costs, our tolerances for those privacy invasions to fight crime will also vary. Each individual's tolerance will depend on his attitude about the specific crime investigated[107] as well as his overall impression of the government's trustworthiness and legitimacy (which may in turn depend on which political party is in power[108]).

For any particular crime, an osbructionist will have very little tolerance for government investigations of a crime he believes should not be enforced. For example, a college student may endorse very stringent Fourth Amendment rules when considering the investigation of marijuana possession laws. Meanwhile, those in favor of the substance of a law could embrace the same investigation techniques. These points of view cannot be reconciled in a single standard, and a compromise will be painful for both groups.

Striking the right balance for the Fourth Amendment becomes all the more complex when third party records are used to investigate more than one crime. After all, most people have much greater tolerance for law enforcement aimed at preventing serious crimes like terrorist attacks.[109] But unless the Fourth Amendment develops use restrictions prohibiting the government from using information collected in the pursuit of one type of crime in order to prosecute for another.[110] Even good faith uses of surveillance to detect murder or terrorism can expand to cover more trivial crimes. Law and policy debates recognize a danger when the government's desire to detect one type of crime, like drug distribution, is parasitic on the government's collection of information under the guise of some other, more serious crime (like terrorism), and potentially could drive expansions of surveillance. For example, drug enforcement could motivate the Transportation Security Administration to continue using X-ray style bag searches even after the development of new

---

[107] In theory, the Fourth Amendment is indifferent to the crime that is investigated, and at least one Justice (Scalia) has insisted that a search is a search whether the police are investigating murder or jaywalking. Jones, 132 S. Ct. at 954. But in practice, courts tacitly use a sliding scale, requiring less evidence to support probable cause when the police investigate serious crimes. Craig Lerner, *Reasonable Suspicion and Mere Hunches,* 59 VAND. L. REV. 407 (2006). Moreover, the Fourth Amendment constraints may be loosened considerably for the investigation of terrorism (even domestic terrorism). United States v. U.S. District Court, 407 U.S. 297 (1972) ("the Keith Case").

[108] Orin Kerr, *Liberals and Conservatives Switch Positions on NSA Surveillance*, THE VOLOKH CONSPIRACY, December 24, 2013.

[109] Slobogin, *supra* note 17 at 15 ("The law, including Fourth Amendment law, routinely relaxes restrictions on the government when its aim is to *prevent* serious harm.").

[110] Use restrictions are not entirely unprecedented. Randolph v. Georgia, 547 U.S. 103 (2006) (excluding evidence against only the *nonconsenting* resident when the other provides consent to search).

technologies that can search for the presence of the chemicals from explosives (and, importantly, can ignore the chemicals from illicit drugs.)[111]

If privacy and security were the only interests at stake, a use restriction would achieve the optimal amount of surveillance activity. The government would engage only in the information-gathering that offers decent marginal returns for detecting the serious crime justifying the intrusion in the first place. But although a use restriction rule would elegantly solve an activity level problem for one form of surveillance, it would also drive the police to increase other, traditional types of surveillance to investigate the lesser crimes. It would also, by design, waste opportunities to repurpose already-collected data even if the surveillance activity level is calibrated to be no greater than needed for serious crime. These results will have serious consequences to the other societal interests explored in this Article—namely reduced discretion, exoneration, and evenhanded enforcement.

This Article will not offer a final, definitive path out of the bog. But it will identify values, other than general law enforcement, that should be taken into account by third party doctrine reform efforts and will offer some first steps for reform. Those first steps include the elimination of unfettered suspect-driven data collection and some restrictions on bulk data collections.

Throughout, I will demonstrate how my proposals differ from others. I will pay special attention to proposals put forward by Christopher Slobogin[112] and by the American Bar Association[113] not because they are fatally flawed, but for just the opposite reason. Both proposals have much to offer in terms of privacy, practicability, and operability. However, both will pose unnecessary conflicts with some worthwhile innovations in policing. The criminal justice scholars are guided by many good intuitions and have raised awareness to problems that deserve to be corrected. But properly understood in the larger context of constitutional values, their proposals put the Fourth Amendment at risk of more incoherence and unintended consequences.

The next Part considers the value of "crime-out" investigations, which can be profitably separated from other types of investigations because of their inherent limitations on police discretion.

V. THE FOURTH AMENDMENT V. CRIME-OUT INVESTIGATIONS

When scholars and judges describe the perils of the third party doctrine, they focus attention on two forms of practice: the large-scale dragnet, and the unrestricted access to a particular target's data without the faintest connection

---

111 *New TSA Scanners Will Be Able to Read EVERY Molecule in Your Body and Tell What You Had for Breakfast,* DAILY MAIL ONLINE, October 6, 2012; Andrea M. Simbro, *The Sky's the Limit: A Modern Approach to Airport Security,* 56 ARIZ. L. REV. 559 (2014).

112 Slobogin, *supra* note 17.

113 ABA Standards, *supra* note 16.

to a suspected crime. The notion that a policeman can gather the records relating to a chosen suspect without any minimum amount of individualized suspicion and without any restriction on its use reverberates precisely the sort of unchecked discretion and raw police power that offends core Fourth Amendment principles.[114] I will refer to this model of policing as "suspect-in." The policeman chooses a suspect, and then filches through third party records in the hope that there will be some evidence of a crime. Suspect-driven policing begs the question why *this* person was singled out for attention.[115]

There is, however, a different type of investigation that does not follow the suspect-in model. "Crime-out" law enforcement begins the investigation with the clues left from an already-committed crime and traces them toward a suspect, rather than the other way around.[116] Police access to third party records could be extremely useful without raising the concerns of suspect-in investigations because police access to data is tethered to a particular harmful event (a completed crime), and collection can be limited based on the particulars of the crime rather than the beliefs or of the police.

Some routine forms of crime-out third party data access will be non-controversial, as when law enforcement uses routing and IP address information to identify a malicious hacker, or requests the footage of a security camera near the scene of a crime.[117] This type of crime-out investigation would fit within a warrant requirement if access to records is expected to lead directly to, and only to, the guilty.[118] But if the Fourth Amendment evolves to require a warrant, probable cause, or even reasonable suspicion in order to access third party records, the process might not be flexible enough to accommodate some valuable and legitimate crime-out investigating.

---

[114] Debra Livingston, *Police Discretion and the Quality of Life in Public Places: Courts, Communities, and the New Policing,* 97 COLUM. L. REV. 551 (1997).

[115] Orin Kerr, *Why Courts Should Not Quantify Probable Cause*, *in* THE POLITICAL HEART OF CRIMINAL PROCEDURE 131 (Michael Klarman et. al. eds., 2012).

[116] This is identical, or at least very similar, to Christopher Slobogin's event-driven versus suspect-driven investigations. CHRISTOPHER SLOBOGIN, PRIVACY AT RISK 191-96. It is distinguishable from Andrew Ferguson's "unknown" or "stranger" variety of law enforcement in which the police don't know the identity of their target but have selected a target based on their observations of his conduct and attributes. Ferguson, *supra* note 77 at *3.

[117] Video footage has also been used to exonerate the wrongfully accused. For example, Rayshard Futrell, who had been convicted of first-degree murder, was eventually released and exonerated when security footage showed Futrell was at the scene of the crime but wearing different clothing from the shooter. Samuel R. Gross & Michael Shaffer, *Exonerations in the United States, 1989-2012,* available at papers.ssrn.com/sol3/papers.cfm?abstract_id=2092195 (2012). With new products like Google Glass, these types of security footage requests could become much more common.

[118] On the other hand, access to some third party records (such as library, hospital, and legal representation records) might be controversial *even when* police are following the leads from a crime scene. In some narrow contexts, we may not even tolerate a warrant process if law enforcement detection could risk deterring guilty criminals from accessing services that we want them to have (the advice of a lawyer, for instance.)

To illustrate, suppose a botched mugging led to a severe assault at the southeast entrance to Central Park around 9:00 p.m. on May 1st, 2013.[119] Ideally, the police should be able to access third party cell phone records in order to identify who was near the southeast entrance to the park around that time. If the police knew which direction the perpetrators ran, the query could be narrower still: cell phone customers who were near the entrance to the park, and then traveled in the right direction. This sort of information could give the police an initial suspect pool that could then be winnowed further with the usual detective work. Police and the FBI have occasionally used location information in a crime-out sort of way to identify jewelry thieves who stole from one location and pawned at another[120], to find a perpetrator with the first name "Chris" who lives on "Thompkins Street"[121], or to identify a rapist with a unique modus operandi who committed crimes in Pennsylvania and Colorado.[122] But they can and arguably should use this approach more often. This approach has all the more potential when the third party records held by telecommunications providers includes video footage collected automatically by Google Glass wearers.[123]

Most existing proposals for third party doctrine reform would not allow this type of crime-out request. The practice could not stand up to a fully loaded warrant requirement like the one adopted by the Eleventh Circuit because police cannot expect to have probable cause for each and every person whose data is released. Indeed, the police can and should expect that most of the records will identify innocent cell phone customers. The practice would also fail the more permissive reasonable suspicion standard that Christopher Slobogin proposes should apply to searches targeting a particular place.[124] Even assuming courts would accept a purely quantitative calculation of reasonable suspicion, the perpetrators are likely to make up only a small

---

[119] My example is, coincidentally, very similar to an example carried out in the ABA's report, although they assess the ethics of accessing information about the details of one particular phone number. ABA Standards, *supra* note 16 at 11-13.

