OTHER PEOPLE'S PAPERS

Jane Bambauer[*]

NOTE: This is an early draft.
Please ask the author for the most recent version before quoting.

The third party doctrine, which crops business records out of the scope of Fourth Amendment protection, was incoherent from the start and bound for reform. This Article explores some of the potential pitfalls that ought to be avoided as we reshape the doctrine. In addition to the usual clash between criminal law enforcement and privacy, this Article identifies some previously overlooked societal interests that compete with Fourth Amendment privacy. If it isn't crafted right, a new third party doctrine could clash with the due process interests of the accused (if the government is unable to easily access exculpating evidence), equal protection (by forcing criminal investigations to focus time and attention disproportionately in poor and minority neighborhoods), and the First Amendment (by hindering the speech of a business that wishes to report illegal behavior of its own volition.)

INTRODUCTION

The third party doctrine will be dismantled soon, and for good reason. It permits the government to access business records and transactional data

[*] 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, Marc Blitz, James Cooper, Alex Marthews, Sasha Romanosky, Bruce Kobayashi, Woodrow Hartzog, Guz Hurwitz, Berin Szoka, Geoffrey Manne, Tom Lenard, Bruce Johnsen, Margaret Hu, Dan Caprio, Daniel Gilman, Tim Brennan, Deven McGraw, Joshua Fairfield, and Kiel Brennan-Marquez. This research was generously supported by the Law and Economics Center at the George Mason University College of Law.

about a company's consumers without implicating the Fourth Amendment even when the company would prefer not to cooperate. [1] The third party doctrine always strained the logic and common sense of search and seizure law[2], and the National Security Administration's bulk collections of telephonic metadata have reinvigorated the demand for reform. [3] The law clearly 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[4] and the practical consequences of a big disruption to police practices[5], but the debate has obscured the ultimate question: how do we want law enforcement to build their cases?[6]

Legal scholars have considered the third party doctrine and its alternatives using a cramped analytical model. They balance the presumptively large privacy interests against general interests in crime-fighting. Consequently, popular proposals to reform the third party doctrine have looked backwards for solutions, embracing rules that restrict access to data based on the sensitivity of the data, and that reify traditional hierarchies of individualized suspicion.[7] These solutions revert law enforcement to an environment where they must conduct personal, observation-driven investigations as they have historically done. They unwittingly promote an outdated criminal investigation system riddled with inequities and error.

---

[1] *U.S. v. Miller*, 425 U.S. 435 (1976).

[2] Andrew D. Selbst, *Contextual Expectations of Privacy*, 35 CARDOZO L. REV. 643, 669-77 (2013).

[3] *See, e.g.,* Ewen Macaskill & Gabriel Dance, *NSA Files: Decoded*, THE GUARDIAN (Nov. 1, 2013),http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1.

[4] DANIEL SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY (2011)

[5] 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);

[6] 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). This article will go one step further by exploring which types of development constitutional law should support, and which types it should not.

[7] For example, The ABA Standards for Criminal Justice recommends that courts categorize records based on their sensitivity, and then apply increasingly heightened procedural safeguards for increasingly sensitive information. See, e.g., Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MARYLAND L. REV. 101 (2011). 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.) Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations,* 24 BERK. TECH. L. J. 1199 (2009).

The scholarly debate has failed to appreciate how our data-rich environment can be used to promote justice in ways that were impossible a generation ago. This Article will show that some of the thorniest problems in criminal justice are orthogonal to privacy. Some problems are *mitigated* rather than exacerbated by law enforcement access to data.

For example, if the police have built a case against a person who is wrongly accused of committing a crime, he should expect that the police will query cell phone time and location data in order to see if a witness or an alternative suspect was at the crime scene at the relevant time. This is the sort of search that only large data archives can facilitate. Although a filter will technically fish through everyone's data in search of the customers who were in the right place at the right time, the privacy harm from an automated rummaging through data should not necessarily outweigh the costs to criminal suspects if the state is barred from accessing exculpating information.

Third party records can also facilitate pattern-driven investigations. These use algorithms to detect which individuals might be engaged in criminal activity. Because pattern-based investigations operate on large databases consisting mostly of innocent data and have great potential for error, they understandably attract controversy. But, with some sensible limits, pattern-driven investigation can redistribute the costs and consequences of criminal law enforcement more equitably by decreasing our dependence on police discretion. Since pattern-driven investigations operate isolated from the identity or demographics of the suspects, they reduce the opportunity for implicit bias and animus to infect an investigation. More bluntly, if law enforcement is prohibited from using data-driven policing, society will entrench the race- and class-based disparities that currently blight criminal investigation. If we insist that the police build cases organically from their individual observations about how a person moved ("furtively") or how a person behaved ("nervously"), then cases will continue to accrue where the cops are: in predominantly poor and minority neighborhoods.

In short, third party records have the potential to dramatically change criminal investigations by providing new routes for suspects to prove their innocence, allowing criminal profiles to be applied to the population in a more even-handed way, and facilitating more crime-out investigations.[8] Each of these uses of third party data differ in important ways from the dragnet practices that have inspired so much hostility to the third party doctrine, and each deserves to be protected from Fourth Amendment reforms.

That said, none of these innovations in criminal law enforcement require the government to have unfettered access to all third party records, as it does now. Rather, this Article suggests that reforms should be careful not to stymie the collection or use of third party records that promote not only law

[8] Crime-out investigations study clues from an already-committed crime. I explain why this category of investigations is special in Part III.

enforcement, but important civil rights and civil liberties interests as well. Our privacy interest in other people's papers is not unbounded.

