St. John's Law Review

Volume 88
Number 2 *Volume 88, Summer 2014, Number 2*

Article 3

October 2015

Of Third-Party Bathwater: How to Throw Out the Third-Party Doctrine While Preserving Government's Ability to Use Secret Agents

Amy L. Peikoff

OF THIRD-PARTY BATHWATER: HOW TO THROW OUT THE THIRD-PARTY DOCTRINE WHILE PRESERVING GOVERNMENT'S ABILITY TO USE SECRET AGENTS

AMY L. PEIKOFF[†]

INTRODUCTION

Whether you refer to Edward Snowden—the former employee of a National Security Agency ("NSA") contractor who has been charged with espionage[1]—as a hero or as a traitor[2] likely depends on your opinion of the programs he has admitted to publicizing[3] via his leaking of highly classified documents. In

---

[†] Visiting Associate Professor of Law and Research Fellow, Southwestern Law School; University of Southern California (Ph.D., 2003); University of California, Los Angeles (J.D., 1998). I am grateful to the Anthem Foundation for Objectivist Scholarship for its support of my research and to APEE for the opportunity to present this Article as a work in progress. I would also like to thank the editorial board and members of *St. John's Law Review* for their assistance in preparing this Article for publication. I dedicate this Article to Edward Snowden, who, as of the time this Article is going to press, is still stuck in Russia.

[1] *U.S. Requests Snowden's Extradition*, WALL ST. J. (June 22, 2013, 4:51 PM), https://web.archive.org/web/20130901080345/http://online.wsj.com/article/SB10001424127887324577904578561731593350320.html.

[2] Andrew Aylward, *Poll: Most See Snowden as Whistleblower Not Traitor*, WALL ST. J. BLOG (July 10, 2013, 12:51 PM), http://blogs.wsj.com/washwire/2013/07/10/poll-most-see-snowden-as-whistleblower-not-traitor/?mod=wsj_streaming_the-surveillance-programs. Among the most vocal of Snowden's critics are former U.N. Ambassador John Bolton, who has repeatedly asked about Snowden, "[W]ho died and made him king?" and the host of Fox News's *Red Eye* and co-host of *The Five*, Greg Gutfeld, who has repeatedly referred to Snowden as a traitor and hypocrite. *See* Melanie Batley & John Bachman, *John Bolton: Snowden 'Committed Act of War Against United States,'* NEWSMAX (June 11, 2013, 2:26 PM), http://www.newsmax.com/Newsfront/bolton-snowden-nsa-leaks/2013/06/11/id/509318/.

[3] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 5, 2013), http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order; Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, THE GUARDIAN (June 6, 2013), http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data. It is not clear whether documents revealing the existence of a third program, a program involving the collection of U.S. email records in bulk, were

one program, Snowden revealed that the NSA has been continuously collecting phone record "metadata" of all Verizon customers for the last seven years.[4] In another, we have learned that the NSA has gained access to e-mail and other forms of Internet communication—including Skype voice and video communications—via a secret program called Prism.[5] The latter has been portrayed by the director of national intelligence, James Clapper, and others as "acquiring" information only about foreigners. However, Clapper's use of the word "acquire" apparently has a tortured meaning, such that "49-plus percent of the communications [intercepted and stored under the Prism program] might be purely among Americans."[6]

Even before Snowden came forward with evidence of these programs, one could regularly read stories about vast government databases—some that already exist, some that are works in progress,[7] some threatened as part of pending

---

leaked by Snowden. *See* Glenn Greenwald & Spencer Ackerman, *NSA Collected US Email Records in Bulk for More than Two Years Under Obama*, THE GUARDIAN (June 27, 2013), http://www.guardian.co.uk/world/2013/jun/27/nsa-data-mining-authorised-obama/.

[4] Greenwald, *supra* note 3. An amendment that would have stopped the NSA from continuing its bulk collection of telephone metadata was voted down last year by a narrow margin in the House. Siobhan Hughes & Siobhan Gorman, *Move to Curb NSA Surveillance Program Defeated in House*, WALL ST. J. (July 24, 2013, 8:25 PM), http://online.wsj.com/article/SB10001424127887324564704578626410846098192.html. This past spring, headlines announced the end of the bulk metadata collection program, when in fact Obama is asking to continue the program, as is, for at least another three months. After three months, we are told, he may request that Congress pass a law requiring the phone companies to retain the metadata. The only significant change would be the length of time the data would be retained: eighteen months instead of five years. Charlie Savage, *Obama To Call for End to N.S.A.'s Bulk Data Collection*, N.Y. TIMES (Mar. 24, 2014), http://www.nytimes.com/2014/03/25/us/obama-to-seek-nsa-curb-on-call-data.html?_r=0.

[5] Greenwald & MacAskill, *supra* note 3; *see also* Kari Rea, *Glenn Greenwald: Low-Level NSA Analysts Have 'Powerful and Invasive' Search Tool*, ABC NEWS (July 28, 2013, 10:17 AM), http://abcnews.go.com/blogs/politics/2013/07/glenn-greenwald-low-level-nsa-analysts-have-powerful-and-invasive-search-tool/ (describing a search tool, accessible to low-level NSA analysts, that would allow the analyst to "listen to the calls or read the emails of everything that the NSA has stored, or look at the browsing histories or Google search terms that you've entered" based on an email address or an IP address).

[6] Jennifer Stisa Granick & Christopher Jon Sprigman, Op-Ed., *The Criminal N.S.A.*, N.Y. TIMES (June 27, 2013), http://www.nytimes.com/2013/06/28/opinion/the-criminal-nsa.html?pagewanted=all.

[7] *E.g.*, James Bamford, *The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)*, WIRED (Mar. 15, 2012, 7:24 PM), http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/; *see also* Kashmir Hill, *Surprise Visitors Are*

legislation[8]—containing various types of personal information about Americans. Snowden, then, in coming forward with documentary evidence of such programs, has succeeded in attracting more attention to them. Now the question is: Will anything be done about them?

Proponents of the programs at issue have argued that, assuming they: (1) collect, in the absence of probable cause and particularized suspicion, nothing more than metadata; and (2) make it easier for the government to identify and track suspected terrorists, they strike the right "balance" between privacy and security. Some have argued, in addition, that the programs are perfectly legal. According to the "third-party doctrine," there is no "reasonable expectation of privacy" in metadata we share with our phone companies, Internet Service Providers ("ISPs"), and so forth. Additionally, the collection of this metadata is authorized by the Patriot Act[9] or the Foreign Intelligence Surveillance Amendments Act ("FISA Amendments Act").[10]

Others disagree with the above normative and legal conclusions; they argue that metadata is more important than most people realize[11] and, moreover, that the arguments for the programs' legality are flawed.[12] With respect to the latter, one can make a few distinct arguments: First, one can argue that the applicable statutes do not authorize these NSA programs—that is, that these programs go too far.[13] Second, one can argue that the relevant statutes are properly applied, but are themselves illegal—actually, unconstitutional—because they do not come

---

Unwelcome at the NSA's Unfinished Utah Spy Center (Especially When They Take Photos), FORBES (Mar. 4, 2013, 12:21 PM), http://www.forbes.com/sites/kashmirhill/2013/03/04/nsa-utah-data-center-visit/.

