

# THE CASE AGAINST THE CASE FOR THIRD-PARTY DOCTRINE: A RESPONSE TO EPSTEIN AND KERR

By Erin Murphy<sup>†</sup>

## TABLE OF CONTENTS

I. NEUTRALITY, CLARITY, AND EQUALITY: A RESPONSE TO KERR .....	1241
A. TECHNOLOGICAL NEUTRALITY .....	1241
B. EX ANTE CLARITY .....	1245
C. ALTERNATIVE JUSTIFICATIONS FOR ELIMINATING THIRD-PARTY PROTECTIONS .....	1247
II. PRIVATE LAW AND THIRD-PARTY DOCTRINE: A RESPONSE TO EPSTEIN .....	1248
III. TOWARD A THEORY OF THIRD-PARTY PROTECTION .....	1250

Professor Epstein, Professor Kerr, and I may at times approach legal questions from different perspectives, but there is one thing that we all agree upon: the current configuration of third-party doctrine under the Fourth Amendment is problematic. However, lest you worry that this unanimity makes for uninteresting commentary, fear not: that might be all that we agree upon.

In his wonderful and thought provoking article, *The Case for Third Party Doctrine*, and in his comments today, Professor Kerr asserts that the chief defect of the third-party doctrine is one of form, not substance.<sup>1</sup> He finds the rule itself—that information disclosed to third parties receives no Fourth Amendment protection—to be basically a good one. Professor Kerr defends the third-party doctrine in principle, and argues two additional points: first that we should justify it differently (as founded in consent rather than in rea-

---

© 2009 Erin Murphy.

<sup>†</sup> Assistant Professor of Law, University of California, Berkeley, School of Law. My thanks to Professor Paul Schwartz and the Berkeley Center for Law and Technology for inviting me to participate in the 2009 Privacy Lecture, and to Professors Epstein and Kerr for providing such wonderful ideas for discussion.

1. Orin S. Kerr, *The Case for Third Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009).

sonable expectations of privacy), and second that we should worry less about it (because other legal regimes exist to protect us).

In contrast, in *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*,<sup>2</sup> Professor Epstein is a bit more skeptical and thus a bit more cautious. A rose by any other name, he observes, smells just as sweet. “Consent” is just another way of saying assumption of risk, which falters in the context of unilaterally imposed, government-generated criminal enforcement. In search of a meaningful restraint on state power, then, eventually we will end up right back where we began: the reasonable expectation of privacy. An imperfect doctrine, Professor Epstein concedes, but one that if by nothing other than by the sheer dint of its popularity must achieve something.<sup>3</sup>

Now, Professor Epstein candidly acknowledges coming at the third-party problem as, if you will, a third party. Specifically, he writes as someone “outside of the field of criminal procedure, but with a strong commitment in favor of the principles of limited government.”<sup>4</sup> This perspective probably explains why he describes his goal as to “parse the arguments in order to develop a unified approach . . . that can win adherents both within the field and beyond it,”<sup>5</sup> rather than come down wholly on one side or another. Such wild ideas are clearly those of an outsider, someone unfamiliar with the norms of the discipline. In criminal justice, you are either with us or against us. You are either working to free all the criminals or you are an apologist for the fascist police state! This is not a field known for its conciliatory, nuanced “unified approaches.”

Having thus stepped into a play that clearly casts Professor Kerr as the defender of the police state and Professor Epstein as the voice of virtuous moderation, I suppose it only remains for me to dutifully assume the role of the advocate for freeing all the criminals. Which, alas, means that Professor Kerr’s lucid and important defense of the much-maligned third-party doctrine, having just been knocked around by the middle, is now to be fully assaulted from the left.

I will start by posing the two major questions at stake: should there be any third-party protection at all, and if so, what should it look like? Since Professor Epstein focused most of his attention on the latter point, I will

---

2. Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 BERKELEY TECH. L.J. 1199 (2009).

3. *Id.* at 1208.

4. *Id.* at 1200.

5. *Id.* at 1200-01.

spend my time more on the former.<sup>6</sup> To answer that general question, I intend to proceed in the following four steps. First, having agreed with Professor Epstein's critiques of Professor Kerr's technological neutrality and ex ante clarity rationales for scrapping third party protection, I will add two critiques of my own. Second, in the spirit of reconciliation, I will provide an alternative defense for denying third-party protection; but then, in a revived spirit of partisanship, I will turn to attack my own rationale. Third, with lingering pique, I will critique Professor Epstein's alternative approach. Fourth and lastly, I will present in the hopeful and ingenuous manner of an assistant professor some thoughts on how to conceive of a viable third-party protection doctrine.