Throughout, this Article analyzes how each of these overlooked interests could affect the third party doctrine's replacement. It pays special attention to the problems in the proposals put forward by Christopher Slobogin[9] and by the American Bar Association[10] 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. Both proposals also enjoy well-deserved recognition from the law and policy communities. However, both will pose unnecessary conflicts with some worthwhile modern policing methods.

The Article proceeds as follows: Part I explains why the third party doctrine is unpopular and theoretically unstable. Part II identifies four potential privacy interests in the government's collection and unfettered use of third party records and assesses their strength. Part III considers the law enforcement interests that predictably run up against Fourth Amendment privacy interests, and demonstrates why courts have extraordinary difficulty striking a balance. Parts IV through VII explore some of the interests that can come into conflict with new constitutional restrictions on government access to records. They are (IV) law enforcement interests in specifically identified, already-committed crimes; (V) due process interests of criminal suspects; (VI) the equal protection interests of society; and (VII) First Amendment interests of the third parties. Each runs counter to Fourth Amendment interests in privacy. Each section suggests how a reformed third party doctrine can avoid these unintended consequences.

Building cases through unfettered, unaccounted access to other people's papers 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* and again in *Smith v. Maryland*, the Supreme Court decided that government access to business records is not a search. Thus, the government could access 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 that Americans do not and should not harbor any expectation of privacy in the numbers they dial because each caller knows that the telephone company uses this information to complete their calls and logs it

[9] Slobogin, *supra* note __.

[10] THE AMERICAN BAR ASSOCIATION, LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS STANDARDS (2013).

to facilitate billing and services. 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.) 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 *United States v. White,* for example, the Court decided that a criminal defendant had no privacy interest in a conversation he had with a snitch who was bugged and working with the government.[11] *White* is emblematic of the Supreme Court's misplaced trust doctrine which had been well-established by the time *Smith* came down the pipes. For the Court, *Smith* was just a corollary to *White*: personal information conveyed to a business or some 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.

In the wake of Edward Snowden's leaks about the NSA's telephonic metadata programs, *Smith* 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.*[12] 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 government's actually having the voluntary cooperation of White's confidant. A theoretical possibility of snitching is not enough, on its own, to remove an expectation of privacy. In other words, in order to fit within the misplaced trust doctrine, the trust had to actually be misplaced.

The third party doctrine, by contrast, does not require the 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[13], and the NSA telephonic metadata program relies on compulsion, too. Verizon and other telecommunications companies have no

---

11 401 U.S. 745 (1971).

12 *See* 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).

13 16 U.S.C. §§3121 et seq.

choice but to hand their records over to the government.[14] Moreover, telecommunications providers are legally obligated to keep the government's confidences through gag orders that accompany the orders compelling the provision of metadata records.[15] Thus, the reasoning of *Smith* is 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 that risk comes to pass.[16]

Smith was never popular among scholars[17], but the sweeping collection programs brought to light by Edward 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. Counting heads on the *U.S. v. Jones* opinion confirms that five out of the nine sitting justices believe the collection of 28 days worth of geo-location data constituted a search even without a technical trespass[18], and Justice Sotomayor's concurring opinion painted a target on the third party doctrine. *Smith* is on death row.

It might be there for a while. Most recognize 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.

Thus, scholars have tinkered with compromises to the Warrant Clause to find a solution to the incoherence of the third party doctrine.[19] Some have suggested requiring either reasonable suspicion, probable cause, or full-fledged warrants depending on the sensitivity of the records.[20] Others suggest increasing procedural safeguards when the police seek greater quantities of information.[21]

---

[14] 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.

[15] Jack Balkin, *Old School/New School Speech Regulation,* __ HARV. L. REV. __

[16] Orin Kerr agrees that the Court never explained why we assume that people "Assume the risk" when they disclose information to a third party. He says "assumption of risk is a result rather than a rationale." Orin Kerr, *The Case for the third party doctrine,* 107 MICH. L. REV. 561, 564 (2009).

[17] 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).

[18] 132 S. Ct. 945 (2012)

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

[20] Stephen Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULLETIN 39, 44 (2011). Henderson's work forms the core of the ABA's proposals.

[21] Deven Desai, *Constitutional Limits on Surveillance: Associational Freedom in the Age of Data Hoarding,* __ NOTRE DAME L. REV. __; Slobogin, *supra* note __ at __.

The trouble for all these scholars (and for myself) is that the Fourth Amendment has no first principles. The Fourth Amendment protects the people from law enforcement, and yet law enforcement is one of the government's "most basic tasks."[22] Historically, 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*. But the accretion of third party records has 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."[23] With stakes that high, courts were naturally hesitant to call something that would colloquially be called a search a "search."[24]

If courts open the definition of "search" to more things, they must have the latitude to engage the "reasonableness" clause of the Fourth Amendment without provoking the Warrant Clause. Reasonableness will be the touchstone. But of course, "reasonableness" isn't stone at all. It is a soup of competing interests.[25]

This Article will not offer a comprehensive proposal to supplant the third party doctrine. Instead, it will identify some of the pitfalls that have been overlooked in the rush to replace it. The next Part considers privacy interests in third party records and some of the conceptual difficulties they raise. The Parts that follow will explore some of the counterweights that push against zealous protection of these privacy interests.

II. THE FOURTH AMENDMENT INTERESTS IN PRIVACY

The last Part showed that 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 of a home or the tapping of a phone line.