[120] Conversation with Thomas O'Malley, assistant United States Attorney.

[121] LEXISNEXIS ACCURINT FOR LAW ENFORCEMENT, CASE STUDIES 3-4 (last visited July 13, 2014).

[122] SLOBOGIN, *supra* note 116 at 191.

[123] This is similar in concept to gunshot-detecting video cameras installed on some street corners. These devices alert the police and begin to transmit footage when the device is activated by the sound of a gunshot. Amit Asaravala, *Shhh… Do You Hear Gunfire?,* WIRED, Noevember 23, 2004. Some jurisdictions have been disappointed with the performance of these systems. Greg Toppo, *Gunshot Detection System in Delaware Comes Up Blank,* USA TODAY, February 7, 2014; *ShotSpotter, Gunshot Detection System, Helps Cops Find Killers,* HUFFINGTON POST, April 25, 2012.

[124] SLOBOGIN, *supra* note 116 at 28, 30. Stephanie Pell and Christopher Soghoian suggest using a reasonable suspicion standard for electronic location data. Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data that Congress Could Enact,* 27 BERKELEY TECH. L. J. 117, 180 (2012).

percentage of the customers whose data could be produced under a tailored crime-out request.

The ABA Committee's report on the use of third party records suggests that it endorses the use of records for crime-out investigations. The report gives two examples: when toll tag records "allow police to learn the culprit in a fatal hit-and-run" and where hospital admission records might lead to the identification of a suspect involved in a shooting. The toll tag records in particular seem very similar—assuming that the hit-and-runner was not the only person driving through the relevant toll booths within the time frame, the example suggests (without saying it) that the police would be able to comb through not only the hit-and-runner's toll tag records, but other peoples' too. And yet, by their own legal scheme, law enforcement would not be able access the records in my Central Park example or their own toll tag hypotheticals unless the suspect is the only person, or one of only three or four, who might be identified by the records search (and could thereby meet the reasonable suspicion standard required for medium sensitivity records.)

This is an unfortunate result of the traditional tiers of Fourth Amendment suspicion. Discrete searches of records tailored to a crime have the hallmarks of good police work and Fourth Amendment legitimacy. Unlike the current, unbounded third party doctrine, this system cannot expand to cover the universe of records. The police initiate a crime-out query of third party records only after a crime has occurred, and they have little control over the selection of people who will be included in the returned results.[125] In other words, crime-out investigating imposes constraints on police discretion.[126]

The Fourth Amendment should not get in the way of small crime-specific "dragnets" that can identify witnesses and suspects based on the specifics of a case. Returning to the New York mugging hypothetical, the police department should be able to issue a subpoena that requires the disclosure of cell phone records on a designated temporal and geographic range. Other types of third party records, too, should be accessible through a crime-driven subpoena that filters for factors related to a particular crime, whatever the data type.[127] The

---

[125] Even if a corrupt police officer were willing to m. ake up a crime out of whole cloth, they would not be able to learn any information about a vindictively chosen target. Unless the officer already knew the records details of the target well enough to know that the target will be included in the query responses.

[126] In the aftermath of *U.S. v. Jones*, Peter Swire and Erin Murphy identified limited discretion as a hallmark of good investigation practices. Peter Swire & Erin Murphy, *How to Address 'Standardless Discretion' After* Jones, available at papers.ssrn.com/sol3/papers.cfm?abstract_id=2122941 (2012).

[127] One exception to this general proposition are data requests that run against law or public policy because the government has a good interest in keeping even the *criminal perpetrator's* records confidential. The most common example is hospital and health care records. Because the state has an interesting in making sure that all people, even criminals, are not dissuaded from seeking medical attention when they need it, many courts have already recognized an exception to the third party doctrine in the context of medical records where an evidentiary privilege would apply.

government should be able to access records about telephone calls, Internet searches, or credit card transactions, too, if the parameters of the data request are appropriately tailored to the specifics of a particular crime.[128]

Slobogin's proposal, the ABA Standards, and most other proposals can be reconciled fairly easily with this approach. The concepts introduced here are not new to the criminal procedure scholarship. Orin Kerr has suggested that law could limit the number of transactional accounts that the police can compel at any one time.[129] And Christopher Slobogin has himself distinguished between "event-driven" and "suspect-driven" investigations in order to justify lower suspicion standards for the former.[130] (Event-driven investigations are equivalent to the practices that I am calling "crime-out.") At one time, Slobogin was prepared to permit a mere "relevance" standard (which in practice is no standard at all[131]) for most private records used in a crime-out investigation[132], but he reversed course in his more recent writing and now advocates for the use of a reasonable suspicion standard.

The trouble is that Slobogin never fully fleshed out why the distinction between the two investigation types mattered as much as it does.[133] Had he explained the benefits that come from crime-out investigations that hold police discretion in check, so that police have much less control in selecting who will be the subject of investigation, the usual suspicion standards (both "probable cause" and its more lenient cousin "reasonable suspicion") would look like the poor fits they are.

My proposal gives wide latitude to crime-out investigations because the privacy tradeoffs are modest. These investigations differ from the crummy scenarios motivating reform in which law enforcement accesses a particular target's personal data based on spite or a bald hunch because the opportunities for spite and misuse are greatly reduced. And crime-out investigations collect

---

128 An *inappropriately* tailored request will result in the return of data that is too numerous to be usefully followed-up by the investigation team and that, therefore, shares the qualities of bulk data collection which, like suspect-driven investigations, I argue is contrary to Fourth Amendment values and serves no other compelling purpose.

129 Kerr, *supra* note 18 at 309. He also suggests that information collected should be subject to use restrictions and data destruction requirements. I have not incorporated these limitations because they could get in the way of defensive/exculpatory uses of the same information. *See infra* Part IV.

130 SLOBOGIN, *supra* note 116 at 186.

131 Ferguson, *supra* note 72 at 15-16 ("In practice, there is little required to obtain information under [the relevance] threshold.") (using the NSA access to telephonic metadata as an illustration. *In re* Application of F.B.I. for an Order Requiring Production of Tangible Things From [Redacted], No. BR 13-109, 2013 WL 5307991).

132 *Id.* But he has consistently recommended the reasonable suspicion standard for telephone records, medical records, and combinations of less sensitive records. *Id.* at 186, 194. He defines "reasonable suspicion" to mean a hit rate of roughly 30% which would wipe out the sort of subpoena I describe in this section.

133 Slobogin points to the lack of sensitivity in the information and the relatively small number of data points to justify the distinction. *Id.* I believe these are much less important than the limitations on discretion.

information on a vastly different scale than the NSA telephonic metadata programs. Moreover, the law enforcement interests are heightened in crime-out investigations because they will usually be prompted by a victim who has reported a crime. Thus, this lenient standard for crime-out investigating will be employed most often for crimes that cause direct harms (like theft and violence) rather than sin crimes (like drug use and gambling), which are perceived to be (and arguably are) less serious offenses.

Next we turn to the Fourth amendment's conflict with innocence. As the next Part will show, access third party records should be available to the government when it has identified a suspect for a particular crime in order to avoid false arrests and wrongful convictions.

VI. THE FOURTH AMENDMENT V. DUE PROCESS

When thinking abstractly about the Fourth Amendment's protections, scholars typically balance privacy against general interests in law enforcement. But once a particular suspect has been singled out, the privacy of others has the potential to obstruct that suspect's exoneration. When this happens, the diffused privacy interests of many are pitted against the acute due process interests of the few.

The state's duties to attempt to exonerate a suspect are vague. It has a duty under *Brady v. Maryland* to disclose exculpating evidence to a criminal defendant, but the duty does not vest until indictment.[134] Also, *Brady* requires only that the government hand over information that it actually has; nothing in the case law obligates the government to perform additional investigation in search of evidence that might prove the defendant's innocence and someone else's guilt.

Sometimes third party records concerning the suspect himself can nullify the suspicion forming around him. Police are likely to seek out these records when working up a case against the suspect. But when a suspect's own records are ambiguous or nonexistent, third party records about *other people* could shed light on what actually happened, and could direct police to witnesses or alternative suspects. Video footage shot by a bystander or by an ATM surveillance camera could conflict with the government's theory about what had occurred (as it did for one Occupy Wall Street protester[135]), or the metadata from photographs posted to Facebook might put the police on the lead of another suspect—somebody in a photograph at the right place and time who was not noticed by witnesses. Thus, third party records could occasionally save a suspect from the heartache and personal costs of having prolonged investigatory attention focused on him. When police are working up

134 Brady v. Maryland, 373 U.S. 83 (1963); Giglio v. United States, 405 U.S. 150 (1972).
135 Nick Pinto, *Jury Finds Occupy Wall Street Protester Innocent After Video Contradicts Police Testimony,* VILLAGE VOICE, March 1, 2013.

a suspect, intrusion into other consumers' lives may be justified not just on the basis of a general societal interest in crime-fighting, but by the specific liberty interests of a suspect.

