SUBSTITUTION EFFECTS: A PROBLEMATIC JUSTIFICATION FOR THE THIRD-PARTY DOCTRINE OF THE FOURTH AMENDMENT

BLAKE ELLIS REID*

INTRODUCTION

In the past half-century, the Supreme Court has crafted a vein of jurisprudence virtually eliminating Fourth Amendment protection in information turned over to third parties—regardless of any subjective expectation of privacy or confidentiality in the information on the part of

* Juris Doctor 2010, University of Colorado School of Law and Editor-in-Chief, Journal on Telecommunications and High Technology Law. This essay is adapted from *Tilting at Windmills: A Response to the Unpersuasive Case for the Third-Party Doctrine*, a paper written for Professor Paul Ohm's Information Privacy seminar in Fall 2008. I thank Mimi Poe for her hard work in helping me to shepherd the essay to completion and Professor Ohm, Professor Orin Kerr, Professor Bill Pizzi, Chris Soghoian, Wendy Seltzer, Devin Looijen, Dan McCormick, Avi Loewenstein, Tyler Martinez, Per Larsen, Doug McQuiston, Kathleen Ellis, and Sara Reid for their helpful feedback. All errors and omissions are my own.

the revealer.[1] This so-called "third-party" doctrine of the Fourth Amendment has become increasingly controversial in light of the growing societal reliance on the Internet in the United States, where nearly every transaction requires a user to turn information over to at least one third party: the Internet service provider ("ISP").

Citing the scholarship that has criticized the third-party doctrine would make for "the world's longest law review footnote."[2] This essay instead focuses instead on a *justification* for the doctrine advanced by prominent computer crime scholar Orin Kerr. In his controversial[3] essay *The Case for the Third-Party Doctrine*, Professor Kerr argues that the third-party doctrine is essential to preclude criminals from substituting private transactions involving third parties (particularly ISPs) for the criminals' formerly public transactions, which were subject to police surveillance.[4] This essay examines various descriptive and normative gaps that potentially undermine the "substitution effects" justification.

I. THE THIRD-PARTY DOCTRINE AND SUBSTITUTION EFFECTS

The Supreme Court succinctly articulated the third-party doctrine in *United States v. Miller*:

> This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.[5]

Normally, a search that yields information of a suspect by law enforcement officials is subject to an inquiry about whether the individual possessed a reasonable expectation of privacy in the information.[6] Under the third-party doctrine, however, an individual usually has no reasonable expectation of privacy in information she turns over to a third party.[7]

---

1. *See, e.g.*, United States v. Miller, 425 U.S. 435, 443 (1976) (internal citations omitted).

2. Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 n.5 (2009).

3. *See generally* Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 BERKELEY TECH. L.J. 1199 (2009); Erin Murphy, *The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239 (2009) (responding to Professor Kerr's justification).

4. Kerr, *supra* note 2, at 573–81.

5. *See Miller*, 425 U.S. at 443.

6. *See, e.g.*, Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

7. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 743–44 (1979). However, the Court has

Professor Kerr's primary argument in support of the doctrine is functional: opportunistic criminals in the absence of the third-party doctrine would simply substitute public aspects of their crimes (e.g., stalking a victim in person) with private transactions (calling the victim on the phone).[8] By neutralizing these "substitution effects," the third-party doctrine arguably ensures the technological neutrality of the Fourth Amendment by deterring criminals from making opportunistic substitutions.[9] Professor Kerr worries that, without the third-party doctrine, opportunistic criminals could weave a web of Fourth Amendment protection and "effectively hide their criminal enterprises from observation."[10]

Under this argument, the Fourth Amendment strikes a balance between privacy and security, drawing a line beyond which law enforcement officers no longer need seek a warrant before performing an investigation.[11] Normally, the line is drawn with little difficulty on the basis of location; for example, officers need a warrant to search a person's home, but not a public field.[12]

However, the line-drawing exercise arguably becomes problematic when officers need a warrant to obtain information placed in the hands of third parties.[13] With the increasing potency of technology, a criminal could plan and execute a crime entirely from her home, knowing that the police could not send in undercover agents, record phone calls, or watch Internet activity without a warrant, thus creating "a bubble of Fourth Amendment protection."[14] With every element of the crime shielded by a reasonable expectation of privacy, law enforcement officers would be stuck in an untenable situation, needing probable cause to observe evidence of the crime but needing to observe the crime to have probable cause.[15] Accordingly, access to evidence from third parties would largely be eliminated from police investigations.[16]

Under the substitution effects justification, the third-party doctrine rights the balance, forcing elements of crimes that technology has made private—such as phone calls and Internet usage—back into the public

been inconsistent in applying the doctrine in recent years. *See, e.g.*, United States v. Kyllo, 533 U.S. 27, 40 (2001) (holding that heat emanations from a home, effectively turned over to any third party that walks by the home, are nonetheless searched by police using a thermal scanner because the scanner reveals "details of the home").