[8] *E.g.*, David Kravets, *Biometric Database of All Adult Americans Hidden in Immigration Reform*, WIRED (May, 10, 2013, 6:30 AM), http://www.wired.com/threatlevel/2013/05/immigration-reform-dossiers/.

[9] The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT ACT"), Pub. L. No. 107-56, 115 Stat. 272 (codified as amended at 18 U.S.C. § 2510 (2012)).

[10] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (codified as amended at 50 U.S.C. § 1881c (Supp. II 2008)).

[11] Daniel J. Solove, *5 Myths About Privacy*, WASH. POST, June 16, 2013, at B03.

[12] *See* Granick & Sprigman, *supra* note 6.

[13] *Id.* (arguing that the Patriot Act and the FISA Amendments Act do not authorize the bulk collection of Verizon customers' metadata and PRISM, respectively).

under the third-party doctrine. Third, one can argue that what one believes regarding the relevant statutes' applicability or purported constitutionality is beside the point—the third-party doctrine itself is flawed and should be eliminated.[14] It is this last position that I wish to support in this Article.

In Part I of this Article, I discuss the third-party doctrine, including its history, the types of cases to which it has been applied, and arguments in favor of and against it, with particular focus on Orin Kerr's defense[15] of the doctrine. In Part II, I propose an alternative—and, I think, better—way of dealing with cases typically thought to fall under this doctrine. My proposal, as we will see, rests upon the model for the legal protection of privacy that I have elucidated and defended in prior articles: a model based on our rights to property and contract.[16] Finally, in Part III, I enlist the help of the common law of contract to address an objection to my proposal, in hopes of improving its appeal to the reader.

I. THE THIRD-PARTY DOCTRINE

The third-party doctrine says that the Fourth Amendment[17] is not implicated when (1) you share information with a third party—for example, your bank, your phone company, your ISP, Skype, or Facebook—even for a delimited purpose; and (2) the third party turns around and shares the information with the government.[18] Most believe this is the case because, per the

---

[14] While not explicitly mentioning the third-party doctrine, Professor Randy Barnett seems to be making either the second or third argument in a recent op-ed piece. Randy E. Barnett, Op-Ed., *The NSA's Surveillance Is Unconstitutional*, WALL ST. J., July 12, 2013, at A13.

[15] Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 562 (2009).

[16] *See, e.g.*, Amy L. Peikoff, *Beyond Reductionism: Reconsidering the Right to Privacy*, 3 N.Y.U. J.L. & LIBERTY 1, 5 (2008).

[17] The Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. CONST. amend. IV.

[18] Kerr, *supra* note 15, at 563. "The 'third-party doctrine' is the Fourth Amendment rule that governs collection of evidence from third parties in criminal investigations. The rule is simple: By disclosing to a third party, the subject gives

usual understanding of the doctrine, you no longer have a "reasonable expectation of privacy" in the information you share with a third party. And since "reasonable expectation of privacy" is, with some exceptions, the current legal test for whether government activity amounts to a search under the Fourth Amendment,[19] this means that the government's obtaining information from third parties, and then of aggregating that information in databases upon which it performs inquiries of various kinds, is not a search. Orin Kerr disagrees with this formulation of the doctrine, saying, "[T]he third-party doctrine is better understood as a form of consent rather than as an application of *Katz*."[20] On either understanding of the rationale for the doctrine, statutes such as the Patriot Act[21] or the FISA Amendments Act[22] may authorize the government's broad information gathering and aggregating activities without the requirement of a warrant based on probable cause and particularized suspicion.

How did we get here? The doctrine first arose and was developed in a series of cases called the "secret agent" cases.[23] Think of Tony Soprano divulging information about the operation of his illegal businesses to a government informant, and the informant later turning that information over to the government prosecutor, who uses it to indict and prosecute Soprano. The fact that the Fourth Amendment does not protect the Tony Sopranos of the world in situations like this probably does not bother us. But then the doctrine was extended, starting in the early 1970s, to apply not only to the Tony Sopranos of the world, but also to

---

up all of his Fourth Amendment rights in the information revealed." *Id.* (footnote omitted).

[19] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[20] Kerr, *supra* note 15, at 588.

[21] The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT ACT"), Pub. L. No. 107-56, 115 Stat. 272 (codified as amended at 18 U.S.C. § 2510 (2012)).

[22] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (codified as amended at 50 U.S.C. § 1881c (Supp. II 2008)).

[23] Kerr, *supra* note 15, at 567–68 (discussing the "secret agent" cases that came before the Supreme Court between the years 1952 and 1971).

you and me (I am assuming that none of us is in the mafia) when we share information with third parties in the ordinary course of doing business and living our lives.[24]

Considering the third-party doctrine's disturbing implications, one would think that, by now, it would have been overturned or its application severely limited. While it might take the revelations of a former employee of an NSA contractor to get the general public interested in this issue, that should not be true of those in the legal profession. For his part, Stephen Henderson argues[25] that the Supreme Court has long refused to apply the third-party doctrine "in a strong form"—that is, as a categorical rule like that described at the beginning of this Part, as well as in *United States v. Miller*[26]:

> [T]he 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.[27]

Henderson describes the 2012 case, *United States v. Jones*,[28] as the most recent in a series of "encouraging" cases, cases in which Supreme Court Justices have shown their willingness to reject the "strong", categorical form of the third-party doctrine in favor of "a case-by-case" approach.[29] In *Jones,* the Court unanimously held that attaching a GPS tracking device to a vehicle, and then using the device to track the vehicle's location, is a search for purposes of the Fourth Amendment.[30] In her concurring opinion, Justice Sotomayor calls for the third-party doctrine to be reexamined:

---

[24] *See id.* at 569–70 (discussing "business records" cases heard by the Supreme Court between the years 1973 and 1980).

[25] Stephen E. Henderson, *After* United States v. Jones, *After the Fourth Amendment Third Party Doctrine,* 14 N.C. J.L. & TECH. 431, 432, 436–42 (2013). "[I]n at least five decisions the Supreme Court has shied away from applying a strong third party doctrine." *Id.* at 442; *see also* Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39, 42–43 (2011).

[26] 425 U.S. 435 (1976).

[27] *Id.* at 443.

[28] 132 S. Ct. 945 (2012).

[29] Henderson, *supra* note 25, at 432, 458.

[30] *Jones*, 132 S. Ct. at 949.

> [I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers.[31]

Given Sotomayor's concerns about telephone and Internet metadata that she expresses in this passage, it seems that she might be ready to overturn the third-party doctrine in an appropriate case challenging the invasive NSA programs discussed earlier in this Article.[32] But note that Sotomayor interprets the doctrine as an application of the *Katz* "reasonable-expectation[s]" test.[33] It is therefore likely that Kerr, and those who agree with his consent-based understanding of the doctrine, would be undeterred by Sotomayor's call to reconsider it, and would continue to defend it.