## I. NEUTRALITY, CLARITY, AND EQUALITY: A RESPONSE TO KERR

### A. TECHNOLOGICAL NEUTRALITY

Like Professor Epstein, I find Professor Kerr's insight about technological neutrality and substitution effects quite compelling—namely, that the third-party doctrine ensures that savvy criminals cannot strategically exploit sophisticated technological methods to evade detection. But, like Professor Epstein, I find that this insight is open to the critique that it also cuts the other way. Specifically, because the technologies left exposed by third-party doctrine are not exclusively deployed for illicit purposes, failing to protect them generates negative externalities (by dissuading innocent, desirable conduct); thus the possibility of “substitution effects” alone cannot justify the existence of the doctrine.<sup>7</sup>

To this observation I would also add a more fundamental critique, however. Specifically, I am not convinced that such “substitution effects” really take place, at least not on the scale and to the degree that would justify forfeiting all third-party protection. In essence, Professor Kerr claims that extending third-party protections would simply inspire “a rational actor bent on

---

6. I will note quickly at the outset, though, that I agree that the “assumption of risk” or autonomy framework is the wrong way to go about thinking about whether disclosures to third-parties deserve protection. I also share Professor Epstein's sense that Professor Kerr's “consent” model seems to just circle back to the reasonable expectation of privacy test. Epstein, *supra* note 2, at 1206. Similarly, I concur with Professor Epstein's observation that a notice principle too readily leads to the evisceration of substantive rights, particularly when the coercive power of the government is at issue. *See infra* Part II. Thus, I join in Professor Epstein's search for alternatives geared toward optimizing social utility (even though I typically tend not to phrase my objectives in such economic terms).

7. Epstein, *supra* note 2, at 1226 (discussing “social inefficiencies with respect to lawful conduct that people naturally wish to keep from the prying eye of the state”).

criminal conduct [to] use as many third-party services as he can to avoid detection.”<sup>8</sup> It is perhaps not surprising that this claim did not capture the attention of Professor Epstein, but it did capture mine—for two reasons.

First, I am not a big believer in the “rational criminal actor.” What we know about the criminal actor is that he is usually poor, uneducated, and high on drugs or alcohol a surprising amount of the time.<sup>9</sup> Thus, in the majority of cases, the criminal actor will not be thinking much of third-party outsourcing as a means of evading detection. Of course, we might speculate that the third-party doctrine arises most frequently in cases in which defendants are better educated and resourced—“white collar” crimes, for instance—and thus more likely to act “rationally.” But I would argue that the sheer degree to which third-party interactions permeate contemporary life, across all socio-economic boundaries, calls that assumption into question. The doctrine is as much about the secrets told a cellmate as those shared with an investment banker, or the DNA left on a soda can as that given to the doctor during an exam. Recall, after all, that of the two foundational opinions setting out the third-party doctrine, one—*Smith*—was essentially a glorified stalking case.<sup>10</sup> Even mob or racketeering cases, for which third-party doctrine currently eases the path of investigation, inevitably ensnare the impulsive little fish along with the more calculating big ones. In this day and age, *cives technologicus sumus*.<sup>11</sup>

Even assuming the rationally acting criminal, I am still not convinced that Professor Kerr’s substitution effect is real. Take the example he gives of Smith the telephone stalker.<sup>12</sup> In the pre-technology world, says Professor Kerr, Smith has to leave the house, drive around, and ring doorbells in order to stalk his victim: all conduct that requires him to be out and about where he can be publicly observed and therefore apprehended.<sup>13</sup> In the technologi-

---

8. Kerr, *supra* note 1, at 580.

9. *See generally* BUREAU OF JUSTICE STATISTICS, U.S. DEPARTMENT OF JUSTICE, CRIMINAL OFFENDER STATISTICS (2007), <http://www.ojp.usdoj.gov/bjs/crimoff.htm#inmates> (describing summary findings from various government reports on the characteristics of state jail and prison inmates, including that roughly 50% were under the influence of drugs or alcohol at the time of the offense, 75% were using drugs or alcohol during that period, roughly 43% had no high school degree or equivalent, and over half have mental health problems). The numbers for federal inmates are only marginally lower. *Id.*

10. *Smith v. Maryland*, 442 U.S. 735, 737 (1979) (describing how Smith was identified as a robber after repeatedly driving through the victim’s neighborhood and making threatening and obscene phone calls).