8. Kerr, *supra* note 2, at 573, 576.
9. *Id.* at 573.
10. *Id.*
11. *Id.* at 574.
12. *Id.*
13. *Id.* at 575–76.
14. *Id.* at 576.
15. *Id.*
16. *Id.*

sphere for the purposes of Fourth Amendment protection, cementing the aforementioned technological neutrality.[17]

Professor Erin Murphy, a vocal critic of *The Case for the Third Party Doctrine*, admits that Professor Kerr's insight regarding technological neutrality and substitution effects is "quite compelling."[18] And Professor Kerr's jurisprudential clout with the courts in the area of criminal procedure and technology is well established.[19] As such, it seems likely that Professor Kerr's novel justification for the third-party doctrine will garner serious consideration both in academia and the judiciary. Accordingly, a closer examination of the descriptive and normative underpinnings of Professor Kerr's argument seems warranted.

II. DESCRIPTIVE PROBLEMS WITH SUBSTITUTION EFFECTS

The substitution effects justification is descriptively problematic in both jurisprudential and political senses. First, the Supreme Court has never embraced the justification, rendering its adoption a radical departure from existing jurisprudence. Second, it is unclear that the third-party doctrine's preclusion of substitution effects in fact maintains any semblance of technological neutrality in the Fourth Amendment.

A. Criminal Motivation: The Supreme Court and Substitution Effects

The motivations behind criminal behavior are not easily distilled.[20] A particular criminal action may be motivated by a need for privacy, a need for public exhibition, some combination of both, or something else entirely. Thus, whether criminals on average opportunistically substitute private acts for public is a complex empirical question. Professor Kerr, however, asserts simply that "any smart criminal will exercise the option" to substitute private acts for public.[21] This rhetorical sweep belies the possibility that, from a policymaking standpoint, the average criminal might *not* engage in opportunistic substitutions,[22] the third-party

17. *See id.* at 577.

18. Murphy, *supra* note 3, at 1241.

19. Professor Kerr's works on criminal procedure and technology have recently been cited by several federal courts. *E.g.*, U.S. v. Johnson, 584 F.3d 995, 1000 n.4 (10th Cir. 2009) (citing Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503 (2007)).

20. *See* CURT R. BARTOL & ANNE M. BARTOL, PSYCHOLOGY AND LAW: THEORY, RESEARCH, AND APPLICATION 409–11, 424–27 (3d ed. 2004) (describing the complex nature of psychological criminology and the psychosocial factors of criminal behavior).

21. Kerr, *supra* note 2, at 580.

22. One reason for this possibility is that the average criminal might not be very smart. As one commentator points out, "The law is designed . . . to catch drug dealers who go ninety miles per hour while carrying a kilogram of cocaine in their trunks—not those who maintain good operational security and only break one law at a time." E-mail from Christopher

doctrine notwithstanding.[23] Called on this point by Professor Murphy,[24] Professor Kerr responds that a criminal's subjective motivations are irrelevant since third-party transactions shielded by the Fourth Amendment are always problematic.[25]

The debate over subjective intent notwithstanding, Professor Kerr argues that substitution effects explain the jurisprudential foundations for the third-party doctrine—in particular, the Supreme Court's opinions in *United States v. Miller* and *Smith v. Maryland*.[26] As discussed below, however, the criminals in those cases arguably did not opportunistically substitute private acts for public. Accordingly, the Court could not have considered the substitution effects justification, much less embraced it, in those seminal third-party doctrine cases. As such, explicit adoption of the justification by courts in the future would constitute a radical change in third-party doctrine jurisprudence rather than a consistent application of past precedent.

1. *United States v. Miller*

In *Miller*, a bootlegger purchased equipment for an illicit alcohol production operation using his checking account.[27] Alcohol, Tobacco, and Firearms Bureau (ATF) agents, who had no warrant, obtained from the bootlegger's bank the checks used to purchase the equipment.[28] Copies of the checks were introduced at trial,[29] and the bootlegger was convicted.[30] Affirming the third-party doctrine, the Supreme Court held that the bootlegger, by using checks, had effectively turned over information about his purchases to a third-party (the bank) and, accordingly, had no legitimate expectation of privacy in the checks.[31]

Imagining a hypothetical "world without banks," Professor Kerr argues that the availability of the checking account created a substitution effect, allowing the bootlegger to substitute a private act (paying with a check) for a public act (paying with cash).[32] Without banks, or so the

Soghoian, Ph.D. Candidate, Indiana University, to Blake Reid (Jan. 8, 2010, 15:57 MST) (on file with author).

23. The substitution effects justification also presumes that criminals know about and understand the third-party doctrine—a presumption for which no evidence is presented.

24. Murphy, *supra* note 3, at 1241–45.

25. Orin S. Kerr, *Defending the Third-Party Doctrine: A Response to Epstein and Murphy*, 24 BERKELEY TECH. L.J. 1229, 1233–34 (2009).

26. *Id.* at 577-79.

27. United States v. Miller, 425 U.S. 435, 436–37 (1976).

28. *Id.* at 437.

29. *Id.* at 438.

30. *Id.* at 436.

31. *See id.* at 442–43 ("The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.") (citations omitted).