Privacy objections to the collection and use of third party records can be organized into five categories of harm. They are: 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

---

[22] Gregg v. Georgia, 428 U.S. 153, 226 (1976) (White, J., concurring).
[23] AKHIL AMAR, THE BILL OF RIGHTS 68-77 (2006).
[24] Indeed, the reasoning in *White v. United States* for allowing the government to use secret agents hinged on the practical effects that the opposite rule would have for law enforcement.
[25] This problem is on naked display in the cell phone search incident to arrest cases currently before the court. 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*).

adds an additional layer of risk); obstruction (privacy can help thwart the unjust application of criminal laws as well as the application of unjust criminal laws); 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. 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 potentially abuse. But even apart from the potential for abuse, collection *at all* can cause unease from the lack of consumer control.

The problems of collection (apart from abuse) are difficult to defend 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[26], which 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.[27] The federal government is the nation's largest employer. The combined employment at all levels of government accounts for 7% of American jobs.[28] 30% of Americans share their health information with their public health insurers (Medicare or Medicaid.)[29] 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

[26] 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).

[27] 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." (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." Privacy's Problem at 1019. But ultimately he focuses on force and coercion rather than information gathering. At 1020, 1034. Stuntz ignored some of the differences between police power that I identify here (the potential for aggregation, the discretion of police in directing charges and prosecutions for vindictive or inappropriate reasons.)

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

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

know what we've written, and in cities with publicly-provided Internet service, the government maintains ISP records.[30]

Each of these examples theoretically can be distinguished from compelled disclosure of records to the government since they involve *quid pro quo* bargains between the government and the governed. 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 reasons. 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.[31] 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.[32] Cities considering congestion taxes for environmental reasons could force taxpayers to transmit detailed geolocation data to the government.[33] Even the Federal Trade Commission, the self-appointed privacy enforcer, uses its subpoena power to collect consumer data and investigate fraudulent practices. Thus, though it seems that the third party doctrine allows the government to circuitously collect from private industry what it couldn't collect itself, 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 noncollection 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 thoroughly data-dependent.

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. [34] In other words, if law

---

[30] As is the case in Culver City, California, and Chattanooga, Tennessee.

[31] 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).

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

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

[34] That said, the third party doctrine does go well beyond standard government information collection practices that we have come to allow. First, few existing government information collection programs have the potential to expose our associations quite as readily as the third

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 law enforcement to harass their rivals and dissenters. Heightened potential for abuse is considered as its own separate privacy concern that I treat 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. This power is considered below as part of the obstructionist and hassle interests in privacy.

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.[35]

B. Risk of Misuse

Much more disconcerting than collection is the risk of government misuse, both intentional and accidental. Any government agent with access to sensitive information might make an inappropriate query and learn something he shouldn't, as when an internal audit uncovered evidence that NSA employees and contractors had looked up their friends and ex-girlfriends.[36] These illegitimate queries are examples of abuse of access. Alternatively, the agency might have a data breach or spill and expose the information to others. These risks of data breach and abusive access are not unique to law enforcement databases, but they are important risks nonetheless.

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

party records held by telecommunications providers. Thus, freedom of association should be an important focal point for privacy scholars redesigning the third party doctrine. Desai, *supra* note __ at __.

[35] Alex Marthews & Catherine Tucker, *Government Surveillance and Internet Search Behavior.*

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

the leaks of government information for unrelated crimes[37], and the IRS's ideologically tilted treatment of non-profit tax treatment.[38]

If those tactics fail, the officer could disclose embarrassing details or use sensitive information to harass the victim.[39] Moreover, the officer might 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. 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.[40]

C. Aggregation

Even if governments at various levels regularly collect sensitive data about its constituents, the aggregation of *all* data presents additional privacy aggravations. 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.[41] First, the combination of different types of information might be more revealing because of relationships between the information.[42] And even without those inferences, 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. Obstruction

The dominant conception of privacy argues that because we all engage in sensitive yet perfectly legal activities (health decisions, political dissent, sexual

---

[37] Emily Bazelon, *Obama's War on Journalists,* SLATE.

[38] Lois G. Lerner, *Emails Show IRS' Lois Lerner Specifically Targeted Tea Party,* WASH. TIMES (September 12, 2013); *But see New Records: IRS Targeted Progressive Groups More Extensively Than Tea Party,* HUFFINGTON POST (April 23, 2014).

[39] 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 law enforcement purposes.

[40] Desai, *supra* note __.

[41] "the 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).

[42] 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.

behavior, and so forth), privacy is important even if we have nothing to hide.[43] 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.[44] 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.

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. 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, or copyright infringement). Obstructionist privacy instincts explain why the public reacts strongly to highly accurate means of criminal detection, such as red light cameras and speed traps.[45] 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.[46]

Privacy provides a convenient surface to wage a counterattack against unjust laws, but using it in this way is likely to be counterproductive. First, if a criminal law is unjust, the best solution is to modify the substantive law. Leaving the crime on the books invites rare, discretionary enforcement. Moreover, as detection for other, more serious crimes becomes costlier, prosecutors and lawmakers are likely 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 statutes or a

---

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

[44] ALAN WESTIN, PRIVACY AND FREEDOM (1970) ("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).

[45] *See* Ilya Somin, *Speed Limits, Immigration, and the Duty to Obey the Law,* THE VOLOKH CONSPIRACY (April 17, 2014).