A. Defending the Doctrine: Orin Kerr

Kerr defends the third-party doctrine on two grounds. First, he says:

> Without the doctrine, criminals could use third-party agents to fully enshroud their criminal enterprises in Fourth Amendment protection. A criminal could plot and execute his entire crime from home knowing that the police could not send in undercover agents, record the fact of his phone calls, or watch any aspect of his Internet usage without first obtaining a warrant. He could use third parties to create a bubble of Fourth Amendment protection around the entirety of his criminal activity.[34]

---

[31] *Id.* at 957 (Sotomayor, J., concurring) (citations omitted).

[32] *See supra* notes 4–6 and accompanying text.

[33] *See Jones*, 132 S. Ct. at 954–55.

[34] Kerr, *supra* note 15, at 576.

With no third-party doctrine, Kerr argues, it would be nearly impossible for the police to gain enough evidence to support a search warrant, particularly when a criminal is clever at substituting private, third-party-assisted actions and transactions for those that were once, of necessity, amenable to public viewing.[35] The doctrine, therefore, in Kerr's terms, avoids the "substitution effect" and thereby preserves the "technological neutrality" intended by the Court in *Katz*.[36] "Just as the new technologies can bring 'intimate occurrences of the home' out in the open, so can technological change and the use of third parties take transactions that were out in the open and bring them inside."[37]

If it is right to understand the Fourth Amendment from this perspective of technological neutrality, Kerr argues, then "it must be a two-way street."[38] So, just as the "reasonable expectation of privacy" test of *Katz* addresses the problem of technology exposing intimate details of one's life, the third-party doctrine addresses the problem of criminals substituting private, third-party transactions for actions conducted out in the open. Kerr notes that the doctrine thus provides another type of neutrality, in that a criminal enjoys "roughly the same degree of privacy protection regardless of whether [the] criminal commits crimes on his own or uses third parties."[39]

Kerr's second argument in defense of the third-party doctrine is that it helps to ensure the clarity of Fourth Amendment rules.[40] The need for clarity, says Kerr, comes from the exclusionary rule's evidence-suppression remedy:

> The severe costs of the exclusionary rule require ex ante clarity in the rules for when a reasonable expectation of privacy exists. The police need to know when their conduct triggers Fourth Amendment protection. Uncertainty can both overdeter police from acting when no protection exists and can lead them to inadvertently trample on Fourth Amendment rights.[41]

---

[35] *See id.* at 575–76.
[36] *Id.* at 580–81.
[37] *Id.* at 580.
[38] *Id.*
[39] *Id.* at 577.
[40] *Id.* at 581.
[41] *Id.* at 582.

The third-party doctrine achieves the necessary clarity, says Kerr, by "guarantee[ing] that once information is present in a location it is treated just like everything else located there."[42] So, for example:

> [A] letter that arrives in the mail, is opened, and sits on the recipient's desk at home . . . . [It] is treated just like all the other papers on the desk . . . . [T]he Fourth Amendment rules [that the police] must follow will be set by the usual rules of home searches rather than special rules for each piece of paper defined by the history of each page.[43]

Kerr seems open to considering an alternative to the third-party doctrine, so long as its application is equally clear ex ante and, presumably, it meets his other requirements for neutrality.[44] He seems skeptical, however, as to whether such an alternative exists. He rejects what he sees as the only alternatives to the doctrine; they amount to the very thing that Henderson says he would welcome: "a case-by-case approach."[45]

In addition to arguing directly in defense of the third-party doctrine, Kerr responds to two criticisms against it. The first is what Kerr calls a "doctrinal" criticism: "[T]he [Supreme Court] Justices are wrong when they contend that a person does not retain a reasonable expectation of privacy [when he shares information with a third party]."[46] As mentioned earlier, Kerr rejects the understanding of the third-party doctrine that characterizes it as an application of the *Katz* "reasonable expectation" test.[47] He argues that, while the Supreme Court seemed like it was getting ready to recognize the doctrine as one of consent, the Court went "off course" when deciding "*United States v. White*, the first third-party case to follow *Katz*."[48] There, writes Kerr, Justice White:

> [C]hose the wrong doctrinal prong. Instead of grounding the doctrine in consent principles, he reasoned that use of a secret agent did not violate a reasonable expectation of privacy. The

---

[42] *Id.*

[43] *Id.*

[44] *See id.* at 586 ("If critics want to replace the third-party doctrine with an alternative, they should be clearer about what that alternative would be and how it would apply in the wide range of cases courts regularly confront.").

[45] *See* Henderson, *supra* note 25, at 458.

[46] Kerr, *supra* note 15, at 587.

[47] *See supra* text accompanying note 20.

[48] Kerr, *supra* note 15, at 588–89 (footnote omitted).

> difference between the two is subtle: If government conduct does not violate a reasonable expectation of privacy, it is not a search, whereas if it violates a reasonable expectation of privacy pursuant to consent, it is a search but one that is constitutionally reasonable.[49]

In other words, Kerr argues that the doctrine's critics are right to think that one's expectation of privacy in the information one shares with third parties is reasonable. However, he argues, what is also reasonable is a consented-to search, and this is precisely what you have in the third-party situation.[50]

The second criticism Kerr addresses is something he calls a "functional" criticism. The criticism is straightforward. It says, "[T]he third-party doctrine . . . gives the police too much power."[51] In particular, Kerr notes, the doctrine's critics are concerned with abuses of power of the sort recently attributed to Internal Revenue Service agents.[52] Kerr's response consists of pointing out that "the Fourth Amendment is [not] the only game in town," and describing "a wide range of tools . . . for addressing police harassment of third-party information outside the Fourth Amendment."[53] He divides the tools according to the sorts of cases in which they are utilized. For the "secret agent" cases, there are entrapment laws,[54] the *Massiah* doctrine,[55] the First Amendment,[56] and internal agency regulations.[57] For the business records cases, there are statutory protections,[58] common law privileges,[59] and the rights of third parties.[60]

---

[49] *Id.* at 589 (footnotes omitted).

[50] *Id.* at 589–90.

[51] *Id.* at 590.

[52] *See, e.g.*, Sam Stein, *IRS Investigator: Tea Party Groups Were Scrutinized More than Progressive Organizations*, HUFFINGTON POST (June 27, 2013, 11:52 AM), http://www.huffingtonpost.com/2013/06/27/irs-2012-election_n_3510455.html.

[53] Kerr, *supra* note 15, at 590.

[54] *See id.* at 591–92.

[55] *See id.* at 592–93.

[56] *See id.* at 593–94.

[57] *See id.* at 594–95.

[58] *See id.* at 596–97.

[59] *See id.* at 597–98.

[60] *See id.* at 598–600.