32. Kerr, *supra* note 2, at 579.

argument goes, the bootlegger and the equipment seller would have had to travel back and forth to their cash "stashes," thus exposing their activities to the public.[33] The check, on the other hand, allowed the two parties to complete the transaction without the need to visit their respective stashes, rendering the entire transaction private.[34]

Further analysis, however, reveals that the use of the check provided no *ex ante* privacy from the police to either the bootlegger or the seller. Furthermore, the use of the check provided *less ex post* privacy to both parties than if the bootlegger had used cash.

From an *ex ante* perspective, the bootlegger needed to travel to retrieve his checkbook, and the seller needed to travel to the bank to deposit his check. Even if the bootlegger had traveled to retrieve cash from his stash, and the seller had traveled to his stash to deposit the cash, *ex ante* observation of the travels would have given the ATF agents no useful information about the transaction itself, nor even any reason to suspect that something was amiss.

Furthermore, the true privacy interest in *Miller* was not in travelling with money, but rather in the transaction itself—the exchange of money for the illegal bootlegging equipment. The use of a check gave the ATF agents the ability *ex post* to discover that the bootlegger had paid the seller for the still. If the buyer had used cash, the ATF agents merely would have been able to discover that the bootlegger had withdrawn cash from his bank account and that the seller had deposited cash in his—or, in the world without banks, nothing at all.

It is unclear why the bootlegger chose to pay with a check. Perhaps he was concerned about being robbed while carrying around a substantial sum of money. Regardless, the less private nature of using a check (from an *ex post* perspective) suggests that the bootlegger's payment choice was probably not motivated by privacy.

2. *Smith v. Maryland*

Of course, some criminals may in fact augment public acts with complementary private acts; *Smith v. Maryland* provides nominal support for that assertion.[35] But *Smith* merely illustrates an *augmentation* of public behavior with a different and complementary private behavior, rather than an opportunistic *substitution*.

In *Smith*, a robber began to stalk his victim following the robbery, making threatening phone calls to her home.[36] The telephone company, at the request of Baltimore police (who, again, had no warrant), installed

33. *Id.*
34. *Id.*
35. Smith v. Maryland, 442 U.S. 735, 737 (1979).
36. *Id.*

a pen register device, which tracked the numbers dialed by the robber, and subsequently caught him calling the victim again.[37] On the basis of this evidence, the police were able to obtain a warrant to search the robber's home and he was eventually convicted of robbery.[38] The Supreme Court again affirmed the third-party doctrine, holding that the robber held no legitimate expectation of privacy in the phone numbers he dialed since he had turned them over to a third party (the phone company).[39]

Professor Kerr argues that the robber intentionally substituted a private act (stalking the woman over the phone) for a public act (stalking her in person).[40] However, the robber stalked the woman in person after the robbery[41] *in addition to* stalking her over the phone. There is nothing to suggest that he undertook the phone stalking *in lieu* of in-person stalking; the fact that he undertook both methods of stalking suggests not that they were substitutes for one another, but rather complementary activities. Thus, the idea that the robber was motivated by privacy when he harassed his victim over the phone is speculative.

3. The Supreme Court Has Not Adopted the Substitution Effects Justification

That *Miller* and *Smith* arguably do not involve opportunistic substitution effects does not necessarily doom future use of the justification.[42] However, as the foregoing discussion illustrates, the Supreme Court has never considered the justification, much less embraced it. Accordingly, the adoption or invocation of the justification by judges and lawyers should not be viewed as in comport with existing jurisprudence, but rather as a radical shift demanding a normative consideration of underlying policy concerns.[43]

B. Technological Neutrality and Surveillance Myths

Accepting the proposition that substitution effects indeed exist,[44] it is nonetheless also questionable whether precluding such effects maintains any meaningful sense of technological neutrality in the Fourth

37. *Id.*
38. *Id.* at 737–38.
39. *See id.* at 745
40. Kerr, *supra* note 2, at 578.
41. *See Smith*, 442 U.S. at 737.
42. E-mail from Orin Kerr to Blake Reid (January 15, 2009, 20:58 MST) (on file with author).
43. This essay argues that Professor Kerr has not presented a sufficient normative case for using the justification. *See* discussion *infra* Part III.
44. Kerr, *supra* note 25, at 1234.

Amendment.

Under Professor Kerr's neutrality argument, precluding substitution effects prevents savvy criminals from taking advantage of new privacy-enabling technology, thus righting a hypothetical balance of privacy and security whenever a given technology would give criminals an advantage over law enforcement.[45]

The neutrality argument, however, relies on the false premise that law enforcement has an *unlimited* capability to surveil low-tech public activities and a *limited* capability to surveil high-tech private activities. As discussed below—both generally and in the context of *Miller* and *Smith*—the opposite is often true.[46] That is, the use of technology often allows law enforcement, with the power of the third-party doctrine, to surveil more people more extensively at lesser expense.