[46] Jane Bambauer, *Defending the Dog* at 1205. 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). 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.

few statutes with greater breadth to give police more opportunities to make legal arrests.[47] Privacy obstructions unwittingly contribute to the arms race.[48]

Moreover, there is no reason to think that there are enough Aaron Swartzes to make up for the Meyer Lanskys and other dangerous criminals who benefit from the same procedural subterfuge. The best way to test whether a criminal statute is appropriately defined and conscribed, and that its penalty is fair, is to aim for greater, more evenly distributed detection. If the entire electorate runs the risk of feeling the pain of enforcement, the punishment is more likely to be proportional to the crime. The senator's daughter test provides 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.[49]

Finally, even if we wanted to decrease detection in order to protect the interests of persecuted political dissidents or whistle-blowers, constricting government access to third party records might counterintuitively exacerbate the problem. 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 and behaves more or less like everyone else. A warrant requirement (or something like it) will prevent the defendant or the investigator's superiors from having the data to show that the police had willfully ignored similar suspicious behaviors in other people.

Consider one example, coming from data that the government does produce. 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.[50] 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.[51] 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.

This is one of the few instances where 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

---

[47] Stuntz, *supra* note __ 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.).

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

[49] Jane Bambauer, *Defending the Dog* at 1209-10 (using the chance that the senator's daughter will get caught as a gauge for evenhanded enforcement).

[50] Bowman and Heise, *Rebellion II, supra* note __ at 537.

[51] *Id.*

and systematically chooses to ignore, the consequences could have a cleansing effect on discretion. For example, the defendant in *Whren v. United States* was pulled over for making an illegal u-turn, though the actual motivation was to investigate whether Whren and his friends had drugs. The government acknowledged that the true motivation for making the traffic stop was to follow up on a slightly-more-than-hunch that the youths were up to no good. Defense counsel insisted that race played a role (Whren was black.) Whren's lawyers argued that a defendant should be able to challenge a traffic stop, *even if* the defendant had violated the law, if the stop was not usually enforced. Justice Scalia dismissed that argument with a breezy conclusion that Whren's empirical, objective test is *actually* subjective, and in any case impractical. If Whren had had access to data showing that the police who pulled him over had observed and ignored the illegal U-turns of all other drivers, Whren's lawyers' proposed test would have at least been operable. Regardless of the Fourth Amendment meaning of such evidence, it would surely be useful for any police department or society committed to studying and conscribing the use of discretion.

E. 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 impose significant costs in terms of time, humiliation, and insecurity. I have called these costs "hassle" in other work.[52]

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.[53] 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.[54]

---

[52] Jane Bambauer, *Hassle,* 113 MICH. L. REV. __ (2014)

[53] Andrew Guthrie Feguson, *Big Data and Predictive Reasonable Suspicion,* __ U. PENN. L. REV. __ (forthcoming 2014).

[54] 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.

Next we move to the interests that run against Fourth Amendment privacy values, the first of which is the most often frequently invoked: security. We will then move on to consider other interests that are incorporated into the Fourth Amendment balance less frequently. I identified and probed the privacy interests because some of the themes reemerge. While many privacy interests are significant, some dissolve into problems of unchecked discretion. In the end, we might consider restricting police and prosecutor discretion, if possible, in order to achieve the fairness and political neutrality that drive privacy concerns.[55]

III. THE FOURTH AMENDMENT V. PERSONAL SECURITY

If the government's collection and use of third party records requires Fourth Amendment balancing under the Reasonableness Clause (as opposed to having to comply with the Warrant Clause), crafting the right rule requires 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.[56] 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.[57] Some people care deeply about control of their personal information, others don't, and the two camps do not understand each other.[58]

---

[55] William J. Mertens, *The Fourth Amendment and the Control of Police Discretion*

[56] United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring) (balancing "privacy and public safety in a comprehensive way"); Daniel J. Solove, *Data Mining and the Security-Liberty Debate,* 75 U. CHI. L. REV. 343, 344 (2008); Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations,* 24 BERK. TECH. L. J. 1199, 1202 (2009).

[57] Alessandro Acquisti, Leslie John & George Loewenstein, *What Is Privacy Worth?*; 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).

[58] Hassle has the best chance of garnering consistent reactions from Americans since most people agree that there is some liberty interest at stake if the innocent are stopped, searched, or arrested. However, hassle is no walk in the park for measuring privacy harm, either. It introduces some nightmare accounting. Each involuntary interaction with the police would have to be weighted appropriately. The first *Terry* stop probably would not cause a lot of harm if conducted respectfully and lasts only a short time. But the second and third would be experienced differently. The intensity of the hassle would grow exponentially with each encounter. And the intensity of each individual seizure or search introduces variability as well

Even if we did have a consistent and generally accepted measure of privacy costs, our tolerances for those privacy invasions to fight crime are likely to run the gamut. Each individual's tolerance will depend on his attitude about the specific crime investigated[59] 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[60]). 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, a strong law-and-order type may 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 if third party records can be 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.[61] 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[62], even good faith uses of murder or terrorism exceptions can expand to cover ordinary law enforcement. Law and policy debates recognize a danger when the government's desire to detect one type of crime, like drug distribution, is parasitic or even motivates the government's collection of information under the guise of some other, more serious crime (like terrorism or air hijacking).[63] On the other hand, if a new Fourth Amendment rule drastically reduces government collection in order to avoid this reverse motive problem, it will fail to capture benefits from new privacy innovations that limit reuse and misuse after collection.