B. *Challenges to Kerr's Defense*

Erin Murphy and Richard Epstein both think that the "negative externalities" of the third-party doctrine outweigh the benefits it provides in ensuring technological neutrality and preventing substitution effects.[61] "Specifically," writes Murphy, "the technologies left exposed by third-party doctrine are not exclusively deployed for illicit purposes."[62] Therefore, she says, "[F]ailing to protect [these technologies] . . . dissuad[es] innocent, desirable conduct."[63] Similarly, Epstein writes that the doctrine "creates social inefficiencies with respect to lawful conduct that people naturally wish to keep from the prying eye of the state."[64] Yes, the third-party doctrine may prevent a would-be thief from hiding evidence of his crime behind his ISP, e-mail server host, online bank, and so forth. But criminal activity is only a small fraction of the activities for which such businesses and technologies are used. So, for every crime that is either prevented or made more detectable because of the doctrine, there is much valuable activity that is discouraged. This is particularly true after Snowden's revelations about the NSA's activities. Online anonymity, which entails enjoying less of what the Internet has to offer, is now the latest in fashion.[65]

Murphy's critique goes farther than does Epstein's; she challenges Kerr's substitution effects insight at a fundamental level. First, she questions whether the average criminal would be capable of acting rationally enough to deliberately substitute, for publicly observable means, third-party-assisted means of achieving his goals.[66] Writes Murphy, "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."[67] She also

---

[61] Erin Murphy, *The Case Against the Case for Third-Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239, 1241 (2009).

[62] *Id.*

[63] *Id.*

[64] Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 BERKELEY TECH. L.J. 1199, 1226 (2009).

[65] *See generally* Stuart Jeffries, *Internet Anonymity is the Height of Chic*, THE GUARDIAN (June 12, 2013), http://www.guardian.co.uk/technology/2013/jun/12/internet-anonymity-chic-google-hidden.

[66] Murphy, *supra* note 61, at 1242.

[67] *Id.* (citing BUREAU OF JUSTICE STATISTICS, U.S. DEP'T OF JUSTICE, FEDERAL JUSTICE STATISTICS, 2007—STATISTICAL TABLES (2010), http://www.bjs.gov/content/

doubts whether there are technological, third-party-assisted alternatives available for the commission of many crimes.[68] Sure, it might be easier to evade detection while stalking someone online instead of stalking them in the physical world; but, as Murphy notes, "One generally cannot murder, rape, or cause serious bodily injury via technology alone."[69] Moreover, she says, even if Kerr wanted to focus his examination on the most frequently committed offenses, he would find little support for his view: "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."[70]

Yes, there are some crimes that seem particularly well suited for "third-party technological outsourcing," as Murphy calls it.[71] With respect to these, however, she suggests that what is at play is not a substitution effect, but rather "a sub-species of crimes in which third-party participation is an indispensable component (or even instrument) of the offense."[72] Any increased difficulty in investigating such crimes in the absence of a third-party doctrine is not, she says, due to substitution of the Internet for other means of committing the crime.[73] Murphy thinks the difficulty comes from the fact that the Internet and digital duplication technology make it possible for there to be many more offenders—for example, producers and consumers of child pornography—whom the police must apprehend.[74]

Murphy also rejects the idea of using the third-party doctrine as a means of "equalizing" offenses that are public with offenses that are private or particularly heinous.[75] She notes that the Constitution "[does] not obliterate privacy protections for the home, for instance, just because the vast majority of child sexual

---

pub/html/fjsst/2007/fjs07st.pdf (title renamed from "Criminal Offender Statistics" by the Bureau of Justice Statistics)).

[68] *Id.* at 1243.

[69] *Id.*

[70] *Id.*

[71] *Id.*

[72] *Id.* Murphy gives "child pornography or internet fraud" as examples. *Id.*

[73] *Id.*

[74] *Id.*

[75] *Id.* at 1244.

abuse occurs there."[76] Most importantly, Murphy challenges Kerr's assertion that, in the types of cases that truly invite technology substitution—"offenses like theft, fraud, or [certain] white collar crimes"[77]—substitution will make it harder for the police to do their job. In fact, Murphy suggests that the difficulty of the police's job will be roughly the same whether or not substitution occurs.[78] "Third parties," she writes, "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."[79] The police may need to get a warrant based on probable cause in order to obtain pieces of evidence in the possession of third parties; however, "that is not a particularly high [] standard to meet."[80] And once the police get their hands on that evidence, she notes, chances are it will turn out to be more valuable, more probative, than, for example, "the testimony of [a stalking] victim that some guy keeps coming around."[81] Finally, Murphy adds that, should there be a particularly thorny case that police need to investigate, there is always "the grand jury, which is virtually immune from Fourth Amendment strictures."[82]

Kerr responds to many of Murphy's criticisms in an essay[83] published alongside hers and Epstein's. First, he says that her observation that most criminals are not rational actors is beside the point.[84] The substitution effect exists so long as criminals in fact replace their publicly observable acts with protected third-party transactions; what their motivation is for doing so is irrelevant.[85] Also beside the point, says Kerr, is the relative prevalence of crimes for which third-party substitution is possible.[86]

> [T]he key question is not whether the third-party doctrine is necessary for the police to investigate every type of crime. The question is whether, on the whole, the rule enables the proper

---

[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] *Id.*
[80] *Id.*
[81] *Id.*
[82] *Id.* (citing United States v. Dionisio, 410 U.S. 1, 11–12 (1973)).
[83] Orin S. Kerr, *Defending the Third-Party Doctrine: A Response to Epstein and Murphy*, 24 BERKELEY TECH. L.J. 1229, 1233–36 (2009).
[84] *Id.* at 1233–34.
[85] *Id.*
[86] *Id.* at 1234.

> balance between privacy and security given the need for rules that encompass investigations into all different types of crimes.[87]

Kerr says his "favorite of Murphy's arguments" is her contention that it is risky for criminals to rely on third parties in the commission of their crimes, because it makes it easier for them to be caught.[88] In his response, Kerr first sets aside the idea of criminals engaging in a rational cost-benefit analysis before deciding whether to use third parties.[89] He then argues that, insofar as the use of third parties leaves a trail of evidence behind, that trail of evidence is virtually inaccessible in the absence of the third-party doctrine: "In a world without the third-party doctrine, the risks of group crimes would be much lower. The now-exposed paper trail presumably would be as protected as secret plans stored in the suspect's sock drawer."[90] Moreover, says Kerr, even if there were some real cost-benefit analysis to be performed, the most controversial applications of the third-party doctrine involve third parties—banks, phone companies, and ISPs—who pose the least risk in terms of becoming snitches.[91] They are companies that, in the normal course of business, engage in minimal customer monitoring and have a market incentive to preserve customer privacy.[92]

I found Kerr's response to Murphy to be unconvincing with respect to a few issues. First, I agree with Murphy that police investigation of crimes involving third parties, in the absence of the third-party doctrine, would not be as difficult as Kerr suggests. To commit a crime means, concretely, to initiate force or use fraud against another person or his property. No matter what means one employs to do this, there will be some trail of evidence left behind, a trail that can be followed and used to apprehend the criminal. Yes, in the absence of the third-party doctrine a warrant may be required to figure out, for example, who uses the Internet Protocol address linked to an online theft from a bank account. However, as Murphy says, that should not be too difficult to get.