Joshua Fairfield and Erik Luna argue that criminal defendants should have access to the same digital records as the government so that the wrongly accused are better able to prove their innocence.[136] Their work in defining "digital innocence" is so thorough and convincing that the defensive access to records they propose is a no-brainer. (Indeed, on the same logic, a murder suspect in Florida convinced a judge that he should have access to phone records held by the NSA in order to defend himself.[137]) However, Fairfield and Luna do not go so far as to endorse government collection of third-party records in the investigation phase. In fact, they explicitly distance their project from government data collection, calling it "anathema to a liberal, open democracy,"[138] despite the obvious benefits that third party data could have for innocent suspects, arrestees, and defendants.

Fairfield's and Luna's unwillingness to explore exoneration as a factor in the debates about data collection is perfectly understandable. Their argument—that defendants should have the same access to records that the government does—is valid no matter how much or little the government is able to collect. A thorough discussion on the ethics of data collection would distract readers from the power of their reasoning. But their declaration against data-collection is confusing given their enthusiasm for its exoneration potential. Government collection of third party data could come to the aid not only of the wrongfully convicted (a group that constitutes as much as 1-4% of convicts[139]) but also the wrongly arrested and suspected, who could be spared the hassle and pain of searches, seizures, and charges.

This tension between normative commitments for exoneration and against collection is not unique to data. DNA databases have bedeviled criminal justice scholars for the same reasons: innocence is better served by collecting everybody's DNA, and privacy is better served by collecting nobody's.[140] Expanding Fourth Amendment privacy rights to thwart the

---

136 Joshua A. T. Fairfield & Erik Luna, *Digital Innocence,* 99 CORNELL L. REV. 101 (2014).

137 Order Requiring Response from Government, United States v. Daryl Davis et al., No. 11-60285-CR-Rosenbaum (S.D. Fl. 2013).

138 *Id.*

139 Samuel R. Gross et al., *The Rate of False Convictions of Criminal Defendants Who Are Sentenced to Death,* working draft available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2431520 (2014) (estimating that 4.1% of convicts sentenced to death would be exonerated if reinvestigation of the cases remain under the pressures of impending execution); Fairfield & Luna at *15; Marvin Zalman, *Quantitatively Estimating the Incidence of Wrongful Convictions,* 48 CRIM. L. BULL. 221, 230 (2012) (estimating that wrongful convictions across all crimes occur at a rate of about 1%).

140 Erin Murphy, *License, Registration, Cheek Swab: DNA Testing and the Divided Court,* 127 HARV. L. REV. 161 (2013) (criticizing collection); Jason Kreag, *Letting Innocence Suffer: The Need for Defense Access to the Law Enforcement DNA Database,* 36 CARDOZO L. REV. __ (forthcoming 2015) (arguing for greater access to DNA databases by criminal defendants).

collection of information—whether DNA or data—will come at great cost to the unlucky subset of suspects whose innocence would become apparent from that information. These tradeoffs are seldom acknowledged, so we lack the analytical tools to determine how a compromise between privacy and innocence should be reached.[141]

Even if the small chance of exonerating the innocent cannot justify third party data collection on a vast scale, surely the interests of potentially innocent criminal defendants should tip the scales at moments when data collection is most likely to suss out exonerating information— when police have probable cause to make an arrest.

The crime-out process described in the last Part can and should be used to access records that can confirm or disprove the guilt of a specific, arrestable suspect. For example, returning to the hypothetical mugging that occurred on the southeast entrance to Central Park, suppose the criminal investigation has centered on a particular suspect and a search or arrest warrant can be justified on probable cause. Before the police take any of those formal steps, they should be able to use a crime-out subpoena to access data that might lead the police to more witnesses or other suspects. These witnesses can corroborate or refute the police's working theory of the case. Ideally, in light of how simple and inexpensive these sorts of searches could be, the government should have an affirmative obligation to access them to find evidence that supports either the government's or the defendant's arguments. But in the absence of affirmative obligation the Fourth Amendment should at the very least avoid getting in the way.

There are other ways in which police access to third party records might have unexpected positive effects on civil liberties. Access to third party records may chill crime more effectively, and with fewer restrictions on liberty, than traditional law enforcement. This is one rationale for the historic rise in the number of wiretaps sought to detect white-collar crime: while law enforcement is important, prosecutors also wanted Wall Street to understand that the government is paying attention.[142] Similarly, the Rialto, California, Police Department's adoption of recording equipment worn at all times by police officers in the field had the immediate effect of drastically diminishing the number of complaints about police brutality.[143] The equipment did not need to collect evidence of police abuses of force because the surveillance stopped the abuse from occurring in the first place.

Of course, there are some significant dangers to using surveillance as a means of deterrence. This sort of "preventative law enforcement" may achieve the population control outcomes that tyrannical governments always want

---

141 Jane Bambauer, *Collection Anxiety,* 99 CORNELL L. REV. ONLINE 195 (2014).
142 Zachary Goldfarb, *Insider Trading Case Ensnares Six: Prosecutors Accuse Hedge Fund Manager, Otehrs of Raking in $20 Million,* WASH. POST, October 17, 2009.
143 Rory Carroll, *California Police Use of Body Cameras Cuts Violence and Complaints,* THE GUARDIAN (November 4, 2013).

without having to face a constitutional challenge.[144] That is, government access to third party records may chill many good and socially productive behaviors, not just criminal ones.[145] Because it seems extraordinarily difficult to cultivate one kind of chill (crime) and not others (political dissent and other valuable behaviors), I mean only to flag this as a topic of further research.[146]

The opportunity to deter crime without activating the full machinery of arrest, prosecution, and incarceration is controversial, but well worth consideration. Bill Stuntz famously argued that America's addiction to incarceration was the result of having too few police on the streets. Police presence, Stuntz argued (in part based on Steve Levitt's empirical research), is a vastly more effective deterrent against both crime and police misconduct.[147] Indeed, the ABA picked up on this theme by pointing out that one of the advantages in using third party data is to transform investigation into something much less confrontational and dangerous to police and suspects.[148] But this insight did not persuade the Committee to stray from the traditional individualized suspicion models, and it was certainly not on the minds of the Eleventh Circuit panel when it abandoned the third party doctrine and introduced a warrant requirement.

It is a bit troubling that, after third party doctrine reform, a policeman might be able to holler at a person, forcibly spin him around, press him to the hood of a car, and publicly feel up his entire body easier than he could get access to his Amazon records. A total reversal of the third party doctrine will add new internal inconsistencies to the body of Fourth Amendment law. More modest reforms can solve the current paradoxes brought about by the current laisez-faire third party doctrine without adding a new set of paradoxes.

Next we will explore another aspect of the third party doctrine's role in the criminal justice system as a whole: evenhandedness. The next Part will explore how law enforcement use of third party records can promote the fair distribution of the costs of criminal investigation.

---

[144] Jack Balkin warns that "government will create a parallel track of preventative law enforcement that routes around the traditional guarantees of the Bill of Rights." Balkin, *supra* note 55 at 15.

[145] For example, Alex Marthews and Cathleen Tucker have uncovered some evidence that government surveillance changes search behavior. Marthews & Tucker, *supra* note 66.

[146] Michael Rich offers a model for assessing whether we should use technological intervention to make some crimes impossible which includes benefits not only in the form of reduced crime, but reduced incarceration and investigation costs, too. In the case of driving under the influence, he argues we should consider redesigning technology so that drivers with a high blood-alcohol level cannot start their cars. Michael Rich, *Should We Make Crime Impossible?,* 36 HARV. J. L. & PUB. POL'Y 795, 805-07, 830, 846.

[147] William J. Stuntz, *Law and Disorder: The Case for a Police Surge,* THE WEEKLY STANDARD, February 23, 2009; William Stuntz, *Unequal Justice*, 121 HARV. L. REV. 1969, 2033 (2008).

[148] ABA Standards, *supra* note 16 at 4.

VII. THE FOURTH AMENDMENT V. EQUAL PROTECTION

The most immediate goal of criminal law enforcement is to deter the commission of crime. But to achieve that goal and to do it fairly, courts must monitor the *distributional effects* of law enforcement. John Hart Ely called the Fourth Amendment the "harbinger of the Equal Protection Clause."[149] Although the Supreme Court largely disagrees[150], distributional justice is an important social goal within and outside the Fourth Amendment.

Third party records could have a starring role in a modern, more equitable style of law enforcement by facilitating pattern-based data mining—one of the least understood and most feared innovations in modern policing. Algorithmic policing has a long and distinguished list of detractors for the predictable reasons (error, power, and the lack of individualization).[151] But it has an equally impressive list of supporters.

Big data techniques came of age in the wake of the September 11th attacks. The timing was unfortunate. Early uses of data-driven crime prediction were frantically directed at solving an impossible problem: detecting terrorism. Predicting which people are terrorists is a futile task because virtually no one is. Like any rare crime (e.g. mass shootings), using a lot of external data may outperform common sense instincts about which types of people are at slightly elevated risk of committing a terrorist act, but even the best algorithms are lousy. Since the government is hell-bent on avoiding Type II errors (letting a terrorist slip through), the algorithm will inevitably make a lot of false alerts.[152] Add to all this the fact that the American government's profiles attached great weight to religiosity and national origin and the result is an understandable deep distrust of data-driven policing within the legal academy.[153]

But most crimes are not as rare as terrorism. And some of those crimes leave patterns—watermarks in third party records that show a high probability

---

[149] JOHN HART ELY, DEMOCRACY AND DISTRUST 97 (1980). Tracey Maclin and Anthony Thompson have argued that racially disparate effects should be incorporated into the analysis of Fourth Amendment law, and Christopher Slobogin has adapted John Hart Ely's political process theory to search to argue that Fourth Amendment searches on subgroups of the population must be performed in an even-handed way. Tracey Maclin, *Race and the Fourth Amendment,* 51 VAND. L. REV. 333, 362 (1998); Anthony Thompson, *Stopping the Usual Suspects: Race and the Fourth Amendment*, 74 N.Y.U. L. REV. 956, 962 (2006); Slobogin, *supra* note 17 at 4.