1. Low-Tech Langour, High-Tech Hypertrophism

Low-tech surveillance, such as committing officers to stakeouts and tracking work, is expensive—and funding of boots-on-the-ground police presence seems to be on a problematic decline in the United States. Professor William Stuntz points out that "[t]he key problem that faces American policing today is that not enough money is spent on it."[47]

For example, in New Orleans, an area devastated by high crime since Hurricane Katrina, the police department was relegated to operating out of portable trailers and was even forced to take a collection to pay for the cleaning of their portable toilets.[48] Worse yet, worried officers had to turn to local donors to replace water-damaged bulletproof vests and weren't able to get enough to protect the entire force.[49] Thousands of alleged criminals were released because the police were unable to gather sufficient evidence to charge them; only a single fingerprint examiner and only one firearm examiner remained on the force as of June 2007, despite the city having experienced a nation-high 90 murders during the previous six months.[50]

A recent Wisconsin killing spree illustrates the underfunding problem in the particular context of low-tech surveillance.[51] Law

45. Kerr, *supra* note 2, at 579–81.

46. For a more generalized articulation of police surveillance capabilities in low-tech and high-tech circumstances, see Paul Ohm, *Probably Probable Cause: The Diminishing Importance of Justification Standards*, 94 MINN. L. REV. 1514 (2010).

47. William J. Stuntz, *Accountable Policing* 5 (Harvard Public Law Working Paper No. 130, 2006), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=886170.

48. *See* Gilbert Cruz, *New Orleans: Police Still Underfunded*, TIME, June 20, 2007, http://www.time.com/time/nation/article/0,8599,1635439,00.html.

49. *Id.*

50. *Id.*

51. *See* Sandy Cullen, *Witzel Manhunt Reveals 'Limited Resources' of Police*, WIS. ST. J.,

enforcement agencies were on the lookout for a fugitive in the hours after he killed a man for allegedly having an affair with the fugitive's ex-girlfriend.[52] The fugitive successfully evaded the police for nearly 2000 miles before predictably returning a week later to his ex-girlfriend's Wisconsin home to kill one of her family members.[53] "It doesn't really surprise me," commented Michael Scott, the director of the Center for Problem-Oriented Policing at the University of Wisconsin at Madison.[54] "It does kind of point out the limited resources police, under the best of circumstances, have," Scott continued.[55] "We sometimes get a false sense of security about what the police can do to protect us."[56] Asked why the police, knowing that the killer might turn up at the ex-girlfriend's house, didn't simply surveil the house 24 hours a day, Scott commented that such surveillance would be a "near impossibility" for police in a rural community and something even police in a major city would likely be unable to do.[57] The sheriffs involved agreed, pointing out that no more than two to four deputies were normally available on a given night to police the *entire county*[58] (which covers over 750 square miles).[59] "We wouldn't do that on any case," one sheriff commented, "[unless] we expected there would be a great likelihood of a crime."[60]

While many police departments seem to be struggling to implement effective low-tech surveillance (even to prevent serious crimes like murder, as in the previous example), the high-tech surveillance of third-party related activities is on the rise. Professor Christopher Slobogin points out that government agencies have been "eager" since the terror attacks of September 11, 2001 to experiment with "data-mining," the process of analyzing information recorded about its citizens through various transactions.[61] In 2003, Congress opened the door for ominous, Orwellian-sounding programs such as TIA (Total Information Awareness), ADVISE (Analysis, Dissemination, Visualization, Insight, and Semantic Enhancement), and TALON (Threat and Local Observation Notice).[62] These programs, recently culminating in the $380

Nov. 14, 2008, http://www.madison.com/wsj/topstories/314347.

52. *Id.*

53. *Id.*

54. *Id.*

55. *Id.*

56. *Id.*

57. *Id.*

58. *Id.*

59. Wisconsin Online, Iowa County, Wisconsin, http://www.wisconline.com/counties/iowa/ (last visited May 10, 2010).

60. Cullen, *supra* note 51.

61. Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 317 (2008).

62. *Id.* at 317–19.

million Information Fusion Center project, bring together data from the public and private sector to centralize information about individuals, including "banking and finance, real estate, education, retail sales, social services, transportation, postal and shipping, and hospitality and lodging transactions."[63] If operational difficulties[64] can be overcome, these programs could provide law enforcement officers with an unprecedented view of the daily lives of American citizens—particularly criminals[65]—and companies like Google and Oracle are poised to fill in the gaps where the government has failed thus far.[66]

2. *Miller* and *Smith* Revisited

Miller aptly showcases the low-tech/high-tech surveillance dichotomy. Recall the argument that the bootlegger in *Miller* substituted a private act (paying with a check) for a public act (paying with cash).[67] The implicit assertion that the bootlegger's malfeasance would have been easily discovered if the bootlegger had paid with cash[68] is only true if the ATF had infinite surveillance capabilities.

To be precise, the argument goes:

> If you need to pay for something in this world, you would need to get the money to do it: You would need to travel to your stash, pick up the money, and then travel to the place where you are making your purchase. If you are the seller, you need to take the money, take it back to your stash, and store it away for safekeeping. There are public parts of the transaction on both sides.[69]

While there are several public aspects of the transaction, it is unclear why the ATF would have surveiled any of them—unless it was engaged in suspicionless, dragnet surveillance of everyone. The bootlegger, for example, did nothing to arouse ATF suspicions until well after the transaction was complete.[70] Thus, it is unlikely that ATF agents would have uncovered any evidence of the transaction if the bootlegger had paid with cash.