---

[87] *Id.*
[88] *Id.*
[89] *See id.* at 1234–35.
[90] *Id.* at 1235.
[91] *See id.*
[92] *Id.*

The second point to make is that Kerr, in his response to Murphy, seems to assume that the government plays no role in the decisions companies make about monitoring their customers or preserving their privacy. As we have learned recently, Verizon has for years been subjected to court orders demanding continuous collection and reporting of customers' metadata, regardless of Verizon's own business needs or preferences for preserving customer privacy.[93] Finally, Kerr fails to respond to an important point Murphy raises about the Constitution: There are some things the Constitution will protect—for example, the home—even though removing that protection might yield a bonanza in terms of facilitating investigation of particularly heinous crimes.[94]

Overall, Murphy provides a formidable challenge to Kerr's arguments about the third-party doctrine's role in preventing substitution and preserving the technological neutrality of the Fourth Amendment. Kerr is concerned that eliminating the third-party doctrine would encourage substitution of third-party-assisted means of committing criminal offenses, and that this would help criminals to avoid detection of their crimes. Murphy makes us doubt both the incidence of substitution and the gravity of its consequences.

Aside from his observation that the social inefficiencies created by the third-party doctrine may outweigh the substitution effects about which Kerr is concerned,[95] Epstein's critique is implicit in the alternative model he presents in his article. Epstein suggests that the Fourth Amendment might be more flexible in its treatment of third-party cases, allowing courts to ratify not only searches based on probable cause, but also, in the appropriate case, searches based only on reasonable suspicion.[96] In Kerr's response, he notes that Epstein, "[b]y assuming away the all-or-nothing framework [of the Fourth Amendment], . . . dramatically changes the costs and benefits of the third-party doctrine."[97] In essence, Epstein's argument against the substitution effect is to propose a legal framework,

---

[93] *See* Greenwald, *supra* note 3.

[94] *See supra* text accompanying note 76.

[95] *See supra* text accompanying note 64.

[96] Epstein, *supra* note 64, at 1224–25.

[97] Kerr, *supra* note 83, at 1232.

based on different assumptions, in which the substitution effect does not exist. Accordingly, Kerr finds that Epstein "ends up answering a very different set of questions."[98]

Suppose that Kerr is correct, that the substitution effect would be significant and that eliminating the third-party doctrine would adversely affect the technological neutrality of the Fourth Amendment. In that case, one approach would be to balance, as Epstein and Murphy do, the substitution effects against the negative externalities of the third-party doctrine, and decide what to do accordingly. Another approach—one I believe to be preferable—is to treat the question as one of individual rights in the traditional sense, where rights are not "interests" to be balanced against "the public good," or as part of some elaborate utilitarian calculus. On this approach, the only questions to ask would be: What are the rights at issue, and what does it mean for the government to protect these rights in the context of a criminal investigation? Yes, we delegate our right of self-defense to the government, and that entails the government sometimes being able to investigate whether or not the target of the investigation has consented.[99] Nonetheless, delegating one's right of self-defense does not mean that the government can investigate whomever it wants, whenever and however it wants. The government must have some objective reason, typically probable cause, to believe a particular person or group of persons is involved in criminal activity. While a full defense of this overall approach is beyond the scope of this Article, the alternative to the third-party doctrine presented in Part II of this paper will help to further elucidate it and thereby, I hope, contribute to its plausibility in the mind of the reader.

With respect to Kerr's argument about the need for ex ante clarity, again we see Murphy and Epstein concurring in their initial response. If clarity is what you are after, why not opt for what Murphy calls the "libertarian baseline?": "[A] very clear

---

[98] *Id.* Kerr also objects to the fact that Epstein's model "eliminates the institutional choice between constitutional regulation and either statutory or administrative regulation." *Id.* What is, on Kerr's understanding of the Fourth Amendment, the province of either statutory or administrative law becomes, for Epstein, the province of "a flexible Fourth Amendment." *Id.* at 1232–33.

[99] In other words, I join Epstein in rejecting the "libertarian baseline" he mentions in his piece. Epstein, *supra* note 64, at 1211 (describing a "libertarian baseline" which "makes all forms of criminal investigation illegal without the consent of the parties who are investigated").

rule (and one with ample constitutional support) that simply prohibits all third-party investigation without a warrant or probable cause."[100] Murphy then goes further and assumes, for the sake of argument, that ex ante clarity would require eliminating rather than fortifying third-party protections, and tackles a hypothetical Kerr posits in his paper: An anonymous blog commenter writes about a Senator taking a bribe.[101] The problem for police, who would like to subpoena the commenter, is to determine the commenter's relationship to the Senator. Without a categorical third-party doctrine, the relationship between the two is crucial for determining the police's ability to subpoena the commenter.

As with Kerr's concerns about substitution and technological neutrality, Murphy argues that Kerr's concerns here are overblown. A grand jury, she notes, could easily subpoena the ISP for the name of the commenter.[102] A police officer may not be able to do so, but for Murphy, the trade-off is worth it: "Sure, we want to catch . . . 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 [an internet] connection."[103] Once the government knows the name of the commenter, Murphy explains, it can either easily question the commenter in the context of a grand jury investigation; or, in the case of a police investigation, the police can ask about the commenter's relationship to the Senator at the outset of the interview, and either stop or continue the conversation depending upon the answer received.[104]

In Kerr's response, he explains that his hypothetical about the bribe-taking Senator was meant to illustrate a possible alternative to the third-party doctrine: a legal regime "in which the question of whether an expectation of privacy is 'reasonable' must be answered by a probabilistic determination in each case of whether there was a person who once had the information who

---

[100] Murphy, *supra* note 61, at 1245. Note that what Epstein calls the "libertarian baseline" seems to be quite a different animal. *See supra* note 99. Murphy's libertarian seems to believe in limited government, whereas Epstein's libertarian seems to be somewhat of an anarchist.

[101] Murphy, *supra* note 61, at 1245.

[102] *Id.* at 1245–46.

[103] *Id.* at 1246.

[104] *Id.*

reasonably expected privacy."[105] Murphy, in answering the hypothetical, was, so far as I can tell, imagining a world just like ours except that there is no third-party doctrine, and showing that ex ante clarity can be achieved in that world. In other words, she is analyzing Kerr's hypothetical in the world of her "libertarian baseline."[106] Kerr seems to be distracted by the repurposing of his hypothetical, and so he fails to respond to Murphy here. Instead, he decides to point to the fact that Murphy offers only "a few vague proposals" for an alternative to the third-party doctrine as evidence that it is difficult to do so while effectively addressing Kerr's concerns about ex ante clarity.[107] Still, repurposed as it was, I found Murphy's treatment of Kerr's hypothetical convincing with respect to the issue of ex ante clarity. I admit I may be biased, however, because, as we will see, the approach I suggest and defend in this Article is not far from Murphy's libertarian baseline.

Epstein does not take the ex ante clarity issue head-on, but rather proposes an alternative analysis in which he believes the issue of clarity has been adequately addressed. "The boundary lines between these various areas [to which Epstein applies his framework] are for the most part relatively clear, so that the borderline interpretation issues should not muddy the overall inquiry."[108] Kerr does not discuss the issue of clarity in his response to Epstein, but I believe that he would reject Epstein's framework on this ground as well. What Epstein is proposing is, in essence, a case-by-case inquiry into the social utility of protecting privacy.