[150] Whren v. United States, 517 U.S. 806 (1996); Robinson v. California, 370 U.S. 660 (1962).

[151] BERNARD HARCOURT, AGAINST PREDICTION (2007); CAROLE MCCARTNEY, FORENSIC IDENTIFICATION AND CRIMINAL JUSTICE 66 (2006). I aim a sharp critique at the lack of individualization complaint in previous work. *See* Bambauer, *supra* note 76.

[152] Sara Kehaulani Goo, *Cat Stevens Held After D.C. Flight Diverted,* WASH. POST, September 22, 2004.

[153] HARCOURT, *supra* note 151; Daniel J. Steinbock, *Data Matching, Data Mining, and Due Process,* 40 GA. L. REV. 1 (2005); Solove, *supra* note 13. I am in agreement with Daniel Solove that critics of government transparency and scholars urging deference to the executive branch were in a shortsighted crisis-driven panic, especially since lightning continues to be a bigger killer than terrorism. *Id.* at 351.

that a crime has occurred. Credit card fraud, botnets, and ponzi schemes leave telltale signs in consumer transactions and communications metadata, and the algorithms used to detect them are very successful.[154]

Thus, the ABA standards committee, Christopher Slobogin, Tal Zarsky, and Andrew Ferguson have all endorsed the use of data mining to detect signs of criminal conduct under certain conditions.[155] This momentum among criminal procedure scholars may seem troubling amid the growing fears of technological change and a non-transparent government. This Part explains the guarded optimism.[156]

Pattern-driven data mining of third party records can lead to fairer enforcement of our criminal laws through three mechanisms. First, looking at the enforcement of any one particular crime, Subpart A describes how data mining can lead to more equitable enforcement by reducing the opportunities for human bias to infect decision-making. Subpart B shows that pattern-driven data mining of third party records allows for the detection of different *sorts* of crimes—crimes that are almost entirely electronic and often committed by criminals from higher social classes. Subpart C argues that transaction data can also provide badly needed information to law enforcement supervisors, criminal defendants, and the public at large about whether criminal laws are enforced equitably.

However, none of these potential uses can be realized without bulk data collection, and that style of mass collection strains the privacy principles at the center of Fourth Amendment doctrine. This Part concludes with a proposal for facilitating pattern-driven data mining designed with appropriate checks in place. In brief, I argue that bulk data collection should be treated as a Fourth Amendment search since it presents the same risk of discretionary or harassing use as suspect-driven data collection. However, police should be able to make liberal use of the special needs doctrine in order to collect data in bulk for experimental and accountable pattern-driven investigations.

A. Same Crime, Better Suspicion

Some crimes can be investigated crime-out rather than suspect-in. As I explained above, these types of investigations usefully constrain the government to investigating a finite set of suspects (whether they use third party records or not.) They also drive the police to follow evidence-based leads

---

154 *See* discussion *infra* Part VII(b).

155 ABA Standards, *supra* note 16 at 111; Slobogin, *supra* note 17; Tal Z. Zarsky, *Governmental Data Mining and Its Alternatives,* 116 PENN. ST. L. REV. 285, 289-290, 311-12 (2011); Ferguson, *supra* note 77.

156 Tal Zarsky has argued that pattern-based data mining has the potential to radically reduce law enforcement bias and inequities if (*if*) it is done right. Zarsky, *supra* note 155 at 289-290, 311-12; Tal Zarsky, *Law and Technology: Automated Prediction: Perception, Law, and Policy,* 9 COMM. OF THE ACM 33, 33, 35 (2012).

rather than their own hunches and suspicions[157]. However, police cannot limit themselves to investigating crime-out cases. There are too many crimes with diffuse, disempowered, or unaware victims. These include attempts, financial crimes, domestic abuse, and contraband distribution.

From an equal protection standpoint, allowing the government to access third party data has a lot of upsides when compared to the status quo. After all, police must build their cases somehow, and conventional policing put a disproportionate share of the costs of law enforcement on poor and minority communities. The Supreme Court has approved seat-of-the-pants police investigating methods in cases like *Wardlow*[158], *Terry*[159], and *Gates*[160]. These have sent lower courts on the hunt for silly police narratives without any objective evidence that the policeman's inferences are a good measure of suspicion.[161] But heavy reliance on officer testimony is prone to misjudgment or even outright deceit ("testilying."[162]) And judges allow officers to use squishy, subjective factors like "furtive movements,"[163] and inferences based on the officer's "training and experience,"[164] to build these suspicion narratives. These types of factors are likely to incorporate race and class biases, and they also perform poorly at predicting crime.[165]

---

157 Although some of those evidence-based leads, such as eyewitness testimony, has a long track record of inaccuracy and bias. Radley Balko, *Eyewitness Testimony on Trial,* REASON.COM, April 8, 2009.

158 Illinois v. Wardlow, 528 U.S. 119, 122, 124 (2000) (finding that the reasonable suspicion standard was met when the police entered a "high crime area" and saw some teenaged kids burst into "unprovoked flight").

159 Terry v. Ohio, 392 U.S. 1, 6 (1968) (finding that an officer had reasonable suspicion to stop the defendant when he observed casing behavior).

160 Illinois v. Gates, 462 U.S. 213, 227 (1983) (finding that an anonymous letter that reported a future drug delivery predicting odd travel plans partially corroborated by the police provided the basis for probable cause).

161 The problem with the narratives approach to probable cause and reasonable suspicion has been roundly criticized. Craig Lerner, *supra* note 107; Bernard Harcourt & Tracey Meares, *Randomization and the Fourth Amendment,* 78 U. CHI. L. REV. 809 (2011); Max Minzner, *Putting Probability Back Into Probable Cause,* 87 TEX. L. REV. 913 (2009).

162 ALAN DERSHOWITZ, THE ABUSE EXCUSE 235 (1994); David N. Dorfman, *Proving the Lie: Litigating Police Credibility,* 26 AM. J. CRIM. L. 455 (1998); Christopher Slobogin, *Testilying: Police Perjury and What to Do About It,* 67 U. COLO. L. REV. 1037 (1996).

163 People v. Woods, 64 N.Y.2d 736,737 (N.Y. 1984).

164 United States v. Brown, 159 F.3d at 149-50; Harris v. State, 806 A.2d 119, 121 (Del. 2002); State v. Lafferty, 291 Mont. 157, 162 (1998) (abrogated on other grounds in State v. Flynn, 359 Mont. 376 (2011); Terry, 392 U.S. at 27.

165 "High crime area" was used as a justification in over 55% of the stops performed in New York between 2004-2009. Jeffrey Fagan compared the use of "high crime area" as a justification across precincts to see if the justification correlated with actual crime data. They did not. Even in the precincts with the lowest crime rates, "high crime area" was used as a justification nearly 55% of the time. Report of Jeffrey Fagan, Floyd v. City of New York, 08 Civ 01034 at 54 (2010).

None of these use third party records. The conventional style of investigations is built on "small data"[166], relying almost exclusively on the observations of individual police officers and the idiosyncratic, unaccountable, unknowable personal algorithms that they keep in their minds.[167]

Traditional police investigations distribute their suspicion and intrusions in terribly regressive ways. When the beginning stages of an investigation are driven by police observations and curiosity, they focus disproportionately on the poor.[168] This phenomenon is not necessarily the product of any malice or bias on the part of police departments; they spend more time in low income neighborhoods where their help is most needed and most wanted.[169] But the accumulation of recent Fourth Amendment rules has added even more distortion to the unequal attention paid to the poor. The upper classes can afford more home and more curtilage[170], and can avoid living in "high crime areas," which requires police to build slightly more evidence before progressing to a stop or search.[171] Thus, when we force individual police officers to sniff out crime while they are on the beat, the results are unsurprisingly imbalanced. Marijuana convictions provide some evidence: minorities serve a disproportionate share of the prison time for minor drug convictions despite having drug usage rates similar to whites.[172]

The legal scholars who most forcefully accuse law enforcement of systemic racial bias have not carried the burden of laying out practical alternatives to the

---

166 Ferguson, *supra* note 77.

167 Thompson, *supra* note 149 at 985-987 (describing the implicit, unaccountable decisions that each policeman develops during their experience in the field); Minzner, *supra* note 161 (showing great variability in police officer accuracy when assessing probable cause).

168 DAVID K .SHIPLER, THE RIGHTS OF THE PEOPLE: HOW OUR SEARCH FOR SAFETY INVADES OUR LIBERTIES 55 (2012);

169 As Philip Heymann claims, "the great majority of people in almost every city and the clear majority of those in the neighborhoods most threatened by both insecurity and the risks to civil liberties would, if forced to choose, prefer the new forms of policing… the advantages of personal security are that great." Philip B. Heymann, *The New Policing*, 28 Fordham Urb. L. J. 407 (2000).