---

63. *Id.* at 318 (citations omitted).

64. *Id.* at 324–25.

65. *Id.* at 323–24.

66. *Id.* at 327; *see also* Christopher Sohoian, *8 Million Reasons for Real Surveillance Oversight*, SLIGHT PARANOIA, Dec. 1, 2009, http://paranoia.dubfire.net/2009/12/8-million-reasons-for-real-surveillance.html (describing the extensive surveillance capabilities provided to law enforcement by telecommunications companies).

67. Kerr, *supra* note 2, at 579.

68. *See id.*

69. *Id.*

70. In *Miller*, the police were actually alerted to the bootlegger's illicit activities by a fire in his warehouse. United States v. Miller, 425 U.S. 435, 437 (1976).

On the other hand, the bootlegger's use of a check allowed the agents to find evidence of his transactions *ex post* without using any prospective surveillance. That the bootlegger used more advanced technology (a check) actually broadened the scope and accuracy of the surveillance techniques available to the agents—without any corresponding increase in cost. Thus, the third-party doctrine in *Miller*, did not maintain technological neutrality, but rather provided the police with better, cheaper surveillance than they would have had prior to the technological advance.

Smith provides another example of the low-tech/high-tech surveillance dichotomy. Recall the argument that the stalker substituted a private act (over-the-phone stalking) for a public act (in-person stalking).[71] The implicit assertion that the police would have an easy time catching the stalker in person[72] is only true if the police had unlimited surveillance resources. They would have had to canvas the neighborhood, staking out the victim's house until the stalker showed up, with little reason to expect that he would do so. It is unlikely that the Baltimore police, who struggled with record-high crime rates in the 1970s,[73] would have dedicated the resources necessary to catch the stalker in person.

However, the substitution of a high-tech activity (the frequent harassing phone calls) gave the police the necessary suspicion to canvas the neighborhood and discover the stalker's identity, allowing them to set up the pen register on his phone.[74] Again, the third-party doctrine provided not technological neutrality, but a substitution of cheap, hands-off surveillance for expensive, in-person surveillance, thereby increasing the evidence that the police were able to obtain.

3. A Thought Experiment

As illustrated by *Miller* and *Smith*, the simultaneous lack of surveillance capabilities for low-tech public acts and overdevelopment in the high-tech surveillance of private, third-party facilitated acts indicate that the third-party doctrine may often provide law enforcement officials with *more* power to collect evidence about and prevent private crimes than public crimes. This outcome indicates technological bias, rather than neutrality, in the third-party doctrine.

---

71. Kerr, *supra* note 2, at 578.

72. *See id.* at 577–78.

73. For example, the robbery rate in Baltimore began a historic increase in the late 1970s, nearly double that of the neighboring cities of Washington, D.C. and Philadelphia. RALPH B. TAYLOR, BREAKING AWAY FROM BROKEN WINDOWS: BALTIMORE NEIGHBORHOODS AND THE NATIONWIDE FIGHT AGAINST CRIME, GRIME, FEAR, AND DECLINE 35–36 (2001).

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

To confirm this with a thought experiment, consider crimes committed entirely over the Internet in comparison to their physical-world equivalents—for example, hacking into a bank website and virtually transferring money to another account, versus breaking into and robbing a brick-and-mortar bank.

With the brick-and-mortar robbery, the police will need to obtain a warrant and dedicate significant resources to find evidence of the crime (e.g., the robbers may stash the stolen money and weapons used in the robbery in one of their own houses) and may need to conduct widespread low-tech surveillance to prevent the destruction of evidence (e.g., the robbers may have a sophisticated money laundering operation).

On the other hand, because Internet service providers are now able to keep accurate logs of all users' online activity,[75] the police will be able to obtain evidence of every step taken during the crime simply by calling the ISP and asking for it—with no need for a warrant under the third-party doctrine.[76]

Contrast the two crimes: with the physical robbery, a public crime with no third parties involved, the police are placed at least at a nominal disadvantage in terms of obtaining evidence of the crime; they must obtain a warrant and dedicate significant officer resources toward surveillance to obtain the evidence. With the online robbery, a private crime facilitated with the help of an Internet service provider, a third party, the police need not obtain a warrant or invest any officer resources towards surveillance if the ISP chooses to cooperate.

It follows, then, that the third-party doctrine often fails to maintain technological neutrality, instead giving the police unbounded access to evidence where the Fourth Amendment previously would have posed limits.

III. INNOCENCE CONSIDERATIONS: A NORMATIVE GAP

The descriptive problems with the substitution effects justification demand further normative investigation. Indeed, the preclusion of substitution effects is a normatively problematic basis for crafting Fourth

75. This is no longer a paranoid fantasy for the tin-foil hat set. Professor Paul Ohm argues that pervasive "complete monitoring" of all user traffic by Internet Service Providers (ISPs) is a real possibility. *See generally* Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. ILL. L. REV. 1417 (2009). Furthermore, there is a push to require such logging statutorily. *See* Kevin Fayle, *Congress Pushes (Again) For ISP Data Retention*, THE REGISTER, Feb. 12, 2007, http://www.theregister.co.uk/2007/02/12/congress_isp_data_retention_push/.