Taking up Kerr's treatment of the "doctrinal" critique of the third-party doctrine in his own article, Epstein rejects Kerr's consent-based understanding of the doctrine. Just as it begs the question to say that one who shares information with a third party "assumes the risk" of disclosure, Epstein explains, a similar objection can be made to the claim that one "consents" to the disclosure of information by sharing it with a third party.[109] Epstein describes what is going on in a case covered by the third-

---

[105] Kerr, *supra* note 83, at 1236.
[106] *See* Murphy, *supra* note 61, at 1245–46.
[107] Kerr, *supra* note 83, at 1236.
[108] Epstein, *supra* note 64, at 1202.
[109] *Id.* at 1201.

party doctrine as tantamount to "fraud in the inducement."[110] He notes that the common law will not hold one who gave his consent accountable as against the party who committed a fraud in order to induce that consent.[111] "In Fourth Amendment cases," writes Epstein, "this party is the government, so we are back at square one."[112] For my part, I wonder whether Epstein's observation is true in all Fourth Amendment cases, or just in the "secret agent" cases, but I agree with Epstein that it is question-begging to say that a person consents to have his information shared with a third party, the government, simply because he shared it with a second party for a limited purpose. Epstein writes:

> To be sure, there are many cases where the consent of the party searched meets the standard of individualized consent developed in private law settings. But in other cases the nominal consent is presumed on the ground that on balance people are better off from the ex ante perspective if they are forced to submit to some searches against their will.[113]

In other words, "consent" is often just a proxy for social utility. Murphy agrees with Epstein in his critique of Kerr's consent-based analysis of the doctrine. "I . . . share Professor Epstein's sense that Professor Kerr's 'consent' model seems to just circle back to the reasonable expectation of privacy test."[114] She also agrees with Epstein that a viable alternative to the doctrine might be "geared toward optimizing social utility."[115] I agree with Epstein and Murphy about the essential identity of "consent" and "reasonable expectations" understandings of the doctrine, as well as with their sense that, whichever of these two concepts you use to explicate the doctrine, the doctrine is unworkable. However, as we will see, I would not frame the alternative in terms of maximizing social utility.

In his response to Epstein's article, Kerr observes that Epstein, after drawing upon "insights from libertarian political theory, the common law of torts, and Fifth Amendment takings law, . . . concludes that the question of 'reasonable expectations'

---

[110] *Id.*
[111] *Id.*
[112] *Id.* at 1202.
[113] *Id.* at 1206.
[114] Murphy, *supra* note 61, at 1241 n.6.
[115] *Id.*

requires a cost-benefit analysis."[116] Kerr doubts, however, whether Epstein's "first-principles rethinking" of the third-party situation actually adds anything to existing doctrine, and offers examples from existing case law and statute in which the cases are treated essentially the same as what Epstein envisions.[117]

Kerr's discussion of the functional critique of the third-party doctrine warrants some attention as well. Recall that Kerr's response to this critique, which says that the doctrine gives the government too much power, is to note that "the Fourth Amendment is [not] the only game in town," and to discuss the supplemental privacy protections afforded by statutory and administrative law, as well as common law rules and evidentiary privileges.[118] Murphy's answer to Kerr here is brief. She emphasizes the fact that these alternatives are "non-constitutional"—that is, that they do not provide the same protection afforded by the Fourth Amendment—and says she does not think they are "anywhere near adequate."[119]

I will defer to Murphy with respect to her evaluation of the adequacy of criminal procedure doctrine. With respect to statutory protection for access to business records, note that what a statute giveth, a statute may taketh away: The invasive activities of the NSA described in the introduction to this Article were apparently authorized by statute, despite the statutory protections relied upon by Kerr. More importantly, and likely also relevant to the legality of the NSA's activities, Kerr admits that "[i]n many . . . cases, the statutory privacy laws provide less protection than would the analogous Fourth Amendment standard of a probable cause warrant."[120] As for the privileges, even if Murphy were wrong in saying that they "are barely worth the paper they are printed on,"[121] I fail to see how they are

---

[116] Kerr, *supra* note 83, at 1230.

[117] *Id.* at 1231–32. I might quibble a bit with Kerr's conclusion here. Kerr offers the following quotation from *Hudson v. Palmer* as a sample of a court conducting a cost-benefit analysis: "[R]ecognition of privacy rights for prisoners in their individual cells simply cannot be reconciled with the concept of incarceration and the needs and objectives of penal institutions." *Id.* at 1231 (quoting Hudson v. Palmer, 468 U.S. 517, 526 (1984)). Insofar as the Court discusses the "*concept* of incarceration," and perhaps even the "*objectives* of penal institutions," it seems to be going beyond simple cost-benefit analysis. *See id.* (emphasis added).

[118] *See supra* text accompanying notes 53–60.

[119] Murphy, *supra* note 61, at 1250–51.

[120] Kerr, *supra* note 15, at 597.

[121] Murphy, *supra* note 61, at 1251.

relevant to a situation involving me and my cell phone company, or me and my ISP, or me and Facebook. Finally, it is true that third parties may often assert the rights of their customers and, as Kerr notes, "Protecting customer privacy is good for business."[122] However, with respect to the aforementioned NSA programs, third parties have had to conduct these challenges entirely in secret and then, when ultimately compelled to turn over their customers' data, they have been forced to deny any knowledge of or participation in the programs.[123] Further, Murphy points out that, even in cases in which the companies have the opportunity to fight subpoenas publicly, few are willing to stand up to the government—and those few are relegated to using legal doctrines that seem inapposite.[124]

Drawing upon critiques by Murphy and Epstein, and throwing in a few of my own, I hope I have poked enough holes in Kerr's defense of the third-party doctrine to have further motivated the search for an alternative. It is to that alternative that we now turn.

II. AN ALTERNATIVE PROPOSAL

A. *A Model for Legal Protection of Information Privacy Based on Our Rights to Property and Contract*

My proposal rests on a free-market model for the protection of informational privacy that I have been elucidating and defending for several years.[125] What I have suggested is that we return to the era of protecting privacy on the basis of our rights to property and contract, as was the case before a famous 1890 law review article[126] written by Samuel D. Warren and Louis D. Brandeis. In other words, I reject the so-called right to privacy. My argument starts with the same observation as that of those

---

[122] Kerr, *supra* note 15, at 598.

[123] *See* Dominic Rushe, *Google and Facebook Ask DoJ for Permission To Publish Fisa Requests*, THE GUARDIAN (June 11, 2013), http://www.theguardian.com/technology/2013/jun/11/google-doj-permission-publish-fisa-requests; Dominic Rushe, *Yahoo Wants Fisa Objections Revealed*, THE GUARDIAN (July 10, 2013), http://www.theguardian.com/technology/2013/jul/11/yahoo-wants-fisa-objections-revealed.

[124] Murphy, *supra* note 61, at 1251 (discussing Google's challenge to a government subpoena for its customers' information, in which Google appealed to trade secret doctrine).

[125] *See generally* Peikoff, *supra* note 16.