170 For example, Florida v. Jardines, 133 S.Ct. 1409 (2013), found that bringing a drug-sniffing dog to the door of a house constituted a search. But because the opinion relied on physical trespass onto the curtilage, lower courts have permitted the same technique on the front doors of apartments. *See* State v. Nguyen, N.D. No. 20130159 (N.D. 2013).

171 Police may be less familiar with the signs of suspicious and trustworthy behavior in communities that are not their own. Tracey Maclin, *Terry v. Ohio's Fourth Amendment Legacy: Black Men and Police Discretion,* 72 ST. JOHN'S LAW REV. 1271, 1281 (1998) (hypothesizing that police are less likely to detect the subtle signs that a person is law-abiding and reliable within black communities).

172 Stephen Gutwillig, *The Racism of Marijuana Prohibition*, L.A. TIMES, September 7, 2009; CDC Drug Usage Table. However, the government may use drug offense pleas to bargain away the prosecution of more serious crimes. *See* K. Jack Riley et al., RAND Corp., Just Cause or Just Because?: Prosecution and Plea-Bargaining Resulting in Prison Sentences on Low-Level Drug Charges in California and Arizona (2005).

current system.[173] The use of data-driven policing and suspicion is probably not what they have in mind. Meanwhile, some scholars have rushed to criticize the practice of profiling with data[174], but most have not seriously considered the injustice in a police investigation system that profiles *without* data.

Without data, police must rely on their intuitions, observations, and other highly discretionary means of investigating. With data, on the other hand, police can detect and investigate everybody who exhibit similar types of suspicious behavior without letting unconscious factors or geographic limitations affect their investigation decisions.

Today, police departments can use data to investigate crimes that were once investigated using the usual accretion of faulty evidence. They have already used social media comments to learn about gang activity and membership[175], and they have mined their own crime data to predict in advance precisely where burglaries and other crimes are likely to happen, and when.[176] This can have real implications for individual suspects. If a person with some minimal signs of suspicious behavior appears in one of these data-derived hot spots, behavior that would ordinarily fall short of the *Terry* standard could justify a stop when combined with the hot spot prediction. Similarly, Elizabeth Joh and Andrew Ferguson have already anticipated that police could use data to more objectively and reliably define which parts of a city are "high crime areas" (justifying increased suspicion under *Wardlow*.)[177]

So far these data-driven operations have involved public information or the police department's own crime data, so they have not taken advantage of the much richer sources of information currently residing in the servers of private companies. But if a police department did want to collect third party records in bulk and apply a suspicion algorithm, there is little in the current law that would constrain them.

Ferguson has hypothesized that the purchases of large numbers of mini-Ziploc bags (suggestive of drug dealing)[178] or purchases of fertilizer by a non-farmer (suggestive of bomb-building)[179] could contribute to suspicion. Or perhaps prescription data combined with geolocation and telephone metadata could fairly accurately predict which patients abuse and resell their Schedule II

---

173 *See, e.g.,* Charles J. Ogletree et al., *Criminal Law: Coloring Punishment: Implicit Social Cognition and Criminal Justice,* IMPLICIT RACIAL BIAS ACROSS THE LAW 45 (Justin D. Levinson & Roger J. Smith eds., 2012).

174 HARCOURT, *supra* note 151.

175 Ferguson, *supra* note 77 at *2; Somini Sengupta, *Privacy Fears Grow as Cities Increase Surveillance,* N.Y. TIMES, October 13, 2013.

176 Somini Sengupta, *In Hot Pursuit of Numbers to Ward off Crime,* N.Y. TIMES BITS, June 19, 2013; Erica Goode, *Sending the Police Before There's a Crime,* N.Y. TIMES, August 15, 2011.

177 Elizabeth Joh, *Policing by Numbers: Big Data and the Fourth Amendment,* 89 U. WASH. L. REV. 35, 46, 56 (2014); Ferguson, *supra* note 77 at *4, *44; Illinois v. Wardlow, 528 U.S. 119, 124-25 (2000).

178 Ferguson, *supra* note 77 at __.

179 Ferguson, *supra* note 72 at 11.

narcotics. These are just a sampling of ideas. Once the imagination is permitted to flow freely, law enforcement could come up with countless ways for transaction records, store security camera videos, and geolocation data to be used separately or in combination to predict crime. Some of them will be able to meet high standards for correctly predicting crime, so the more important ethical questions involve issues other than efficacy.

Although data mining raises larger questions about criminal justice and privacy, the prospect of using data mining should not be casually dismissed before thoughtful consideration as to how it can be structured to make law enforcement more systematic and less discretionary.

B. Different Crimes

Some crimes offer little hope of detection without the aid of third party data. Malicious hacking, possession of child pornography, laundering money through gambling websites, and insider trading leave very few clues in the physical world.[180] As Rachel Barkow says, "Law enforcement cannot literally walk a beat [] in the business crime context."[181]

Privacy instincts that seem perfectly sensible in the context of street crime can have unfortunate unintended consequences outside of it. This is a story that has played out before, in the context of government subpoenas for first party records (our own papers). In *Boyd v. United States*[182], the Supreme Court ruled that a subpoena requiring the disclosure of our own documents violated both the Fourth and Fifth Amendments. *Boyd* is an old case involving importation records, and most of its holding has been seriously compromised by later case law, especially *Fisher v. United States*.[183] The rule from *Boyd* was destined to fail because its effects on law enforcement were severe and regressive. Railroad executives took advantage of the *Boyd* privilege to obstruct antitrust investigations, which were impossible to prove without documents. First party records were overprotected. We should not repeat the mistakes with third party records.[184]

---

[180] Indeed, Jack Goldsmith thinks that our concern over NSA surveillance will be moot soon enough when we realize that we need to enlist the government's help protecting against cyberattacks and cyberwar. Jack Goldsmith, *We Need an Invasive NSA,* THE NEW REPUBLIC, October 10, 2013.

[181] Rachel E. Barkow, *The New Policing of Business Crime*, 37 SEATTLE U. L. REV. 435, 464 (2014).

[182] 116 U.S. 616 (1886).

[183] 425 U.S. 391 (1976).

[184] Christopher Slobogin disagrees with this history, and has argued that the Court may never have treated subpoenas as outside the scope of the Fourth Amendment if it had known that the Fifth Amendment protections against subpoenas would be dismantled. SLOBOGIN, *supra* note 116 at 142. Slobogin would prefer to allow subpoenas for records in the course of investigating a business or corporation but to disallow them (most of the time) if the subpoenas are used to investigate individuals. *Id.* at 186. As a descriptive matter, I do not think this is correct. Slobogin himself points out that the opinion dismantling first party protections against subpoenas was decided on the same day as the *United States v. Miller,* the

Third party records play an important role in the early stages of white collar crime investigations. When the SEC started its insider trading investigation of the Galleon Group, a hedge fund that produced impossibly good results for its clients with the help of non-public information, the case started with a workup of its founder's telephone and email records.[185] Those records led the investigators to Roomy Khan, an Intel employee who fielded an unusual number of calls from the Galleon Group.[186] The investigators rightly expected Khan was funneling nonpublic information to Galleon's executives. The SEC and FBI eventually switched to non-data means of building cases by engaging in public surveillance, securing the cooperation of informants, and eventually using wiretaps.[187] But the investigation started with data.

The SEC has its own Quantitative Analytics Unit that uses algorithms to identify suspicious trades and overly successful investment performance.[188] Algorithms can also come into service to identify less sophisticated frauds (such as the sale of non-existent cars over several different Craigslist pages, or the use of scareware.)[189] And the calling behavior of prepaid "burner" cell phones can give away whether they are used for illicit purposes.[190]

The FBI is devoting a larger portion of its resources than ever before to the detection of white-collar crime.[191] This shift is admirable, especially since white-collar profiles run against the image of traditional bad guys. White-collar criminals evoke sympathies from their prosecutors that would be unimaginable in other criminal contexts. For example, Lanny Breuer aggressively faught corruption and financial fraud crimes as Assistant Attorney General, but even he hesitated before bringing charges. "In reaching every charging decision, we must take into account the effect of an indictment on innocent employees and shareholders," he explained. Collateral damages to employees and families are not given the same consideration when street criminals are charged with crimes.[192]

---

first case establishing the third party doctrine. *Id.* at 152. As a prescriptive matter, corporate criminal law investigations can often wind up with somebody going to jail, so it is not surprising that the courts have not wanted to build distinctions between corporate and non-corporate investigations into the Fourth Amendment doctrine.

185 *To Catch a Trader,* FRONTLINE. For a description of how analyses of networks can be used in policing, *see* Joh, *supra* note 177 at 46-47.

186 *To Catch a Trader, supra* note 185; William Alden, *Roomy Khan, Figure in Galleon Insider Case, Sentenced to One Year in Prison,* N.Y. TIMES (January 31, 2013).

187 Wiretaps are a relatively new tool applied to white collar crime. Patricia Hurtado, *FBI Pulls Off 'Perfect Hedge' to Nab New Insider Trading Class*, BLOOMBERG, December 19, 2011.