11. That is, playing on the famous Roman incantation of “*civis romanus sum*,” we are all citizens of technology—bestowed with both the privileges and burdens of our subjugation.

12. Kerr, *supra* note 1, at 580.

13. *Id.* at 578-79.

cal world, though, Professor Kerr proposes that Smith can stalk his victim by phone or Internet with the curtain drawn at home, thereby eluding easy detection if the law interposes an impediment in the form of third-party protection.<sup>14</sup> Thus, he concludes, what stalker would not go with the technological route? You don't even have to change out of your pajamas! But get rid of those protections, argues Professor Kerr, and Smith the phone-stalker is as amenable to detection as Smith the window-peeper.<sup>15</sup>

But is that the right way to frame the issue? A lot of crime does not come with an obvious technological alternative, or to the extent that outsourcing is possible, it fundamentally alters the nature of the offense. One generally cannot murder, rape, or cause serious bodily injury via technology alone. Even if the proper measurement is not the seriousness of the offense but its rate of occurrence, technological outsourcing still raises no real concern. Technology does not offer much by way of protection from accusations of disorderly conduct, or drinking and driving, or even drug distribution—the kinds of crime that, for better or for worse, make up the vast majority of criminal offenses in our country.<sup>16</sup> To the extent that there might be some subset of crimes—say, child pornography or internet fraud—that are disproportionately amenable to third-party technological outsourcing, then it is still worth asking how much of what is involved is a true *substitution* effect as opposed to simply a sub-species of crimes in which third-party participation is an indispensable component (or even instrument) of the offense. Erecting third-party protections would make investigating such crimes more difficult, to be sure, but less because the offender substitutes the Internet for stepping out to the mailbox to get his illicit images than because there are so many more images, and offenders, to police. If that is the case, then third-party doctrine is not so much creating technological neutrality as it is forging a technological exception.

So if it's not universally the case that technology makes possible or incentivizes substitution effects, then is there anything about the nature of how technology is deployed in crime, either its capacity to be private rather than

---

14. *Id.*

15. *Id.* at 578.

16. In 2007, for example, there were over 14 million arrests reported by law enforcement agencies participating in the Uniform Crime Reporting System. A significant number of those were for crimes that seem resistant to substitution, such as drugs (1.8 million), property crimes like burglary, theft, and arson (1.6 million), DUI (1.4 million), assault (1.3 million), disorderly conduct (709,105), liquor violations (633,654), and drunkenness (589,402). CRIMINAL JUSTICE INFORMATION SERVICES DIVISION, FEDERAL BUREAU OF INVESTIGATION, U.S. DEPARTMENT OF JUSTICE, *Table 29: Estimated Number of Arrests, in CRIME IN THE UNITED STATES, 2007* (2008) [http://www.fbi.gov/ucr/cius2007/data/table\\_29.html](http://www.fbi.gov/ucr/cius2007/data/table_29.html).

public or the nature of the offenses that are committed via technology, that requires “equalizing”? Do we have to let the police access Google search records without fear of the Fourth Amendment either because they cannot come to your living room to watch your websurfing, or because the kinds of crimes committed online are particularly heinous? In essence, this is just another way of asking whether private crime, and in particular really heinous private crime, should be rendered as readily policeable as public crime. To this, the Constitution has already given us an answer: no. For better or for worse, we have a trans-substantive Fourth Amendment. We do not obliterate privacy protections for the home, for instance, just because the vast majority of child sexual abuse occurs there. Besides, constitutional criminal procedure has crafted other means of dealing with the problems posed by complex or difficult to investigate crimes—namely, the grand jury, which is virtually immune from Fourth Amendment strictures.<sup>17</sup>

Moreover, even to the extent that there are categories of offenses like theft, fraud, or white collar crimes that are more readily outsourced via technology, it still is not clear that third-party participation makes policing all that harder or easier. In fact, it seems probable that the more that third-parties are involved or technology is deployed, even with a robust conception of third-party protections, the more likely it becomes that the criminal will be apprehended. This is for the simple reason that enlisting third-party assistance in crime tends to generate, rather than obfuscate, opportunities to get caught. Third parties increase the possibility that a trail will be left or witnesses will be created, all of which only helps the state in building its case.