This Article will not offer a clear and complete path out of the bog. Instead, it will identify some values, other than general law enforcement, that should be taken into account by third party doctrine reform efforts. The next Part considers the value of "crime-out" investigations, which can be profitably

based on the intrusiveness of the search (e.g. car versus house versus body cavity) or the aggressiveness of the stop (polite detention versus frisk versus use of force).

[59] 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. (U.S. v. Jones) But in practice, courts tacitly use a sliding scale, requiring less evidence to support probable cause when the police investigate serious crimes. (Craig Lerner article.) And the Fourth Amendment constraints may be loosened considerably for the investigation of terrorism (even domestic terrorism). (The Keith Case.)

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

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

[62] Such use restrictions are not unheard of. Randolph v. Georgia, 547 U.S. 103 (2006).

[63] Get DEA articles from NSA scandal; airport security stats

separated from other types of investigations because of their inherent limitations on police discretion.

III. THE FOURTH AMENDMENT V. CRIME-OUT INVESTIGATIONS

When scholars and judges describe the perils of the third party doctrine, they focus attention on the unrestricted access to *anyone*'s data (thine and mine) without the faintest connection to a suspected crime. The prospect that a policeman can choose to gather the records relating to a chosen suspect without any minimum amount of legitimate individualized suspicion reverberates precisely the sort of unchecked police discretion that justice abhors.[64] I 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.[65]

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.[66] 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 preferences 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 harassment suspect. 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.[67] 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.

---

[64] Debra Livingston, *Police Discretion and the Quality of Life in Public Places: Courts, Communities, and the New Policing*

[65] Orin Kerr, *Why Courts Should Not Quantify Probable Cause*

[66] This 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 __ at *3.

[67] 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 resulting in a severe assault occurred at the southeast entrance to Central Park around 9:00 p.m. on May 1st, 2013.[68] 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 usual detective work.

Most existing proposals for third party doctrine reform would not allow this type of request. This practice could not stand up to a fully loaded warrant requirement 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.[69] Even *if* courts accepted a purely quantitative calculation of reasonable suspicion, the perpetrators are likely to make up only a small 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 or their own toll tag hypotheticals unless the suspect is the only person, or one of only a handful, who might be identified by the records search (and could thereby meet the reasonable suspicion standard required for medium sensitivity records.)

Narrow 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.[70] In other words, crime-out investigating imposes natural constraints on police discretion.[71]

---

[68] My example is, coincidentally, very similar to an example carried out in the ABA's report.

[69] Slobogin, *supra* note __ at 28, 30.

[70] Even if a corrupt police officer were willing to make up a crime out of whole cloth, they would not be able to learn any information about a vindictively-chosen target. Unless the

To fix this problem in Slobogin's, the ABA's, and other proposals for third party reform, a police department or magistrate judge should be able to issue a specialized subpoena that authorizes the NYPD to collect cell phone records on a designated number of people in order to further their investigation of an already-committed crime. If a supervisor within the NYPD or a magistrate issued a "50 record subpoena," the police would need to structure their query to Verizon, AT&T, and the other cell phone carriers in three steps. First, the NYPD would home in on a time and geography most likely to capture people who may have seen or committed the crime. Second, the NYPD would do a "cell size" request to each cellphone service provider to see how many of their customers' location data put them within the requested temporal and geographic window. Third, if the total number of customers sits below the threshold set by the supervisor or magistrate, the NYPD would issue a subpoena for the identifying records. (If the total number exceeds the magistrate's threshold, they must start over again with a more limited geographic or temporal range, if possible.)

Although this sweeps wider than any requirement based on individualized suspicion could, the tradeoff seems sound where the interests of an actual, realized victim are at stake. This system is especially promising for crimes that cause direct harms (like theft and violence) rather than internal or indirect harms (like drug use and gambling), which tend to go unreported for obvious reasons.

A similar, but more permissive, subpoena process should be available to the government when it has identified a suspect for a particular crime for reasons I discuss next.

IV. 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.[72] Also, *Brady* requires

officer already knew the records details of the target well enough to know that the target will be included in the query responses.

[71] 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 (2012).

[72] Brady v. Maryland, 373 U.S. 83 (1963); Giglio v. United States, 405 U.S. 150 (1972).

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 a particular suspect 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 an ATM surveillance camer could conflict with the government's theory about what had occurred[73], 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 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.[74] 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.[75]) 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,"[76] despite the obvious benefits that third party data could potentially show the innocence of a suspect before the government even makes an arrest.

Fairfield's and Luna's unwillingness to bring the interests of exoneration into the predicate question of government information-collection is understandable (scholars writing about DNA databases use the exact same splitting move[77]) but unsatisfying. Even if the small chance of exonerating the

---

[73] Nick Pinto, *Jury Finds Occupy Wall Street Protester Innocent After Video Contradicts Police Testimony,* VILLAGE VOICE (March 1, 2013).

[74] Joshua A. T. Fairfield & Erik Luna, *Digital Innocence,* __ CORNELL L. REV. __ (forthcoming, 2014).

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

[76] *Id.* at __.

[77] Erin Murphy, *License, Registration, Cheek Swab: DNA Testing and the Divided Court,* 127 HARV. L. REV. __ (criticizing collection); Jason Kreag, *Letting Innocence Suffer: The Need for Defense Access*

innocent cannot justify third party data collection on a vast scale, surely it is relevant at moments when data collection is most likely to help out the wrongly accused—a group that constitutes a healthy proportion of arrestees and as much as 1% of convicts.[78]

The crime-out subpoena process described in the last Part should be relaxed to allow even more access to records when they are used defensively (that is, on behalf of a specific, named 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 subpoena similar to the one described above but with a larger permissive cell size count (perhaps no cell size limit at all) to find witnesses or other suspects at the scene of the crime who can corroborate or refute their working theory of the case. Ideally, the government should have an affirmative obligation to access these sorts of potentially exonerating third party records, but in the absence of affirmative obligation the Fourth Amendment should at least refrain from 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 crime detection. 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 listening.[79] Similarly and, perhaps, more effectively, 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.[80] The equipment did not need to collect evidence of police abuse of force because the surveillance stopped abuse from occurring in the first place.