76. Of course, this hypothetical experiment ignores the real-world impact of the Wiretap, Pen Register, and Stored Communications Acts, since they are congressionally mandated rollbacks to the sweeping nature of the third-party doctrine that probably would have been unnecessary in the doctrine's absence.

Amendment jurisprudence because it disproportionately focuses on criminal activity and efficient law enforcement without adequately considering the privacy rights of innocent citizens. Although the prospect of letting a guilty criminal go free often favors expansive search abilities for the police,[77] both the Supreme Court and scholars have demanded an approach to Fourth Amendment jurisprudence based at least partly on innocence considerations.

Applying this normative framework to the substitution effects justification reveals that the third-party doctrine, even if it works as advertised, may problematically preclude innocent citizens, not just criminals, from opportunistically substituting private acts for public. Furthermore, the third-party doctrine may induce innocent citizens to avoid socially productive uses of technology—perversely causing inverse substitution effects.

A. Innocence Ideology and the Fourth Amendment

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ."[78]

At least from a textual perspective, the primary purpose of the Fourth Amendment is to protect the privacy of citizens from inappropriate governmental intrusion. The Supreme Court agreed in *Schmerber v. California*: "The overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State."[79]

The motivation for such an intrusion may simply be the desire for efficiency by law enforcement officials. George Orwell grimly points out, though, that the motivation for seeking the power to intrude on the privacy of citizens indiscriminately may be insidiously self-evident:

> [We seek] power entirely for its own sake. We are not interested in the good of others; we are interested solely in power. . . . We know that no one ever seizes power with the intention of relinquishing it. Power is not a means, it is an end. . . . The object of persecution is persecution. The object of torture is torture. The object of power is power.[80]

77. S*ee* Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 MICH. L. REV. 1229, 1230 (1983) (noting the proclivity of the Supreme Court to incorrectly focus on the guilty, including the particularly egregious example of *United States v. White*, 401 U.S. 745 (1971)).

78. U.S. CONST. amend. IV.

79. 384 U.S. 757, 767 (1966).

80. GEORGE ORWELL, 1984, at 263 (Signet Classic 1950) (1949).

Regardless of the motivation, the Court further acknowledges that "[t]he security of one's privacy against arbitrary intrusion by the police" is "at the core of the Fourth Amendment" and "basic to a free society."[81]

Professor Arnold Loewy argues that the Fourth Amendment serves to shield the privacy rights of *innocent* civilians, and that the guilty are merely "incidental beneficiaries" of the amendment's protections.[82] Indeed, the amendment puts a textual thumb on the scale, favoring the privacy of innocent citizens over the desire to catch and punish criminals.

To illustrate this point, imagine that a robbery is committed in a small, isolated town with one thousand homes. The police are certain that the culprit lives in town, but have no idea who he or she is. Accordingly, the police search every home in town for the stolen goods, and eventually find them, thus identifying the robber.

From the perspective of catching and punishing criminals, the situation is a success on two levels. An *ex ante* evaluation would predict that the searches collectively have a one-hundred percent likelihood of finding the stolen goods; an *ex post* evaluation would reveal that the searches indeed succeeded in finding the goods and catching the criminal. Yet, the searches almost certainly would violate the Fourth Amendment.[83] As a result, evidence of the stolen goods would be excluded from use in prosecuting the robber,[84] who would likely get off scot-free despite damning evidence of his criminal conduct.

This non-intuitive result is arguably a positive one, however. An *ex ante* evaluation would predict that an individual search has a one-tenth of one percent chance of catching the criminal and a ninety-nine point nine percent chance of violating the privacy of an innocent citizen; an *ex post* evaluation would reveal that, indeed, nine-hundred and ninety-nine of the searches violated the privacy of innocent civilians and failed to catch the criminal.[85] Such a result would be too a heavy price to pay in the eyes

81. Wolf v. Colorado, 338 U.S. 25, 27 (1949).

82. Loewy, *supra* note 77, at 1229–1230.

83. The Fourth Amendment would govern the search of each house. *See* Lewis v. U.S., 385 U.S. 206, 211 (1966) ("Without question, the home is accorded the full range of Fourth Amendment protections."). Warrantless searches of homes for objects (the stolen goods, in this case) are generally prohibited absent probable cause. Agnello v. U.S., 269 U.S. 20, 33 (1925) ("Belief, however well founded, that an article sought is concealed in a dwelling house, furnishes no justification for a search of that place without a warrant. And such searches are held unlawful notwithstanding facts unquestionably showing probable cause.") Though probable cause is "not readily, or even usefully, reduced to a neat set of legal rules," *Illinois v. Gates*, 462 U.S. 213, 232 (1983), it is hard to imagine a court considering a one percent likelihood "probable" in any sense of the word.

84. *See* Ker v. California, 374 U.S. 23, 30–31 (1963).

85. Of course, if the police were to stop the search immediately after finding the evidence for which they were searching, they might search fewer than all the homes. Then again, thoroughness concerns might motivate them to extend the search to all of the houses "just in case."

of the Fourth Amendment.