Think again about Smith. Suppose Smith took Professor Kerr’s technological route, and instead wrote emails or made phone calls. It is true that in a world of third-party protections, the police would likely need something like a warrant and probable cause to get their hands on them. But that is not a particularly high a standard to meet. Even in *Smith* itself, the police had the description of the robber and the make and model of a car at the scene, which matched the car (by license plate) that drove slowly by the victim’s house at the time she received threatening and obscene phone calls from the robber.<sup>18</sup> That alone likely constitutes probable cause for a warrant. And once Smith was arrested, wouldn’t it be easier to make out the stalking case with the emails and phone calls than, for instance, with just the testimony of the victim that some guy keeps coming around?

In truth, Smith’s best bet for evading detection for his stalking was probably not the highly public act of skulking around, nor the intensely private,

---

17. *United States v. Dionisio*, 410 U.S. 1, 11-12 (1973).

18. *Smith v. Maryland*, 442 U.S. 735, 737 (1979).

technologically-substitutive act of calling or emailing, but rather an intermediate public/private, high-tech/lo-tech hybrid of typing and mailing old-fashioned letters (so long as he did not lick the envelope). Thus, if anything, the hypothetical demonstrates that the most likely “substitution effect” of technology may be the slight creation of a front end problem (getting your hands on evidence) in favor of a nice solution to a back end problem (that evidence being persuasive). If that is the case, then it is even less clear which way substitution actually cuts, and this need for “technology neutrality” to level the playing field does not really exist.

#### B. EX ANTE CLARITY

So then what about Professor Kerr’s argument for third-party doctrine on the grounds of ex ante clarity? Like Professor Epstein, I find this point unpersuasive as a normative justification for the lack of protection. After all, if the primary aim is clarity, then I would instead vote in favor of a very clear rule (and one with ample constitutional support) that simply prohibits all third-party investigation without a warrant or probable cause—the “libertarian baseline,” if you will.

But even assuming that the ex ante clarity rationale points toward eliminating rather than bolstering third-party protection, then is devising a legal regime really so unworkable and unclear? Professor Kerr argues that the need for clarity is particularly acute with regard to information in the hands of third parties, because sourcing the origins of information ex ante is virtually impossible.<sup>19</sup> This he calls the “information history” problem, and he sums it up nicely with the example of the anonymous blog commenter who posts about a rumored bribe to a Senator.<sup>20</sup> If the government wants to subpoena the commenter, Professor Kerr asks, how will it know whether doing so would violate the Senator’s rights under the Fourth Amendment? Professor Kerr posits five scenarios to tease out the issue, in which the blog commenter is: (1) a bank teller who deposited the bribe for the Senator; (2) a bank customer who overheard the Senator’s deposit; (3) a bank robber who stole the records; (4) the briber; or (5) the Senator herself.<sup>21</sup> Although a reconstituted third-party doctrine might protect some of these, the government would not know ex ante, at the time of its subpoena, which was the operable scenario.

I have to admit this one stumped me for a while. But then I realized that, as framed, it is not quite right. The scenario actually implies two levels of possible third-party problems. The first regards the request to the blogger’s

---

19. Kerr, *supra* note 1, at 582.

20. *Id.* at 584.

21. *Id.*

ISP for the name of the commenter. But that should not be a problem, third-party protection or no third-party protection, because the Fourth Amendment does not apply to grand jury subpoenas to appear and testify, and the only limit on subpoena *duces tecum* is that it not be “unreasonable.” So, done.

But what if there is no grand jury investigation? What if it is just the police officer, kicking around on the Internet, trying to come up with a to-do list for tomorrow? Well, in that case, I say so be it. If an anonymous tip about a person with a gun is not enough to shake someone down on the street,<sup>22</sup> then I am comfortable saying that an anonymous tip of a Senator with a bribe should not be enough to shake someone down on the Internet. Sure, we want to catch gun-toting bus stop patrons and Senators with fat pockets, but not at the expense of trading individual liberty for blind faith in the statements of any Tom, Dick, or Jane with a DSL connection. If the Internet has taught us anything, it has taught us not to believe everything we read, especially when it comes from someone unwilling to back up their allegations with their true name.