The opportunity to deter crime without activating the full machinery of arrest, prosecution, and incarceration is well worth consideration and study. Bill Stuntz famously and controversially 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 research), is a vastly

to the Law Enforcement DNA Database, 36 CARDOZO L. REV. __ (describing the value for criminal defendants).

[78] Fairfield & Luna at *15; Marvin Zalman, *Quantitatively Estimating the Incidence of Wrongful Convictions,* 48 CRIM. L. BULL. 221, 230 (2012).

[79] Zachary Goldfarb, *Insider Trading Case Ensnares Six: Prosecutors Accuse Hedge Fund Manager, Otehrs of Raking in $20 Million,* WASH. POST (October 17, 2009).

[80] Rory Carroll, *California Police Use of Body Cameras Cuts Violence and Complaints,* THE GUARDIAN (November 4, 2013).

more effective deterrent against crime and police misconduct.[81] 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.[82]

It is a bit troubling that, after third party doctrine reform, a policeman might be able to yell 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. But putting aside the internal inconsistencies of the entire body of Fourth Amendment law, the benefits of data-collection as a deterrent to crime or aggressive police interactions is an interesting idea. Of course, the danger is that access may chill many good and socially productive behaviors, not just criminal ones.[83] 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.

Next we will explore how law enforcement use of third party records can promote the fair distribution of the costs of criminal investigation.

V. 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."[84] Although the Supreme Court largely disagrees[85], distributional justice is an important social goal within and outside the Fourth Amendment.

Tal Zarsky has argued that pattern-based data mining—one of the least understood and most feared innovations in modern policing—has the potential to radically reduce law enforcement inequities if (*if*) it is done right.[86] Christopher Slobogin has also endorsed the use of data mining to detect signs

---

[81] 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).
[82] ABA Report, *supra* note __ at 4.
[83] Marthews & Tucker, *supra* note __ at __.
[84] 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); 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, 4 (2012).
[85] Whren v. United States, 517 U.S. 806 (1996); Robinson v. California, 370 U.S. 660 (1962).
[86] Tal Z. Zarsky, *Governmental Data Mining and Its Alternatives,* 116 PENN. ST. L. REV. 285, 289-290, 311-12 (2011).

of criminal behavior under certain conditions.[87] But this convergence among criminal procedure scholars may seem troubling in the wake of the NSA revelations and growing fears of technocratic and non-transparent government. This Part explains the guarded optimism. Pattern-driven data mining techniques using third party records have the potential to promote law enforcement parity across race and class lines.[88]

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 an impossible task because virtually no one is. Like any rare crime (e.g. mass shootings), using a lot of external data may slightly improve on common sense instincts about which types of people are at relatively greater risk of committing a terrorist act, but even the best algorithms will be lousy. If the government is hell-bent on avoiding Type II errors (letting a terrorist slip through), the algorithm will necessarily make a lot of false alerts.[89] Add to all this the fact that the American government at all levels weighted religiosity and national origin heavily and the result is an understandable deep distrust of algorithmic policing within the legal academy.[90]

But most crimes are not as rare as terrorism. And some of those crimes leave patterns—watermarks in third party records that can show that a crime has occurred and identify the person responsible. 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. Pattern-driven data mining of third party records can lead to fairer enforcement of our criminal laws through two mechanisms. First, looking at the enforcement of any one particular crime, data mining can lead to more equitable enforcement by decreasing our reliance on the observations of police officers, and thereby reducing the opportunities for human bias to infect decision-making. Second, 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 middle- and upper-class criminals.

A. Same Crime, Better Suspicion

---

87 Slobogin, *supra* note __.

88 I will not limit the discussion to those *Carolene Products* discrete and insular minority classifications (race, gender, national origin) that receive constitutional scrutiny.

89 Sara Kehaulani Goo, *Cat Stevens Held After D.C. Flight Diverted,* WASH. POST (September 22, 2004).

90 BERNARD HARCOURT, AGAINST PREDICTION: PROFILING, POLICING, AND PUNISHING IN AN ACTUARIAL AGE; Solove, *supra* note __. I am in agreement with Daniel Solove that critics of government transparency and scholars urging deference to the executive branch were in a short-sighted crisis-driven panic, especially since lightning continues to be a bigger killer than terrorism. *Id.* at 351.

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 rather than their own hunches and suspicions[91]. However, police cannot limit themselves to investigating crime-out cases. There are too many crimes with diffuse, disempowered, or unaware victims. The range includes 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, Terry,* and *Gates*. 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.[92] The emphasis on an officer's testimony about what he or she observed is prone to misjudgment or even outright deceit ("testilying."[93]) And judges allow officers to use squishy, subjective factors like "furtive movements,"[94] "suspicious bulges,"[95] the officer's "training and experience,"[96] "surveillance-conscious behavior," and "high crime areas" to build up their stories of suspicion despite ample evidence that these factors perform poorly in practice.[97]

None of these use third party records. The conventional style of investigations is built on "small data"[98], relying almost exclusively on the

---

[91] Although some of those evidence-based leads, such as eyewitness testimony, has a long track record of inaccuracy and bias.