This example underscores Professor Loewy's point: inherent in the Fourth Amendment is a focus on protecting the privacy of innocent citizens. Even when a search tactic is *guaranteed* to be successful in catching a criminal, the Fourth Amendment may preclude it if it is likely to violate the privacy of innocent citizens.[86] Accordingly, focusing solely on the capture of the guilty when evaluating Fourth Amendment doctrine is insufficient; a holistic approach should consider the privacy of innocent citizens as well.

B. The Substituting Innocent Citizen

The innocence rubric reveals an unanticipated consequence of the third-party doctrine: if it precludes criminals from opportunistically substituting private acts for public, it may do the same to innocent citizens.

Assume *arguendo* that the bootlegger in *Miller* and the stalker in *Smith* engaged in opportunistic substitutions in committing their crimes. It might be tempting, then, to justify the third-party doctrine by solely evaluating the judicial outcomes—in both cases, the criminal was captured and convicted, a desirable result. But consider the innocent citizens whose records were searched in each case. Perhaps the bootlegger wrote alimony checks to an ex-wife, the amounts of which suddenly became known to the police. Perhaps the stalker made calls to his therapist, revealing their relationship. Everyone to whom the bootlegger wrote checks and who wrote checks to the bootlegger had their identities revealed to the police.[87] Everyone to whom the stalker placed a call had her identity similarly revealed.[88] Presumably, all of these people were innocent, or at least not suspected by law enforcement of having committed any crime. Perhaps many of them had chosen to use checks and telephones to substitute *innocent* private acts for previously public acts. The police violated the privacy of each of those individuals.

It is not difficult to imagine that the third-party doctrine could facilitate even more insidious privacy violations. For example, a journalist may be working on a story on police corruption. In retaliation, the police, without violating the Fourth Amendment, could log everyone that the

86. That the criminal "incidentally benefits," as Professor Loewy puts it, by having the evidence against her excluded from use in prosecution is not the goal of the Fourth Amendment, but merely a necessary incentive to prod the police into being reasonably sure that their tactics do not violate the privacy of innocent citizens. *See* Elkins v. United States, 364 U.S. 206, 217 (1960) ("The [exclusionary] rule is calculated to prevent, not to repair. Its purpose is to deter—to compel respect for the constitutional guaranty in the only effectively available way—by removing the incentive to disregard it.") (citation omitted).

87. *See* United States v. Miller, 425 U.S. 435, 437–38 (1976).

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

journalist calls—and reveal the identity of a previously anonymous whistleblower in their department.

It is quantitatively difficult to compare the privacy costs to innocent citizens with the cost to society of letting some criminals go free. Of course, the courts in the foregoing cases both decided (perhaps unconsciously) that the cost to society was higher. And there are ways to protect the privacy of individuals associated in private transactions with criminals. For example, the police in *Smith* could have filtered out all phone calls except to the victim.[89] But as a normative matter, it seems essential to balance the efficiency gains for law enforcement against the privacy costs to innocent citizens prior to invoking the third-party doctrine.

C. Self-Flagellation and Reverse Substitution Effects

It is possible that the aforementioned privacy costs of the third-party doctrine to innocent citizens may cause them to stop making socially productive, privacy-enhancing substitutions. Even more perversely, though, it may, in the long run, cause them to make reverse substitutions—from private acts to public acts—to avoid abuse by the police.

Judge Richard Posner's *reductio ad absurdum* argument considers the hypothetical consumer seeking absolute privacy: a veritable hermit who gives up his driver's license (because of the required disclosure of personal information to the DMV), his job (because of the required verification of references), his credit cards (because of the required submission to an intrusive credit check), his phone (because of possible government surveillance) and so on.[90] The Internet provides a poetic illustration of such a consumer: anonymous Slashdot[91] poster "KlaymanDK," who queried the digital masses about the privacy costs of third-party

89. Of course, the police are not necessarily likely to implement filters—and filters may be difficult or impossible to implement in some situations. In *Payner v. United States*, an IRS special agent on the hunt for a narcotics trafficker arranged an illegal scheme to search the banker's briefcase without the banker's knowledge, photographing over 400 pages of documents. 447 U.S. 727, 730 (1980). Though the documents lead to the conviction of the scofflaw, it's unclear that the IRS was actually looking for him in the first place. Thus, the IRS likely could not have filtered the evidence to protect details of the bank transactions of innocent citizens. The Colorado Supreme Court recently used this rationale to reject the third-party doctrine in context of a police search of over 5,000 tax returns seized from a tax preparer, pointing out that the search was an impermissible "fishing expedition" into the files of clients, "the substantial majority of which were free from any evidence of wrongdoing." *See* People v. Guiterrez, 222 P.3d 925, 944 (Colo. 2009) (en banc) ("[T]he limitations imposed by the warrant on the scope of the search were ineffective, as the officers seized *all* tax returns in [the preparer's] custody, including those not authorized by the warrant.").

90. Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. CHI. L. REV. 245, 247–48 (2008).