What about the second level, then? Assume now that the government knows the name of the commenter, but has to determine whether questioning the commenter about the bribe will violate the Senator’s rights. Here, again, this poses no problem in the context of a grand jury investigation. There may be other protections that come into play—for instance, the Senator, the Robber, and the Briber might all have Fifth Amendment privileges, but other than that no Fourth Amendment concerns arise.

What if the context is not the grand jury, but just ordinary investigatory policing? In that case, I disagree with Professor Kerr that the problem posed by third-party doctrine is how the police will figure out from where the information comes. After all, discerning the nature of the source of information is a critical and common part of determining its reliability. It should be expected that officers would ask the commenter, “who are you and how did you learn about this bribe?” right after flashing their badges. In that case, we can easily imagine a functional third-party rule (hinging on the confidence in which the information is transmitted or obtained) that would immediately clue investigators in to proceed no further if the answer is: “I work at the bank,” or “I’m the Senator’s best friend” or “I stole it,” as opposed to “I overheard it on the street” or “I made it up.” Indeed, in all likelihood officers would ascertain that information before knocking on the door. It might even be readily apparent from running a routine background check on the information given to them by the ISP that the person is a lobbyist or a bank employee or a criminal with a history of bank robbery or the Senator herself.

---

22. Florida v. J.L., 529 U.S. 266, 274 (2000).



C. ALTERNATIVE JUSTIFICATIONS FOR ELIMINATING THIRD-PARTY PROTECTIONS

Having joined forces with Professor Epstein in disputing Professor Kerr's twinned virtues of the third-party doctrine—that it affords technological neutrality and that it provides *ex ante* clarity—is it thus a foregone conclusion that the doctrine should go? Let me provide one half-hearted attempt to supply an alternative justification, which might be deemed technological neutrality in another sense of the term.

If it is true that third-party protections largely come into play with regard to white-collar or organized crime or other sophisticated policing efforts, then even if third-party doctrine is not exclusively a rich people's problem, it is at the very least a middle and upper class issue. In that case, eliminating third-party protections may have an equalizing effect—not between private and public criminality or technological and non-technological offenses as Professor Kerr maintains, but between street and sophisticated crime, or poor people and not-so-poor people crime. The true substitution effect, in other words, is not the manner in which the same criminal commits his crime, but rather one kind of criminal defendant (rich) for another (poor). In Professor Bill Stuntz's terms, it is a matter of displacement and incentives: the more procedurally difficult it is for investigators to obtain the things they need to net the big fish, like bank or phone or ISP records, the more they might be inclined to focus on netting the small, corner fish instead.<sup>23</sup>

Accordingly, it might be posited that third-party doctrine as it currently stands levels the *investigatory* playing field. This alone might serve as a legitimate justification for third-party doctrine: not that it enforces technological non-substitution, but that it ensures socio-economic non-substitution. Yet for several reasons, I believe this defense cannot stand. Most notably, as I suggested earlier, I dispute the initial premise that third-party doctrine primarily affects or applies to white-collar cases.<sup>24</sup>

But even assuming that eliminating third-party constitutional protections creates socio-economic equality, the problem remains that, for the most part, resourced people will not tolerate that equality. Resourced people do not like having their bank, e-mail, and video records open for the government to see. So they call Congress. And they get things passed. And suddenly there is the Wiretapping Act and the Electronic Communication Privacy Act and HIP-PAA and the Video Privacy Act and so on. Meanwhile, no one lobbies for

---

23. See generally William J. Stuntz, *The Pathological Politics of Criminal Law*, 100 MICH. L. REV. 505, 574-75 (2001); William J. Stuntz, *The Uneasy Relationship Between Criminal Procedure and Criminal Justice*, 107 YALE L.J. 1, 3-4 (1997).

24. See *supra* text accompanying notes 10-11.

the Thin Walls and Crowded Conditions of Public Housing Privacy Act, or the I Never Should Have Said That To My Cellmate Act, or the I Cannot Afford a Private Car or Gulfstream 5 and So I Am Stuck Handing My Bag and My Liberty Over to Greyhound Act.