[92] The problem with the narratives approach to probable cause and reasonable suspicion has been roundly criticized. Craig Lerner, *Reasonable Suspicion and Mere Hunches*, 59 VAND. L. REV. 407 (2006); 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).

[93] 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).

[94] People v. Woods, 64 N.Y.2d 736,737 (N.Y. 1984).

[95] People v. De Bour, 40 NY2d 210, 221 (1976); People v. Hudson, 527 N.Y.S.2d 919 (1988).

[96] 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.

[97] "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, at 54.

[98] Ferguson, *supra* note __ at __.

observations of individual police officers and the idiosyncratic, unaccountable, unknowable personal algorithms that they keep in their minds.[99]

Traditional police investigations distribute their suspicion and intrusions in terribly regressive ways. It's no secret that discretion- and observation-driven policing lead to more searches of the poor.[100] This is at least partially a result of where police spend their time. Police are deployed in greater numbers to poor and minority neighborhoods, where their help is most needed and most wanted.[101] But the accumulation of recent Fourth Amendment rules has exacerbated the unequal attention paid to the poor. The upper classes can afford copious curtilage[102], hang out in "low crime areas," and prefer to wear form-fitting bulgeless clothing.[103] 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 blatant evidence: minorities serve a disproportionate share of the prison time for minor drug convictions despite having drug usage rates similar to whites.[104]

The legal scholars who most forcefully decry precedents like *Terry v. Ohio* and who most publicly accuse law enforcement of discriminatory tactics have not carried the burden of laying out practical alternatives to the current system. 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[105], but most have not seriously considered the injustice in a police investigation system that profiles *without* data.

---

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

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

[101] 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).

[102] 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).

[103] 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).

[104] 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).

[105] HARCOURT, *supra* note __.

Today, police departments can use data to investigate crimes that were once investigated using the usual accretion of faulty evidence. They use social media comments to learn about gang activity and membership[106], and they mine their own crime data to predict in advance precisely where burglaries and other crimes are likely to happen, and when.[107] 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 be insufficient to rise to the level of *Terry* reasonable suspicion, it could nevertheless suffice when combined with the data-driven designations of criminal hot spots. Elizabeth Joh and Andrew Ferguson have anticipated that police are using data to more objectively and reliably defining what a "high crime area" means.[108]

So far these examples involve public information and the police department's own crime data, but there's nothing inevitable about this limitation. Third party records can be used, too. Ferguson has spun out an example where the purchases of large numbers of mini-Ziploc bags could contribute to suspicion,[109] and one could imagine how ATM data, store security camera videos, and other transaction records could be used to predict crime. But let me propose one more counterintuitive reason we may prefer for police to have access to third party records: if they can't, the government can always mandate disclosure.

Consider Sudafed. Its active ingredient, pseudophedrine, is the base for most homemade methamphetamines as every Breaking Bad fan would know. In an alternate world, we could be debating the ethics and Fourth Amendment legality of government access to drug store purchase records in search of suspiciously large quantities of pseudophedrine. Instead, Congress passed the Combat Methamphetamine Epidemic Act of 2005, which prohibited purchases of pseudophedrine in large quantities or by minors and compelled the collection and disclosure of identifying information for the purchases of small quantities.[110] This is hardly the better outcome on the basis of privacy, efficiency, or autonomy.

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

---

[106] Ferguson, *supra* note __ at 2; Somini Sengupta, *Privacy Fears Grow as Cities Increase Surveillance,* N.Y. TIMES (October 13, 2013).

[107] 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).

[108] Elizabeth Joh, *Policing by Numbers: Big Data and the Fourth Amendment,* 89 U. WASH. L. REV. 35, 46, 56 (2014); Ferguson, *supra* note __ at *4, *44.

[109] Ferguson, *supra* note __ at __.

[110] Combat Methamphetamine Epidemic Act of 2005, H.R. 3199.

through gambling websites, and insider trading leave very few clues in the physical world.[111] As Rachel Barkow says, "Law enforcement cannot literally walk a beat [] in the business crime context."[112]

Privacy instincts that seem perfectly sensible as a policy matter can have bad unintended consequences. 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*[113], the Supreme Court ruled that a subpoena requiring the disclosure of our own documents (the case involved some importation records) violated both the Fourth and Fifth Amendments. *Boyd* is an old case, and most of its holding has been seriously compromised by later case law, especially *Fisher v. United States*.[114] The rule from *Boyd* was destined to fail because its effects on law enforcement were 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.

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.[115] Those records led the investigators to Roomy Khan, an Intel employee who fielded an unusual number of calls from the Galleon Group.[116] 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.[117] 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.[118] 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.)[119] And the calling behavior of prepaid "burner" cell

---

111 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).

112 Barkow, *supra* note __ at 464.

113 116 U.S. 616 (1886).

114 425 U.S. 391 (1976).

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

116 *Id.*; William Alden, *Roomy Khan, Figure in Galleon Insider Case, Setnenced to One Year in Prison,* N.Y. TIMES (January 31, 2013).

117 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).