91. A website devoted to "News for Nerds, Stuff that Matters," http://www.slashdot.org.

transactions:

> Over the last decade or so, **I have strived to maintain my privacy**. I have uninstalled Windows, told my friends 'sorry' when they wanted me to join Facebook, had a fight with my brother when he wanted to move the family email hosting to Gmail, and generally held back on my personal information online. But since, amongst all of my friends, I am the only one doing this, it may well be that my battle is lost already. Worse, I'm really putting myself out of the loop, and it is starting to look like **self-flagellation**. Indeed, it is a common occurrence that my wife or friends will strike up a conversation based on something from their Facebook 'wall' (whatever that is). Becoming ever more unconnected with my friends, live or online, is ultimately harming my social relations. I am seriously considering throwing in the towel and signing up for Gmail, Facebook, the lot. If "they" have my soul already, I might as well reap the benefits of this newfangled, privacy-less, AJAX-2.0 world. It doesn't really matter if it was me or my friends selling me out. Or does it?[92]

KlaymanDK is an example of a presumably innocent citizen worried about turning personal data over to third parties—particularly corporations. He seems concerned about privacy in general; of course, there are many ways for corporations to violate privacy that don't implicate the Fourth Amendment, such as losing data to identity thieves. However, several responses to KlaymanDK's question indicate that Fourth Amendment concerns lurk just beneath the surface for similarly privacy-conscious innocent citizens:

> How do you know your lawful activities will always be lawful? Every time I see someone react with 'I'm not a criminal' fallacy, all I can think of is the question "Are you now, or have you ever been associated with a member of the Muslim faith?" We're not far away from a witch hunt of that flavor.[93]

Applied for a job, while sharing a name with a convicted criminal

92. Posting of kdawson to Slashdot, *Give Up the Fight For Personal Privacy?*, http://yro.slashdot.org/article.pl?sid=08/10/07/2112249 (Oct. 7, 2008, 17:29) (emphasis added). Facebook is a "social-networking" website available at http://www.facebook.com; for a useful primer on the privacy concerns surrounding Facebook, consult Catherine Rampell, *What Facebook Knows That You Don't*, WASH. POST, Feb. 23, 2008, at A15. Gmail is an Internet-based free e-mail service operated by Google available at http://www.gmail.com. For further information on Gmail privacy concerns, consult the website Gmail Is Too Creepy, http://www.gmail-is-too-creepy.com/. Finally, AJAX, or Asynchronous JavaScript and XML, is a term for the collective programming techniques that underlie many modern websites like Gmail and Facebook. For a lay-accessible explanation, see *What is Ajax?*, RIASPOT.COM, July 7, 2008, http://www.riaspot.com/articles/entry/What-is-Ajax-.

93. Posting of Hyppy to Slashdot, Give Up the Fight For Personal Privacy?, http://yro.slashdot.org/article.pl?sid=08/10/07/2112249 (Oct. 7, 2008, 18:37).

> who lives near you? Been pulled over by the police or sent fines for speeding, because someone cloned your car's plates?[94]
>
> [Something may] happen in the future to make currently acceptable, moral, lawful behavior illegal.[95]
>
> I manage to stay out of friend's pictures for this reason. . . . [k]eep in mind that [law enforcement] agencies do look at it during criminal investigations, and use it as evidence. Just some things to keep in mind . . .[96]

Perhaps Professor Loewy was prophetic when he predicted that the police could use evidence wrongfully obtained about innocent citizens "for parlor games, practical jokes, or harassment."[97] These Slashdot users are not just worried about the inability to use Facebook or Gmail—they are worried about police harassment, religious persecution, and false prosecution. And if their self-flagellating avoidance of beneficial technology becomes pervasive, the social costs may be immense.[98]

Even though the third-party doctrine may not be solely to blame for these users' concerns about online privacy, the chilling effect of the doctrine on legitimate, socially productive activities such as the usage of data-collecting Internet web sites by innocent, privacy seeking consumers must also be considered when invoking the preclusion of substitution effects as a justification for the third-party doctrine.

CONCLUSION

Articulating a viable justification for the third-party doctrine is tempting to scholars, particularly given the mountain of critical scholarship indicating that no such justification exists; to justify the doctrine successfully is to triumph over the conventional wisdom. Professor Kerr's argument for the substitution effects justification is compelling in many ways, but its adoption must be tempered by consideration of its descriptive and normative problems.

---

94. Posting of Anonymous Brave Guy to Slashdot, Give Up the Fight For Personal Privacy?, http://yro.slashdot.org/article.pl?sid=08/10/07/2112249 (Oct. 7, 2008, 19:01).

95. Posting of maillemaker to Slashdot, Give Up the Fight For Personal Privacy?, http://yro.slashdot.org/article.pl?sid=08/10/07/2112249 (Oct. 7, 2008, 17:54).

96. Posting of NJRoadfan to Slashdot, Give Up the Fight For Personal Privacy?, http://yro.slashdot.org/article.pl?sid=08/10/07/2112249 (Oct. 7, 2008, 18:36).

97. Loewy, *supra* note 77, at 1253.

98. Even citizens looking for an intermediate approach between shunning technology and giving up their privacy are faced with a dizzying array of technical considerations. *See, e.g.*, Electronic Frontier Foundation, What Can I Do To Protect Myself?, https://ssd.eff.org/3rdparties/protect (last visited May 10, 2010).