So to the extent that I might be able to rally some support for eliminating third party protection on the grounds that it would create congruence in Fourth Amendment coverage (or more accurately put, *lack* of coverage) for the rich as well as the poor, then the existence of all those statutory protections that Professor Kerr later cites as bulwarks against abuse somewhat dims my enthusiasm for that approach. Besides, if leveling the gap between the rich and the poor is to occur, I would much prefer the extension of protection to the poor, rather than the reduction of privileges held by the rich. After all, who finds a sinking-tide-sinks-all-boats theory an attractive axiom for doling out rights?

## II. PRIVATE LAW AND THIRD-PARTY DOCTRINE: A RESPONSE TO EPSTEIN

Having disputed both of Professor Kerr's rationales for eliminating third-party doctrine, and then having supplied (and disputed) an alternative rationale of my own, it remains now to ask from where third-party protections—if they existed—might draw some principled guidance. It is on this question that Professor Epstein focuses most of his attention. Specifically, having rejected the autonomy rationale for eliminating third-party protection, Professor Epstein undertakes a theory grounded in optimal social utility, thereby giving content to the reasonable expectation of privacy by means of social conventions and drawing particularly on private law analogies.

Professor Epstein frames the background inquiry as “are there things that the police can do without regard or resort to their state power, because ordinary citizens can do them too?” If private law prohibits the private actor, so too might it forbid the public actor. If private law allows it, then so too might the Constitution. Of course, Professor Epstein acknowledges a zone of hard cases, but then the question becomes one of nuanced calibrations in which even the hard cases, like those involving fraud committed in the name of public as opposed to private interest, have delicate contours in private law that might or might not transfer to the public law context.

At base, I agree with his general project of attempting to locate some set of overarching principles to guide the formulation of a reconstituted third-party protection. My concern, however, is that lost in this astute and interesting series of analogies is an acknowledgement of that which differentiates private and public law, or private and public power, and which distinguishes

the ordinary citizen from the officer of the state. The question of who is doing something, and why, is as important to me as the question of under what authority it is being done. Private law develops and operates against a backdrop of assumptions that, to my mind, do not hold when applied to the criminal context. Private law actors are presumed to be equal; they are autonomous; they are rational, capable of contracting, and subject to consequences for their actions and choices. What is different about public actors, and why we need special restraints, is that these assumptions no longer necessarily remain true. Indeed, for effective policing to take place, they necessarily remain *not* true. Professor Epstein agrees with all of this in rejecting Professor Kerr's consent and assumption of risk based model, but I fear he too readily relinquishes the profundity of this observation in formulating his own alternatives.

In simpler terms: It is true that I, Erin Murphy, can knock on your door and ask to come in and that the police can knock on your door and ask to come in. We may both have the same authority (namely, none), but you will not experience those knocks in the same way. I do not mean as a subjective matter, which is obviously the case. I mean it objectively as well. For instance, if I shove my way in, you have a means of getting me out (calling the police). If the police shove their way in, you are pretty much at their mercy. If I start asking you a lot of questions about your finances or habits, you will assume I am a nosy person and tell me to bug off. If the police start asking you a lot of questions about your finances or habits, you will assume that telling them to bug off will get you nowhere, and will likely feel pressured to answer. If I get mad that you are not cooperating, and put you in handcuffs and lock you up for twenty-four hours for no reason, I can get convicted, go to jail and be held civilly liable. If the police get mad and put you in handcuffs and lock you up for twenty-four hours for no reason, you have probably just lost twenty-four hours. If I pull a gun on you, or steal your briefcase, I am definitely committing a crime. If the police pull a gun on you, they might just be making a good faith mistake. Even if they steal your briefcase, the most you might get is a stern reproach from the Supreme Court saying "no one should condone" such "possibly criminal behavior."<sup>25</sup> And good luck collecting damages in civil court.

I could go on, but you get the picture. Citizens and the police are not the same. We should never treat them the same. The police can do things that ordinary citizens cannot, for the most part, do: carry guns, lock people up, and conduct searches. The police benefit from default presumptions that ordinary citizens lack: police desires and actions are presumed to be consonant

---

25. *United States v. Payner*, 447 U.S. 727, 733 (1980).

with their public protection mission, whereas the same desires and actions by a private person are presumptively illegal or criminal. The police are protected from consequences in a way that ordinary citizens are not.