188 Barkow, *supra* note 181 at 451.

189 INTERNET COMPLAINT CRIME CTR., INTERNET CRIME REPORT 13 (2012).

190 Andrew Ferguson describes a great example of this from the investigation of a multi-million dollar heist in Sweden. Ferguson, *supra* note 77 at *46.

191 Barkow, *supra* note 181 at 469.

192 *Id.*

Many scholars and journalists have criticized the government for its lax enforcement and soft penalties in the white-collar space[193], but the demand for more enforcement is on a collision course with expanded Fourth Amendment privacy protections in third party records.[194] Law enforcement will need access to telephone and Internet communications data and other third party records in order to track down the financial crimes.

C. Proof of Disparate Treatment

One summer evening in the District of Columbia, a truck with two young black men caught the attention of a pair of police officers.[195] The truck had been sitting at an empty intersection for about twenty seconds, and the driver was looking intently at the lap of his passenger. The officers followed the truck for a short while until they could take advantage of a traffic violation—turning right without using a turn signal—to investigate further.[196] When the police approached the stopped truck, they saw proof of what they had suspected all along. The objects in the passenger's lap were two large bags of illegal drugs.[197]

The young men challenged the officers' decision to pull their vehicle over for such a trifling traffic infraction. The case, *Whren v. United States,* has come to be known as the precedent that allows police to make pretextual stops[198], but the challenge was more sophisticated than that. The petitioners did *not* argue that the officers' actual subjective intent mattered for the purposes of their Fourth Amendment challenge. Instead, they asked for an objective rule that would look for evidence that the police did not ordinarily enforce the law that formed the basis of probable cause for the traffic stop.[199]

The petitioners in *Whren* had an uphill battle to keep the law and ethics on their side. After all, the police arguably did exactly what was expected of them: they saw something suspicious (but which fell short of the reasonable suspicion standard required to conduct a stop), and they pursued their hunch using every legal means. Courts would struggle to condemn this type of action where the hunch actually turned out to be correct—a frequent problem when

---

193 MATT TAIBBI, THE DIVIDE: AMERICAN INJUSTICE IN THE AGE OF THE WEALTH GAP (2014).

194 Miriam Baer and Christopher Slobogin have foreseen this clash. Baer believes Justice Sotomayor's concurring opinion in *U.S. v. Jones* contains the seeds of a solution. Miriam H. Baer, *Secrecy, Intimacy, and Workable Rules: Justice Sotomayor Stakes Out the Middle Ground in* United States v. Jones, 123 YALE L. J. FORUM, March 24, 2014. Slobogin, in early work, distinguished between corporate and non-corporate records. The distinction may allow some white-collar investigations to proceed on lower standards. SLOBOGIN, *supra* note 116 at 186.

195 These are the facts of Whren v. United States, 517 U.S. 806, 808-09 (1996).

196 *Id.*

197 *Id.*

198 Christopher R. Dillon, *Whren v. United States and Pretextual Traffic Stops: The Supreme Court Declines to Plumb Collective Conscience of Police,* 38 B. C. L. REV. 737 (1997); Geoffrey S. Kay, *Whren v. United States: the Constitutionality of Pretextual Stops,* 58 LA. L. REV. 369 (1997).

199 *Whren*, 517 U.S. at 810.

Fourth Amendment rights are defended almost exclusively by the guilty. Because some hunches are good hunches, courts are reluctant to probe these types of actions too thoroughly.[200]

Still, *Whren v. United States* haunts the academy, and for good reason. If many laws are frequently broken and rarely enforced, the police have ample discretion to pull over whomever they choose. There is already evidence that drug possession prohibitions and other laws much less trivial than failing to use a turn signal are disproportionately enforced against poor and minority violators.[201] The mercy given to nearly everyone can be an invisible vehicle for bias against those unlucky few who are actually charged.[202]

Indeed, even Justice Scalia, whose opinion for the court in *Whren* openly mocked the petitioners' proposed test, was raddled enough to point out that there is another avenue for recourse if the police enforce the laws in disproportionate ways.[203] This alternative form of recourse, the Equal Protection clause, would not give the petitioners relief in the form of the exclusionary rule which, given their predicament, was their first priority.[204] But the bigger problem standing in the way of Whren's proposed rule, and Scalia's compromise, is operability. We rarely have information about the unlawful conduct that police do or should know about and choose not to enforce.[205]

This could change, and change radically, with the help of third party data. If law enforcement agencies begin to use algorithms to identify potential violations of the law, equal protection claimants will have a great resource at their disposal. Without data, the police will be able to plausibly deny that opportunities to enforce the law evenly presented themselves. With data, on the other hand, police will have to explain why they *didn't* act on opportunities to investigate or enforce a law when they could have.

Let me illustrate using the facts from *Whren*. If the *Whren* defendants had access to GPS data and ran a query for every instance in which a vehicle performed an illegal U-turn (e.g. not at an intersection) near a police car, the

---

200 Lerner, *supra* note 107.

201 Jamie Fellner, *Race, Drugs, and Law Enforcement in the United States,* 20 STAN. L. & POL'Y REV. 257, 266-72 (2009).

202 Dan Markel has explored this poignant relationship between mercy and equality. Dan Markel, *Against Mercy,* 88 MINN. L. REV. 1421 (2004). *See also* Joh, *supra* note 85 at 232 ("The problem is that we cannot accept the positive good of discretion without the attendant risks and potential harms.") Joh believes that losing the positive aspects of discretion is an inevitable cost if technology is used to limit police discretion. I am not so sure this is correct. Technology can be modified, over time, to incorporate new rules for positive discretion such that law-breakers in certain scenarios—cars that end their travel at a hospital, for example—are taken out of the enforcement pool.

203 Whren, 517 U.S. at 813.

204 Some scholars have argued it should. Brooks Holland, *Racial Profiling and a Punitive Exclusionary Rule,* 20 TEMPLE POL. & CIV. RTS. L. REV. 29 (2010).

205 Indeed, legal scholars have gone to great pains to try to estimate this missing data. *See* Katherine Barnes, *Assessing the Counterfactual: The Efficacy of Drug Interdiction Absent Racial Profiling,* 54 DUKE L. J. 1089 (2005).

Whren defendants would have strong evidence of racial bias if the data showed a great racial disparity in the proportion U-turns that were ticketed.[206]

D. Proposals

If the third party doctrine is dismantled, courts should not reject bulk data collection outright since pattern-driven data mining has the redistributive qualities described above. Over time, they can correct popular misconceptions about what seems "suspicious," and they can even correct themselves (through machine learning) when dynamics on the ground change. Algorithms cannot guarantee evenhanded treatment, but the decisions and profiles that are programmed into an algorithm are auditable and usually tested against real outcomes (actually finding evidence of a crime, for example). Thus, they are much more accountable and fixable than the ad hoc system courts rely on today.[207]

Christopher Slobogin argues that we should allow statute-authorized data mining programs as long as the most affected groups have "meaningful access to the legislative process" and the statute is applied even-handedly.[208] A legislative action requirement is overly restrictive. After all, Slobogin's proposal operates against a backdrop of traditional policing methods that require police to build their cases the usual ways—from tips and their own experiences. This status quo is even further from even-handededness and political accountability than law enforcement-initiated data mining. In the absence of an authorizing statute, it isn't clear why police departments should be prohibited from developing pattern-based data mining programs if they are effective and less likely to be skewed toward poor and minority populations. Indeed, political process might direct police attention toward the same politically weak

---

[206] In fact, third party records can open avenues to an entirely new sort of equal protection lawsuit. If third party data can adequately identify potential law-breakers, police forces will have to defend racial disparities not only in arrests but in investigatory stops and searches, too. I describe how this can be done in previous work. Bambauer, *supra* note 76.

[207] Some factors (like prior convictions and geography, for example) that might be used in an algorithm will correlate with race and class. But quantitative systems can test whether these factors are overweighted, and in any event will steer police to the factors that *do* matter (even if they happen to correlate with race) rather than allowing racial bias to play a role on top of noisy search patterns. In a different article, I proposed a theory to challenge the use of an algorithm that has disproportionate effects on a minority community *even when* the algorithm does not intentionally make use of race information. The idea is that if minorities bear a disproportionate number of fruitless searches or stops (false positives), use of the algorithm must be reduced. *Id.*

[208] Slobogin, *supra* note 17 at 16, 30-31; Christopher Slobogin, *Government Dragnets,* 73 L. & CONTEMP. PROB. 107 (2010). Richard Worf has also defended the democratic process as a reasonable means of regulating searches and seizures that are conducted without suspicion. Richard Worf, *The Case for Rational Basis Review of General Suspicionless Searches and Seizures,* 23 TOURO L. REV. 93 (2012). Worf comes out in support of a range of general searches and seizures that is much broader than the ones Slobogin considers, or the ones I consider here.

communities that already bear the costs of traditional policing. The politically powerful may prefer to avoid detection of the crimes that they commit—tax fraud, EPA violations, etc.—and design law to encourage detection of the crimes committed by the relatively powerless.[209]

Instead, a third party doctrine overhaul should develop a process to allow temporary collection of third party records for the sake of validating, and eventually applying, suspicion algorithms.[210] The legal scholars and criminologists who have devoted attention to this problem often converge on three key features for a legitimate data mining program[211]:

First, the program should require *accuracy*. Specifically, it should have a mechanism that creates incentives for decreasing Type I error (false alerts). And the government should be prohibited from actually using an algorithm until validation studies have shown that it has a low enough Type I error. (Slobogin suggests 50%.[212] But the threshold could depend on what the government aims to do. 50% seems right for arrests and searches, perhaps too high if the algorithm is used only to guide the use of resources for *Terry*-style questioning.[213]) To achieve the accuracy requirements, government must keep records on the outcomes of stops, searches, and arrests stemming from the program.