[126] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 213 (1890).

who, in the literature, are known as "reductionists." Reductionists note that cases in which most of us believe an individual's privacy should be legally protected can be reduced to cases in which the individual is exercising property and contract rights in order to protect his privacy.[127] You do not want someone to see or hear what you are doing in your home? Lock your doors, close your windows, and shut your blinds. You want to keep your financial information private? Well, before the government started compelling the bulk collection and reporting of financial data[128]—something for which we have the third-party doctrine to thank—you could protect your financial privacy simply by having a confidentiality clause in your contract with your bank.

Yes, there are tricky cases involving new technologies in which it can be difficult to see how our rights to property and contract can do the job. I think in many cases, however, courts have given up too easily. Take, for example, *Olmstead v. United States*.[129] There, the government tapped a phone line to listen to Olmstead's phone conversations.[130] The Supreme Court, ostensibly relying on the trespass doctrine, held that the government's conduct did not amount to a search within the meaning of the Fourth Amendment.[131] "The amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants."[132]

I think the Court failed properly to apply the trespass doctrine in that case. There may not have been a physical trespass to "the houses or offices of the defendants," but there was a physical trespass to the phone company's phone lines, just as there was a trespass to the vehicle of Jones's wife in *United*

---

[127] *See generally* Amy L. Peikoff, *The Right to Privacy: Contemporary Reductionists and Their Critics*, 13 VA. J. SOC. POL'Y & L. 474, 474 (2006).

[128] *See, e.g.*, Bank Secrecy Act, 12 U.S.C. § 1829b (2012).

[129] 277 U.S. 438 (1928).

[130] *Id.* at 456–57.

[131] *Id.* at 465.

[132] *Id.* at 464.

States v. Jones.[133] The phone lines may not have belonged to the defendants, but the defendants had purchased exclusive access to them during the time of their calls.[134]

I believe that not only is a distinct "right to privacy" superfluous—as do the reductionists—it is also immoral, in that it tends to displace and thereby undermine our fundamental rights to property and contract.[135] Further, because it is our rights to property and contract that enable us to achieve states of privacy, the consequence of recognizing a distinct right to privacy is, in fact, *less* privacy protection. The recent revelations about intrusive NSA programs are just the latest examples. In an earlier article, after reviewing the 1970s business records cases, I wrote:

> If the controlling standard in these cases had been one's right to property, along with one's right to use his property to enter into contracts, then a man's privacy would not be dependent on others' opinions about what he actually expects and whether his expectations are reasonable. Rather, it would depend solely on his ability to produce values and to trade those values for the means to protect the privacy he seeks. Of course, the government could still issue warrants to compel third parties to disclose information that has been entrusted to them. But at least then the disclosure of information would depend on factors such as particularized suspicion and limited scope of search . . . .[136]

B. Applying the Model to the Third-Party Situation

Applying the above model to the third-party situation would be straightforward: An individual has a contract with a third party—a bank, a phone company, or an ISP. The contract contains a provision, preferably explicit, according to which the third party promises, as part of the consideration for the customer's money and patronage, to keep his information private. If the third party reveals a customer's private information, it has breached the contract and could be compelled to pay damages accordingly. Moreover, the government, in order to compel the third party to breach its contract with you, would need to get a

---

[133] 132 S. Ct. 945, 949, 952 (2012).

[134] One who rents an apartment to live in does not own that apartment, but it is still treated as one's home for Fourth Amendment purposes.

[135] *See* Peikoff, *supra* note 16, at 34–46.

[136] *Id.* at 40.

search warrant or the equivalent, based upon probable cause and particularized suspicion. If it failed to do so, the modern remedy would likely be the exclusionary rule, but I would prefer to return to the traditional trespass model of the Fourth Amendment,[137] under which we might charge the government with tortious interference with contract.

Suppose, for example, the police found, on a publicly available Internet discussion forum, a post by a person who says he wants to blow up participants and spectators at the Boston Marathon. If the police discovered this early enough, such that the threatened attack was not imminent, then they could go to a judge, present the evidence they have amounting to probable cause and pointing to a particular individual or group of individuals, and get a warrant. The warrant would compel the forum host to reveal the Internet Protocol address of the post's author, which could then lead the police to the real person, who could then be investigated as appropriate. If a threat were imminent, criminal procedure would allow for an exception to the warrant requirement;[138] this would be no less true in cyberspace than it is in physical space. What would be gone, on my model, are the days of government, for example, compelling banks to compile and hand over data about all transactions in excess of $5,000, regardless of who engaged in them, and then combining that data with data produced by another "third party"—for example, Facebook—and then running searches on the combined database with no warrant, no probable cause, and no particularized suspicion.

C. *Evaluating the Model*

How might the scholars discussed in Part I of this Article evaluate my suggested model for approaching privacy and, in particular, the third-party cases? While Murphy might agree with my view that the third-party doctrine should be thrown out entirely, she might not approve of my model, based as it is in rights to property and contract. Murphy asks, "Is there any principled basis for allowing [an individual] to voluntarily

---

[137] *See, e.g.*, Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 774 (1994) (explaining that, traditionally, police who conducted an unreasonable search without a warrant could be sued and forced to pay damages in trespass).

[138] *See* Warden v. Hayden, 387 U.S. 294, 298–99 (1967).

provide information or give up documents to investigators . . . while forbidding the same voluntary compliance from third parties? Even if such a basis existed, could it be articulated and enforced?"[139]

I would love to say that the common law of contract is exactly what Murphy is seeking here. However, her half-hearted and self-refuted defense of the third-party doctrine as a socioeconomic equalizer,[140] combined with her worry that relying on legislation to protect our privacy would leave "the poor and disempowered . . . unprotected,"[141] leads me to conclude that Murphy is probably not in favor of returning to a legal system in which our rights to property and contract are strictly enforced.

Epstein might agree with much that my model has to offer, but there would likely be many cases where we would be at odds, due to his embrace of the reasonable expectations test as a proxy for deciding these cases based on social utility. Epstein's "central approach is to use the language of reasonable expectations as a way to forge a sensible set of rules that optimizes social welfare with respect to a given kind of problem."[142] Not only does Epstein rely on a foundation, utilitarianism, which contradicts my entire approach, he also ends up proposing a framework that, although it is different institutionally, yields results similar to what we see today.[143]

I would hope that Kerr would give me plenty of points for ex ante clarity. However, I am fairly sure that he would reject my model as sacrificing too much security for the sake of privacy. He

---

[139] Murphy, *supra* note 61, at 1252.

[140] *Id.* at 1247–48. Murphy suggests that one might argue that the third-party doctrine makes it harder to conceal white-collar crimes, which are presumably committed by upper-class, rich criminals. In this way, she says, the doctrine can be seen as leveling the playing field between rich criminals and poor criminals. *Id.* at 1247. Now, one might wonder why anyone cares to level the playing field between rich and poor *criminals* anyway, but this is not why Murphy rejects this argument. She ends up dismissing it because she doubts the connection between the third-party doctrine and white-collar crime. *Id.* Also, she notes, the rich would-be criminals can spend their money lobbying for Congress to create statutory protection for information we share with third parties, something that would undo whatever equalizing effect the doctrine may have had. *Id.* at 1247–48.