For the most part, these distinctions are as they should be. Every civilized society requires a police force to safeguard the rule of law. A police force should be vested with both social and actual authority to execute its mission appropriately. If a stranger busts into someone's house, we assume that person is acting with ill intent; if the police bust into your house, we assume they are there for good reason. We rely on the police to have that special aura of perceived and actual power. But, accordingly, the background assumption of policing should always be that police are different. Of course, a good libertarian will agree with me, as Professor Epstein does in the context of Professor Kerr's assumption of risk and notice discussion: simple notice arguments do not work in the Fourth Amendment context because power trumps notice every time.

For the same reason, I would proffer that the private analogy path is a dangerous one to go down generally, because public power runs on different cylinders than private ordering. That is not to say that police should not be able to do some of the things that an ordinary citizen does. But that should be the beginning of an analysis, not the end. Sure the operator could see the number that Smith dialed. But you know who couldn't? Every other person in the neighborhood. If we really treated the police like any ordinary citizen, then our result in *Smith* would have to be that the average ordinary citizen cannot see the numbers, therefore they were constitutionally protected. There is a difference between thinking of the police as *any* ordinary Joe versus thinking of the police as *every* ordinary Joe. Confusing these two—and adopting the latter position while stating the former, makes the police not Everyman but *every man*. It makes the police omnipotent and omnipresent. Precisely what, I would argue, the drafters of the Fourth Amendment feared and thus forbid.

### III. TOWARD A THEORY OF THIRD-PARTY PROTECTION

Having abused every theory and done my Chicken Little government-power routine, then, do I have anything left to say for myself? Well, to avoid Professor Kerr's apt invocation of the "takes-a-theory-to-beat-a-theory" mantra, let me give it my best shot.

By now, it is probably obvious by implication that I do not view Professor Kerr's proposed four alternative, non-constitutional routes of protection

as anywhere near adequate. To wit: *Massiah*<sup>26</sup> is a frail and ailing patient (rendered all but comatose by *Montejo* and *Cobb*);<sup>27</sup> entrapment is so dead that I do not even bother to teach it; vicarious assertions seem so unlikely that Google—arguably a force more powerful than the government—stood alone against the government’s subpoenas for search records from large ISPs including Yahoo and MSN, and its most formidable argument rested on commercial trade secret doctrine;<sup>28</sup> and the statutory privileges are barely worth the paper they are printed on. (I am guessing most people these days would happily exchange their priest-penitent privileges for ISP-websurfer ones—although some reports suggest that the two at times may overlap.)<sup>29</sup>

So if I want some kind of constitutional third-party protection, and I recognize that it cannot simply be contiguous with the defendant’s Fourth Amendment rights, then how might I imagine the doctrine? Truthfully, I have no idea.

As I see it, the real obstacle to implementing third-party doctrine is that it creates the potential for conflict between a third party from whom information is sought, and the defendant against whom the action ultimately is taken. This conflict occurs both in terms of each party’s desire to assert the protection and its probability of doing so. In a world in which we afford some third-party protection, when the knock on a third party’s door arrives, how will they experience their authority to assert what feels like the Senator’s rights?

To begin with, how will the third party even know they have rights to assert? Investigatory policing hinges on the fiction of “voluntariness”—police routinely get inside the most sacred of Fourth Amendment spaces, the home, simply by asking permission to come in. But to the extent that we barely accept this fiction of voluntariness in the context of intrusions on suspects themselves—individuals that we expect to have clear instincts against complying—we might be even more uncomfortable in justifying such intrusions

26. *Massiah v. United States*, 377 U.S. 201 (1964).

27. *Montejo v. Louisiana*, 129 S. Ct. 2079, 2091 (2009) (overruling *Michigan v. Jackson*, 475 U.S. 625 (1986), and holding that court’s appointment of counsel does not preclude further police initiation of questioning); *Texas v. Cobb*, 532 U.S. 162, 172-73 (2001) (holding that *Massiah*’s Sixth Amendment right to counsel at the time of interrogation applies only to formally charged offenses and their equivalents under the exceedingly narrow *Blockburger* “same offense” test).

28. Katie Hafner & Matt Richtel, *Google Resists U.S. Subpoena of Search Data*, N.Y. TIMES, Jan. 20, 2006, at A1 (noting that three of its competitors complied without resisting).

29. Ashley Fantz, *Forgive Us, Father; We’d Rather Go Online*, CNN, Mar. 13, 2008, <http://www.cnn.com/2008/LIVING/wayoflife/03/13/online.confessions/> (discussing rise in both religious and non-religious online confession sites).

as voluntary compliance when it is a third party being asked to sell someone else down the river.