118 Barkow, *supra* note __ at 451.

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

phones can give away whether they are used for legitimate or illegitimate purposes.[120]

The FBI is devoting a larger portion of its resources than ever before to the detection of white-collar crime.[121] This shift is admirable, especially since it runs against some natural instincts among law enforcers to go back to the more comfortable work of nailing traditional bad guys. Many scholars and journalists have criticized the government for its lax enforcement and soft penalties in the white collar space[122], and for good reason. 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.[123]

C. Proposals

If the third party doctrine is dismantled, courts should not reject pattern-driven policing outright. Data mining has some redistributive and privacy-enhancing qualities. 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 thus much more accountable and fixable than the ad hoc system courts rely on today.[124]

Christopher Slobogin argues that we should allow statute-authorized data mining programs as long as the most affected groups have "meaningful access

---

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

[121] Barkow, *supra* note __.

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

[123] Barkow, *supra* note __ at 469.

[124] 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. *See* Bambauer, *supra* note __ at __.

to the legislative process" and the statute is applied even-handedly.[125] This would be an ideal way to proceed, but a legislative action requirement is too restricting. After all, Slobogin's proposal operates against a backdrop of 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 to me why police departments should *refrain* from developing pattern-based data mining programs of the sort described above. While they may lack political buy-in, this hardly distinguishes them from other police practices. Moreover, political process might have precisely the sort of majoritarian domination we would want to avoid. 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.[126]

Instead, a third party doctrine overhaul should develop a special subpoena or warrant process for temporary collection of third party records for the sake of validating, and eventually applying, suspicion algorithms. The details should be developed by expert criminologists, so I will not attempt to build out specifics. But the subpoena process should have three key features.

First, the subpoena 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%.[127] But the threshold should 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. And 50% might not be low enough if the crime is very common.[128]) To achieve the accuracy requirements, government must keep records on the results of stops, searches, and arrests.

Second, the subpoena 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 used to predict suspicious activity[129], but the audit logs should be

---

[125] Slobogin, *supra* note __ at 16, 30-31.

[126] Bill Stuntz commented long ago that political process 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 __ at 1045.

[127] Slobogin, *supra* note __ at __.

[128] Even a good algorithm will force too many innocent people to undergo searches or arrests if the algorithm detects a high occurrence crime, like possession of marijuana. I argue that the Fourth Amendment can and should watch out for this problem. Bambauer, *supra* note __.

[129] 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

comprehensive enough to ensure that the algorithm performed well and that the government did not abuse discretion in deciding which positive alert to pursue.[130]

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.[131] Law enforcement would then make a follow-up request for identifiers of all positive alerts.

These features will go a long way to address the concerns and anxieties of critics. The last countervailing interest to consider is 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.

VI. 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.[132] 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, we 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, even in one's public movements[133], to withstand scrutiny), the plaintiffs' First Amendment challenge is probably well-founded. [134]

However, the case has an interesting wrinkle—one that was unnecessary for the plaintiffs to wade into, but wade they did. DRN made clear that one of its objectives was to disclose the license plate information to law enforcement

---

regressions. Tal Zarsky does not think those benefits are worth the risks. *See* Zarsky, *supra* note __.

130 The ABA recommends data use logging within their framework, too. ABA Report, *supra* note __ at 25.

131 The data need not be "anonymized" or "deidentified" as that term of art is used in debates about reidentification risk. 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.

132 DRN v. Herbert, Case 2:14-cv-00099-CW, available at http://www.scribd.com/doc/207191306/DRN-v-Herbert-Brief.

133 Nader v. General Motors Corp., 25 N.Y. 2d 560 (1970).

134 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. __ (2014).

"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 this type of speech interest would play well with their judge, but it unwittingly walked 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, schools, and telecommunications providers[135] from disclosing the personal information of their clients to *anybody* (let alone the government), and these sorts of narrowly-tailored statutes are presumptively constitutional. The reason is that 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.

However, in situations involving something less than a fiduciary relationship, 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 to be cooperating with them already. If our trust is misplaced, and our friends perform 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

[135] 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 treat telecommunications providers as if they have a fiduciary relationship with their customers. This seems right to me. The restrictions of metadata, however, raise harder questions.

criminal detection that courts tend to separate from the definition of "search."[136]

Third, as a practical matter, incentives of businesses are usually closely aligned to their clients.[137] With the exception of companies like DRN that operate in areas where the 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.[138] 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 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 difficult for courts to monitor the state action line. State action problems come into play if a company's disclosure of customer records is not truly voluntary. What looks like voluntary disclosure may be the result of behind-the-scenes pressure from government agencies.[139] This tactic would presumably increase if the third party doctrine were altered so that the state could not access records through ordinary subpoena power. 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.[140] 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.[141]

Putting difficult state action line-drawing 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.

---

136 Illinois v. Caballes, 543 U.S. 405 (2005).

137 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).

138 Kim Zetter, *Google Challenges FISA Gag Orders on Free Speech Grounds,* WIRED (June 18, 2013).

139 Derek Bambauer, *Jawboning,* (forthcoming); Balkin, *supra* note __.

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

141 U.S. Sec. & Exch. Comm'n, Annual Report on the Dodd- Frank Wistleblower Program: Fiscal Year 2012; Rachel E. Barkow, *The New Policing of Business Crime*, 37 SEATTLE U. L. REV. 435, 439 (2014).

CONCLUSIONS

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

For crime-out investigations, police should be able to use a limited-record subpoena to access third-party records. The subpoena process should be more generous when the police have probable cause to make an arrest and are diligently searching for records that may corroborate or (more importantly) refute their theory about who committed the crime.

For pattern-driven data mining programs, courts should permit law enforcement agencies to analyze de-identified records and access an identification key first on a short-term experimental basis and then, when the program is validated, on a larger scale.

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

* * *