Second, the program should require *accountability*. All uses of pattern-driven algorithms should be subjected to logging so that auditors and criminal defendants can review how the government has used its data mining programs. This does not necessarily require transparency about the precise algorithm

---

[209] On the other hand, Bill Stuntz commented long ago that doesn't seem to explain much when it comes to law enforcement since taxpayers have not taken advantage of the legislative process to avoid accountability, e.g. Stuntz, *supra* note 57 at 1045.

[210] This collection could be understood under Scott Sundby's composite model that distinguishes "initatory intrusions" from "responsive intrusions." Scott E. Sundby, *Fourth Amendment Basics: Undoing the Mischief of* Camara *and* Terry, 72 MINN. L. REV. 383, 418-19 (1988). The former mark the beginning of an investigation before any individualized suspicion can accrue. By the time police are ready to use an algorithm to identify potential criminals, the algorithm will have to live up to the appropriate individualized suspicion thresholds.

[211] At least one of these three features is promoted in the following influential works: SLOBOGIN, *supra* note 116 at 195; ABA Standards, *supra* note 16 at 111; Zarsky, *supra* note 155; DEFENSE ADVANCED RESEARCH PROJECTS AGENCY, REPORT FROM THE INFORMATION SCIENCE AND TECHNOLOGY STUDY GROUP ON SECURITY AND PRIVACY: SECURITY WITH PRIVACY 10 (2002); Ed Felten, *Accountable Algorithms,* FREEDOM TO TINKER, September 12, 2014; Ed Felten, *Accountable Algorithms: An Example,* FREEDOM TO TINKER, September 13, 2014; PALANTIR, PALANTIR & LAW ENFORCEMENT: PROTECTING PRIVACY AND CIVIL LIBERTIES (2014).

[212] Slobogin, *supra* note 17.

[213] 50% might not be good enough if the crime is very common. Even a very accurate algorithm can force too many innocent people to undergo searches or arrests if the algorithm detects a high occurrence crime, like possession of marijuana. I have argued that the Fourth Amendment can and should watch out for this problem. Bambauer, *supra* note 76.

used to predict suspicious activity[214], but criminal defendants and the general public should have access to the information necessary to build confidence in the program. At the very least, criminal defendants should have access to a general model and audit logs comprehensive enough to ensure that the algorithm performed well, that the program did not introduce new race or gender biases, and that the government did not abuse discretion in deciding which positive alerts to pursue.[215]

Finally, the subpoena should require *division of labor*. Identified records should be left with the company or collected and maintained by an independent government entity. The company or independent agency can either run the analyses on behalf of the law enforcement department and provide results only for positive alerts, or the agency can prepare a database for law enforcement use (subject to the audit log requirement above) that has been stripped of direct identifiers.[216] Law enforcement would then make a follow-up request for identifiers on all positive alerts.

These limitations would go a long way to address the concerns and anxieties of critics. But for some scholars, the collection of third party records for the purposes of data analysis will never be consistent with the Constitution, despite precedents like *Smith*. Laura Donohue argues that collection of information falls within the definition of a Fourth Amendment search when done in bulk even if collection of the same type of information would not trigger a search for the occasional suspect, like the defendant in *Smith*. Donohue uses the popular, rarely examined rationale that a difference in quantity creates a difference in quality. That is, an occasional little peek at third party records—a searchlet, let's call it—was acceptable back when it was infeasible for police to do it to everybody, but now that we all face the prospect of this searchlet, it must count for Fourth Amendment purposes.

Spelling it out in this way lays bare how this type of reasoning inadvertently sows the seeds for continued inequity in the criminal justice system. If collecting data on all of us is unconstitutional, even lowlifes like Smith deserve protection. On the other hand, if courts put their energy instead into determining what makes government access to personal data invasive and

---

[214] In fact, I do not even think the algorithm should have to have interperability. One of the benefits of machine learning is that it can assess and revise a model based on relationships between so many variables that the best algorithms may not even look like the standard OLS regressions. Tal Zarsky does not think those benefits are worth the risks. *See* Zarsky, *supra* note 155.

[215] The ABA recommends data use logging within their framework, too. ABA Standards, *supra* note 16 at 25.

[216] The data need not be "anonymized" or "deidentified" as that term of art is used in debates about reidentification risk. *Compare* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization,* 57 UCLA L. REV. 1701 (2010) *with* Jane Yakowitz, *Tragedy of the Data Commons,* 25 HARV. J. L. & TECH. 1 (2011). The removal of direct identifiers paired with detailed logs about data use should reduce most of the risks that a law enforcement agent will cheat.

threatening in the first place, whether in small or large quantities, they are more likely to find a rule that protects all citizens equally. One of the greatest threats is arbitrary or biased deployment of searches and seizures. Bulk collection could mitigate, rather than exacerbate, this problem when the data is used to make investigations more systematic, consistent, and accountable.

Thus, bulk data collection without any constraints on the subsequent use for criminal investigation purposes should be treated as a Fourth Amendment search for the same reasons that suspect-driven investigations like *Davis* should be treated as searches: because they maximally surveil the population without constraining the discretion of police. But police departments that set up a pattern-driven data mining program with basic safeguards for accuracy, accountability, and division of labor should be treated as reasonable searches under the well-established special needs doctrine that applies to checkpoints.[217] The jurisprudence on checkpoints has already noted with approval that the checkpoints found constitutional under the special needs doctrine are governed by internal guidelines that minimize the discretion of the officers implementing the scheme.[218]

The next Part will consider the final counterweight to Fourth Amendment privacy: the First Amendment. Occasionally a third party will positively want to disclose evidence of its customers' criminal wrongdoing to the government. Modifications to the third party doctrine must anticipate the clashes between the third party's speech interests and the consumer's privacy interests.

VIII. THE FOURTH AMENDMENT V. THE FIRST AMENDMENT

In *DRN v. Herbert,* the plaintiff, an automatic license plate reading service, challenged a Utah law prohibiting the use of automatic license plate readers.[219] The law quite obviously interfered with DRN's business model, and took refuge in the First Amendment to enjoin the law's enforcement.

For purposes of this exploration, I will assume DRN's speech interests in taking pictures of license plates and matching the images to public databases are valid. While the existence of a speech interest doesn't end the analysis (the law may be narrowly tailored to a sufficiently important privacy interests to withstand scrutiny), the plaintiffs' First Amendment challenge is probably well-founded. [220]

---

[217] Mich. Dept. of State Police v. Sitz, 496 U.S. 444, 448-49 (1990); Brown v. Texas, 443 U.S. 47 (1979); United States v. Martinez-Fuerte, 428 U.S. 543 (1976).

[218] *Sitz,* 496 U.S. at 452; *Martinez-Fuerte*, 428 U.S. at 559.

[219] DRN v. Herbert, No. 2:14-cv-00099-CW (Utah 2014) (available at http://www.scribd.com/doc/207191306/DRN-v-Herbert-Brief).

[220] At least I think so. Jane Bambauer, *Is Data Speech?,* 66 STAN. L. REV. 57 (2014). *But see* Neil Richards, *Why Data Privacy Law Is (Mostly) Constitutional,* __ WM. & MARY L. REV. __ (forthcoming 2015).

However, the case has an interesting wrinkle—one that was unnecessary for the plaintiffs to draw out. DRN made clear that one of its objectives was to disclose the license plate information to law enforcement "for purposes that range from utilizing near real-time alerts for locating missing persons and stolen vehicles to the use of historical license-plate data to solve major crimes such as child abductions." Thus, DRN claims a speech interest in providing data to law enforcement.

DRN may have assumed that a speech interest would be bolstered by their reference to law enforcement goals, but with the third party doctrine on thin ice, it unwittingly waded into a constitutional quagmire. What is the greater constitutional imperative: a First Amendment right to talk to the government, or a Fourth Amendment right to keep the government's ears shut?

Although First Amendment speech rights are robust, they are not unlimited. Many statutes prohibit doctors[221], schools[222], and telecommunications providers[223] from disclosing the personal information of their clients to *anybody* (let alone the government), and these sorts of narrowly-tailored statutes are presumptively constitutional. They serve significant interests in confidentiality. Confidentiality laws are appropriate for fiduciary relationships (doctor-patient, lawyer-client, priest-confessor) where broader societal interests are served by inducing candor between the counselor and the counseled. These confidentiality laws seem to live up to First Amendment scrutiny, so there's no reason to think that the same types of confidentiality interests can't interfere with disclosures to the government, even when the service-provider (the doctor, the lawyer, the priest) positively *wants* to disclose criminal conduct to the government. But these fiduciary duties are rare. [224]

---

[221] Health Insurance Portability and Accountability Act, 45 CFR §§164.502(a), 164.512(f).

[222] Federal Education Rights and Privacy Act, 34 CFR §§99.30-99.31.