More problematically, what if the third party wants to comply? Even more troubling, what if the Senator wishes they would not? Should a third party's autonomous desire to share the Senator's secret or offer up records given in confidence be restrained in the name of safeguarding the Senator's Fourth Amendment rights? Is there any principled basis for allowing the Senator to voluntarily provide information or give up documents to investigators (perhaps to curry favorable treatment) while forbidding the same voluntary compliance from third parties? Even if such a basis existed, could it be articulated and enforced?

These are real problems, to be sure. But they have available, if imperfect, solutions that fall short of dispensing with third-party protections altogether. For starters, we could simply allow third parties to waive Fourth Amendment rights as easily as we allow the defendant to do the same. Crazy, maybe, but that would make the real risk of disclosure to third parties the possibility of picking someone who doesn't have your back. As it stands, third-party doctrine admits no difference between good choices and bad choices: it draws no meaningful distinction between third parties that want to shield the confidence and those that do not.

But why should this be so? A reconstituted third-party doctrine might recognize that some disclosures are made in confidence, that there is value to such confidence, and that if the parties respect it, then the government should too. In such a regime, disclosures made to informants and undercoverers, of course, would remain unregulated (as "bad choices" in which to repose confidence), but at least constitutional protection would extend to information held by protective entities and true confidantes. Pick a good ISP or best friend, willing to resist government inquiries and assert Fourth Amendment protection, and you can rest assured—well, at least until the government returns with a warrant and probable cause.

We might even devise a sliding scale of protections that aims to embody important communal and constitutional values: the role of trust in our society, the notion of agency, the need and desirability of third-party confidences, and some idea of autonomy and consent. We could imagine an imperfect but viable hierarchy of disclosures, and concomitant ranges of protection to lack of protection, for disclosures that are of absolute necessity (e.g., medical) to those of effective necessity (e.g., banks, utilities, e-mail, etc.) to those of comfort and convenience (e.g., friends, entertainment records) to those that are primarily elective (e.g., social networks, blogs, etc.). The question of which third parties receive protection may be tricky, to be sure. But how to enforce those protections seems less problematic.

Moreover, we might even impose a heightened standard for what constitutes “voluntary” disclosure of information held by third parties. We might, for instance, require covered third parties (imagine for instance banks and medical professionals) to be informed of the Fourth Amendment right of the defendant to keep this information from government hands absent a warrant and probable cause, before being asked whether they are willing to waive it. Statutory regimes that impose civil liability for wrongful disclosure represent a variation on this theme: the third parties all know about the individual’s rights, because they are legally entrusted with safeguarding them.

Most importantly, note that neither suggestion eviscerates the government’s investigative authority. We still preserve the power of the government to seek, through a warrant and probable cause or grand jury subpoena, information held in the hands of third parties. The difference is that we also give those parties a right to resist that is akin to the defendant’s own right, and the defendant in turn may assert that information obtained in a non-compliant fashion should be suppressed as a violation of the Fourth Amendment. In essence, this regime represents a form of limited consent.

If this does not sound so radical, it is because it is not. As Professor Kerr himself points out, current statutory doctrines create similar structures.<sup>30</sup> We have a range of statutory protections for health records, financial records, video records, and so on. In his hypothetical, for example, the bank teller could possibly resist the government request under the Right to Financial Privacy Act. Some ISPs have fought government requests for information by claiming their clients’ First Amendment rights or, as in the well-publicized Google search engine query case, generalized privacy protections. Yet the existence of such protections has not ground investigations to a halt, or left the government hobbled by a confusing web of indiscernible rules. And of course, worst-case scenario: the evidence is suppressed. A wrong call on third-party protection (“what, that was your sister?!”) does no more or less damage than a wrong call on reasonable, articulable suspicion.

In the end, then, it may very well be that Professor Kerr and I differ more as a matter of form or institutional preference than of substance. He says that the legislature should craft such regimes. I worry that the legislature *will* create entitlements for the issues and concerns that are raised by its powerful constituents and lobbyists, but that the poor and disempowered will be left unprotected. And that is a result that, given the values enshrined in the Fourth Amendment, to me seems both unnecessary and indefensible.

---

30. Kerr, *supra* note 1, at 596.