[141] *Id.* at 1253.

[142] Epstein, *supra* note 64, at 1202.

[143] Kerr, *supra* note 83, at 1232–33 (noting that the biggest difference between Kerr and Epstein is that Epstein rejects the "all-or-nothing options of Fourth Amendment law," and "eliminates the institutional choice"); *see also supra* notes 116–17 and accompanying text.

would remind me of the substitution effects made possible by eliminating the third-party doctrine, of how much more difficult I have made it for police to investigate crimes facilitated by third parties. My essential answer to Kerr is that I do not believe it is right to "balance" privacy and security.[144] I think the proper goal is to determine what rights exist, and then to figure out what it means to recognize and protect these rights in the context of law enforcement. If recognizing and protecting individual rights makes the job of law enforcement more difficult, so be it. Still, I do think there is an elaboration on this basic model that will, to some extent, address Kerr's concerns. That is the topic of Part III.

III. ADDRESSING AN OBJECTION: ILLEGAL CONTRACTS

I have not yet explained how I propose to treat Tony Soprano's basement conversations with government informants, and yet it is precisely this type of "secret agent" case that made the third-party doctrine seem plausible in the first place. If there is a way to have the benefit of third-party protections for the majority of us, who do not engage in illegal behavior, while chipping away at some of the "substitution effect" that Kerr warns us about with respect to criminal activity,[145] would that not be ideal? Thankfully, the common law of contracts provides a rule that allows us to address these "secret agent" cases, the cases that gave rise to the third-party doctrine, consistent with my model for the legal protection of privacy.

At common law, illegal contracts are not enforceable.[146] An illegal contract is one whose subject matter—the thing to be done pursuant to the contract, the consideration provided for at least one of the parties' promises—is illegal. Specifically:

> [I]t may be broadly said that a bargain will be declared illegal or unenforceable if:
> 1. The consideration for a promise in it is an illegal act or forbearance;

---

[144] Note that the philosophical foundation for my model of privacy is Ayn Rand's theory of rights and that, according to Rand, rights do not conflict and are not subject to "balancing." *See generally* Peikoff, *supra* note 16 (explaining Rand's theory of rights and its application to the problem of the legal protection of privacy).

[145] *See supra* text accompanying notes 34–39.

[146] *See* 5 SAMUEL WILLISTON & RICHARD A. LORD, A TREATISE ON THE LAW OF CONTRACTS § 12:1 (4th ed. 2009).

2. It is illegal to make some promise in the bargain, even though what is promised might be legally performed;
3. Some performance promised is illegal;
4. A provision is included for a condition in violation of law; or
5. According to the modern view, embodied in the Restatement Second, "the interest in enforcement [of a promise or term] is clearly outweighed in the circumstances by a public policy against the enforcement of such terms," in which case the term will be unenforceable.[147]

The defense is not just a relic taught in law schools and tested on bar exams: One scholar methodically examined all of the federal and state court cases in which any defense falling into the broader category of "public policy" was employed during the latter half of 2009.[148] His analysis showed that defenses based on a violation of a statute or regulation—among these would be those based on illegal contracts—had the highest success rate: fifty-nine percent.[149] Accordingly, David Adam Friedman described the illegality defense as the least "unruly" of the public policy defenses.[150]

In one of the cases he surveyed, the South Dakota Supreme Court refused to enforce a promissory note in excess of $30,000, a substantial portion of which was still due and payable, because a small fraction of the note's total amount, $1,500, was in consideration of a gambling debt.[151] If such cases are representative, it is reasonable to conclude that a court presented with an illegal contract would deny enforcement of any explicit or implicit provision promising to keep private any information shared pursuant to the contract. Tony Soprano's revelations to a

---

[147] *Id.* (footnotes omitted). Note that today there is some overlap, acknowledged in Williston's treatise, between the traditional contract defense of illegality and the modern defense of a contract being against "public policy." My proposal in this Article relies only on the former, as a way to account for the "secret agent" cases in the context of my model for the legal protection of privacy. However, it seems that those who prefer the more pragmatic "reasonable expectation of privacy" standard could employ the "public policy" portion of this defense as an explanatory gloss for the "reasonableness" of one's expectation of privacy.

[148] David Adam Friedman, *Bringing Order to Contracts Against Public Policy*, 39 FLA. ST. U. L. REV. 563, 577 (2012).

[149] *Id.* at 581.

[150] *Id.* at 566–67. The broad category of public policy defenses was famously described by Judge Burrough as a "very unruly horse." *Id.* at 564 (quoting Richardson v. Mellish, (1824) 130 Eng. Rep. 294, 303; 2 Bing 229, 251–52 (Burrough, J.)).

[151] *Id.* at 594–95 (citing Neve v. Davis, 775 N.W.2d 80, 81–82 (S.D. 2009)).

secret agent could therefore be shared with the government and used to prosecute Soprano without a warrant or probable cause. No third-party doctrine is required.

CONCLUSION: BEYOND THE THIRD-PARTY DOCTRINE

In this Article, I suggest how the third-party doctrine might be abandoned while preserving the government's ability to use undercover informants and secret agents. I believe I have shown that the choice we have been given thus far—invasive government programs and security on the one hand versus privacy and vulnerability on the other—is a false alternative. I hope I have also offered further demonstration of the power of a model of legal protection for privacy based on the rights to property and contract.

Getting rid of the third-party doctrine is necessary, not because one has a "reasonable expectation of privacy" in information shared with a third party, but rather because the third-party doctrine fails to recognize and protect our rights to property and contract within the context of government law enforcement activity. In fact, as I have argued elsewhere,[152] the reasonable expectation standard of *Katz* is itself flawed and should be eliminated. I do not think it is enough to carve out enclaves for the traditional trespass doctrine, as Justice Scalia has done in recent cases.[153] Two-tier legal protection for privacy, as Justice Scalia explicitly suggests in *Jones*,[154] might be an acceptable waystation, while the courts figure out how properly to apply property and contract doctrines to cases involving the Internet and other technologies. But the final goal should be to recognize that property and contract are the foundations of privacy, and that Warren and Brandeis were wrong.[155]

---

[152] Amy L. Peikoff, *Pragmatism and Privacy*, 5 N.Y.U. J.L. & LIBERTY 638, 658–61 (analyzing and critiquing the *Katz* "reasonable expectation of privacy" test).

[153] *Id.* at 665–69 (explaining why Justice Scalia's approach in Kyllo v. United States, 533 U.S. 27 (2001), is not, despite appearances, a fundamental departure from *Katz*).

[154] United States v. Jones, 132 S. Ct. 945, 953 (2012) ("[U]nlike the concurrence, which would make *Katz* the *exclusive* test, we do not make trespass the exclusive test. Situations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis.").

[155] This goal may not be that unrealistic: Stephen Henderson, for example, asks "whether *Jones* might be a first step in the Court jettisoning the reasonable expectation of privacy criterion." Henderson, *supra* note 25, at 451.

I am hopeful that today's widespread concern about government databases and invasive NSA programs can be used to motivate courts and legislators to reconsider the third-party doctrine and, ultimately, the whole model for the legal protection of privacy.