[223] The prohibition against disclosures to the government contained in the Wiretap Act, the Stored Communications Act, and the Pen Register Act are an interesting study. When the laws protect the *contents* of communications, they obligate telecommunications providers to keep conversations confidential. Stored Communications Act, 18 U.S.C. §2702(a); Wiretap Act, 18 U.S.C. 2511.

[224] Christopher Slobogin, James Grimmelmann, and Jack Balkin have gone much further by arguing that any company that provides a service of practical necessity (e.g. telecommunications, or Google's Internet search function) should be treated as information fiduciaries, and should have to conform to traditional duties of confidentiality. SLOBOGIN, *supra* note 116 at 158, 161; James Grimmelmann, *Speech Engines,* 98 MINN. L. REV. 868 (2014); Jack Balkin, *Information Fiduciaries in the Digital Age,* BALKINIZATION, March 5, 2014. These arguments sweep much broader than the forms of confidentiality that are likely to withstand First Amendment scrutiny. Duties of confidentiality (and the other fiduciary duties that are usually bundled alongside confidentiality) are justifiable for professions in which there is significant societal benefit from encouraging relationships of trust and candor, and for which the professional is compensated for taking on these additional duties of care. Legal relationships of trust are designed to help the *fiduciaries*, by ensuring that there will be a market for their services. Tamar Frankel, *Definition of "Fiduciary Duties",* THE NEW PALGRAVE DICTIONARY OF ECONOMICS AND THE LAW 127-128. These qualities describe only a narrow set of industries that need confidentiality rules to induce information-sharing.

The speech interests of a company may also be trumped by the speech interests of their customers. When journalists and their sources are the subjects of criminal investigation, the public will have heightened interest to be sure that the state is not exploiting the criminal processes in order to squelch unwanted press. This was a concern, for example, when the Justice Department obtained two months' worth of telephone records of Associated Press journalists.[225]

However, in situations involving something less than a fiduciary relationship or the speech interests of journalists, the clash between a speaker's interests and the customer's interests should be resolved in favor of the speaker for four reasons.

First, finding otherwise would clash badly with *United States v. White*, which reaffirmed the longstanding misplaced trust doctrine. Recall from Part I that *White* decided we all take our chances that our friends and colleagues will go running to the government, or may be cooperating with them already. If our trust is misplaced, and our friend carries out an actual betrayal, the Fourth Amendment has always stood back and allowed the incriminating information to pass to the government.

Second, when a business decides for whatever reason to disclose evidence of criminal behavior to the government, the privacy interests of their customers are at their nadir. Businesses are unlikely to share material that is sensitive-but-legal. Instead, the disclosure to the government will occur when the company has strong evidence of a crime. This is the sort of sui generis criminal detection that courts tend to separate from the definition of "search."[226] A voluntary disclosure of customer data will usually be a trustworthy signal—an auto-corroborated tip.

Third, as a practical matter, incentives of businesses are usually closely aligned to their clients.[227] With the exception of companies like DRN that operate in areas where relationships between businesses and their customers have completely broken down (lenders and borrowers in default, e.g.), most companies do not want to irritate their paying customer base. Thus, Google and Qwest, for example have resisted subpoenas and FISA gag orders in order to vindicate the privacy interests of their customers.[228] Businesses need no extra incentive to collude with their paying customers who happen to engage in crime.

Finally, because the First Amendment also incorporates a (poorly understood) right of petition, companies may have two independent bases for

---

[225] Mark Sherman, *Government Obtains Wide AP Phone Records in Probe,* ASSOC. PRESS, May 13, 2013. These types of investigations run against federal internal investigation policies. Brad A. Greenberg, *The Federal Media Shield Folly,* 91 WASH. U. L. REV. 437, 450 (2013).

[226] Illinois v. Caballes, 543 U.S. 405 (2005).

[227] Orin Kerr has made this point. Orin Kerr, *Defending the Third-Party Doctrine: A Response to Epstein and Murphy,* 24 BERK. TECH. L. J. 1229, 1235 (2009).

[228] Kim Zetter, *Google Challenges FISA Gag Orders on Free Speech Grounds,* WIRED, June 18, 2013.

sharing information with the government: speech rights, and the right to petition the government for help. Each of these fortifies the other.

However, it will be important for courts to monitor whether a company's disclosure of customer records is truly voluntary. What looks like voluntary disclosure may be the result of behind-the-scenes pressure from government agencies.[229] The government may design incentives so that businesses will choose to disclose records more often. Indeed, the government already does this to some extent by paying fees for searches of privately-held records.[230] The government would be motivated to make voluntary disclosures more attractive if the third party doctrine is thoroughly gutted.

If businesses that engage in regular snitching get more favorable treatment from their government regulators or from public grants programs, the courts could take a broad interpretation of "state action" and probe whether the disclosures are meaningfully independent from the government.[231] On the other hand, some amount of government pressure may be consistent with tactics historically deployed in order to secure the help of government informants. For example the SEC uses game theoretic tactics by paying whistleblowers for tips leading to fraud charges, and it promises leniency to corporate employees who turn the company in before their co-workers.[232]

Putting these difficult state action issues aside, revisions to the third party doctrine should allow companies to voluntarily disclose their business records unless common law or statutory prohibitions (consonant with the First Amendment) forbid the disclosure.

CONCLUSION

The third party doctrine has become the Fourth Amendment's supervillain. It puts no constitutional limits on dragnet data collection. And it permits suspect-in investigations that can be motivated by a hunch or something worse. But in the rush to correct these flaws, reformers risk introducing new fault lines into the Fourth Amendment that will undermine its ultimate goals.

So far, critics of the third party doctrine have called for a warrant requirement to protect personal information contained in third party records. This type of reform will block innovations to law enforcement and entrench traditional forms of investigation by force-fitting the system of individualized

---

[229] Derek Bambauer, *Jawboning,* (work in progress); Balkin, *supra* note 32.

[230] Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Date for Law Enforcement,* 29 N.C. J. INT'L L. & COM. REG. 595, 596 (2004).

[231] *See* Derek Bambauer, *Orwell's Armchair*, 79 U. CHI. L. REV. 863 (2012).

[232] U.S. SEC. & EXCH. COMM'N, ANNUAL REPORT ON THE DODD- FRANK WISTLEBLOWER PROGRAM: FISCAL YEAR 2012 (2012); Barkow, *supra* note 181 at 439.

suspicion onto data-driven investigation methods. These reforms will have severe opportunity costs. They will save us from the risks of innovation, but they will also hinder us from harnessing the justice-enhancing power of data. Given the current inequity, inaccuracy, and lack of accountability in law enforcement, courts should not pass up an opportunity to make systemic improvements.

Indeed, well-intentioned third party reforms might not even accomplish their basic goal of constraining government surveillance power. Consider Sudafed. Its active ingredient, pseudophedrine, is the base for most homemade methamphetamines, as every *Breaking Bad* fan would know. In a parallel universe, this Article would explore the ethics and Fourth Amendment legality of government access to drug store purchase records to find suspiciously large acquisitions of pseudophedrine. Instead, Congress passed the Combat Methamphetamine Epidemic Act of 2005, which prohibited purchases of pseudophedrine in large quantities by adults and in any quantity by minors. It also compelled the collection and disclosure of identifying information for the purchases of small quantities.[233]

This comprehensive regulatory scheme has attracted very little criticism on Fourth Amendment privacy grounds, perhaps because the scheme is consistent with the modern regulatory state.[234] The experience with Sudafed demonstrates the danger of changing the third party doctrine without considering the larger picture. If the government is denied access to third party records that it needs to effectively enforce a law, it could reach the same result through comprehensive regulation and disclosure laws. This is hardly the better outcome on the basis of privacy, efficiency, or autonomy.

Although this Article has covered a wide landscape of potential pitfalls, the restructuring of the third party doctrine can avoid them all as long as it provides a workable path to third party records in three instances.

For crime-out investigations, police should be able to access third party records without probable cause or reasonable suspicion. The crime-out investigatory process reduces most of the harms that come from unfettered data access and may simultaneously promote the interests of innocent, wrongly accused targets.

For pattern-driven data mining programs, courts should permit law enforcement agencies to collect and analyze bulk records as long as there are means to test whether the programs are effective and evenhanded. These programs can contribute to a more equitable distribution of law enforcement investigations and prosecutions.

---

[233] Combat Methamphetamine Epidemic Act of 2005, H.R. 3199 (2005).

[234] Some have objected to the restrictions on liberty to buy over-the-counter drugs and the propensity for false arrests. Jacob Sollum, *One Box of Sudafed Over the Line: Florida Woman Arrested for Trying to Relieve Allergy Symptoms,* REASON.COM, July 28, 2014. But there has been no analysis of how this type of regulatory scheme would interact with a reformed third party doctrine.

Finally, unless a confidentiality statute is in place, individuals and businesses should be free to voluntarily share records in their control with the government out of deference to their First Amendment rights.

To put it even more simply, courts and lawmakers do not need to change very much about the third party doctrine to avoid its worst qualities and preserve its best ones. The most pressing privacy problems can be solved by disallowing suspect-driven investigations lacking individualized suspicion and by prohibiting unconstrained mass data collections. If Fourth Amendment or statutory law closes off these exploitative uses of third party records, it will steer law enforcement toward more accountable uses of powerful third party data resources.

* * *