BUYING YOU: THE GOVERNMENT'S USE OF FOURTH-PARTIES TO LAUNDER DATA ABOUT "THE PEOPLE"

Joshua L. Simmons*

Your information is for sale, and the government is buying it at alarming rates. The CIA, FBI, Justice Department, Defense Department, and other government agencies are at this very moment turning to a group of companies to provide them information that these companies can gather without the restrictions that bind government intelligence agencies. The information is gathered from sources that few would believe the government could gain unfettered access to, but which, under current Fourth Amendment doctrine and statutory protections, are completely accessible.

Fourth-parties, such as ChoicePoint or LexisNexis, are private companies that aggregate data for the government, and they comprise the private security-industrial complex that arose after the attacks of September 11, 2001. They are in the business of acquiring information, not from the information's originator (the first-party), nor from the information's anticipated recipient (the second-party), but from the unavoidable digital intermediaries that transmit and store the information (third-parties). These fourth-party companies act with impunity as they gather information that the government wants but would be unable to collect on its own due to Fourth Amendment or statutory prohibitions. This paper argues that when fourth-parties disclose to law enforcement information generated as a result of searches that would be violations had the government conducted the

---

* J.D. Candidate 2010, Columbia University School of Law; B.A. Politics 2006, Brandeis University. The author thanks Judge Debra Ann Livingston and Professor Harold S. H. Edgar for their invaluable advice, guidance, and feedback in the preparation of this piece. The author also gratefully acknowledges Michael Willes, David Zylberberg, and the Columbia Business Law Review staff for their excellent editing assistance.

searches itself, those fourth-parties' actions should be considered searches by agents of the government, and the data should retain privacy protections.

I. INTRODUCTION

Your information is for sale, and the government is buying it at alarming rates. The CIA, FBI, Justice Department, Defense Department, and other government agencies are, at this very moment, turning to a group of companies to provide them with information that these

companies can gather without the restrictions that bind government intelligence agencies. The information is gathered from sources that few would believe the government could gain unfettered access to, but which, under current Fourth Amendment doctrine and statutory protections, are completely accessible:

> With as little as a first name or a partial address, you can obtain a comprehensive personal profile in minutes. The profile includes personal identifying information (name, alias name, date of birth, social security number), all known addresses, drivers license information, vehicle information . . . telephone numbers, corporations, business affiliations, aircraft, boats, assets, professional licenses, concealed weapons permits, liens, judgments, lawsuits, marriages, worker compensation claims, etc.[1]

For years now, the private companies whose websites consumers employ everyday—such as Amazon,[2] Google,[3] and

---

[1] United States Marshals Service, *Sole Source Justification for Autotrack (Database Technologies)* (obtained by the Electronic Privacy Information Center from the United States Marshals Service), *available at* http://epic.org/privacy/choicepoint/cpusms7.30.02j.pdf (last visited Dec. 3, 2009). Just one of the companies that ferret out this information and provide it to the government maintains petabytes of information, which may contain names, ages, birthdays, genders, addresses, and telephone numbers; records of marital status, families, and children's names, genders, ages, and school grades; estimated incomes, home values and size, and the make and price of cars; details of individuals' occupations, net worth, religions, and ethnicities; and what people read, order, and even where they go on vacation. ROBERT O'HARROW, JR., NO PLACE TO HIDE 36–37, 49–50 (Free Press 2006) (2005). One state law enforcement officer once remarked, "I can call up everything about you, your pictures and pictures of your neighbors." *Id.* at 101. In addition, similar companies have turned targeted mailing lists into additional points of information; for example, one company maintains over 100 lists, including "Affluent Hispanics," "Big Spending Vitamin Shoppers," and "Status Spenders." DANIEL SOLOVE, THE DIGITAL PERSON 22 (N.Y. Univ. Press 2004).

[2] Founded in 1994 by Jeff Bezos and located in Seattle, Washington, Amazon seeks to be "earth's most customer centric company; to build a

Facebook[4]—have had the ability to store information about those consumers and use it for purposes their customers would hardly anticipate.[5] In an attempt to construe the

---

place where people can come to find and discover anything they might want to buy online." Amazon.com Investor Relations FAQ, http://phx.corporate-ir.net/phoenix.zhtml?c=97664&p=irol-faq#6986 (last visited Dec. 3, 2009).

[3] Founded in 1998 by Larry Page and Sergey Brin, and now located in Mountain View, California, Google sees its mission as "organiz[ing] the world's information and mak[ing] it universally accessible and useful." Google Corporate Information – Quick Profile, http://www.google.com/intl/en/corporate/facts.html (last visited Dec. 3, 2009).

[4] Founded in 2004 by students at Harvard University, Facebook's stated mission is to "give people the power to share and make the world more open and connected." Facebook Info, http://www.facebook.com/facebook?v=info (last visited Dec. 3, 2009).

[5] For example, by working with social networking sites like Facebook, law enforcement has the ability to track not only identified persons of interest, but anyone in their online social network. *See* John Markoff, *You're Leaving a Digital Trail. What About Privacy?*, N.Y. TIMES, Nov. 29, 2008, at BU1, *available at* http://www.nytimes.com/2008/11/30/business/30privacy.html; *see also*, Carolyn Y. Johnson, *Project 'Gaydar'*, BOSTON GLOBE, Sept. 20, 2009, http://www.boston.com/bostonglobe/ideas/articles/2009/09/20/project_gaydar_an_mit_experiment_raises_new_questions_about_online_privacy/ (describing a project at MIT that claims to be able to determine if someone is homosexual by looking at their Facebook social network). In addition, companies like Sense Networks are using collected data to create algorithms for measuring a variety of user behaviors. *Id.*; *see* Louise Story, *To Aim Ads, Web Is Keeping Closer Eye on You*, N.Y. TIMES, Mar. 10, 2008 ("The web companies are . . . taking the trail of crumbs people leave behind as they move around the Internet, and then analyzing them to anticipate people's next steps.").

In a recent study, researchers found that, "[c]ontrary to what many marketers claim, most adult Americans (66%) do not want marketers to tailor advertisements to their interests." Joseph Turow et al., *Americans Reject Tailored Advertising and Three Activities That Enable It* (2009), *available at* http://ssrn.com/abstract=1478214; *see also* Stephanie Clifford, *Two-Thirds of Americans Object to Online Tracking*, N.Y. TIMES, Sept. 30, 2009. The researchers asked survey respondents whether existing laws provide a "reasonable level of protection for consumer privacy today." Of those who wanted advertising on websites tailored to them, 61% said there was reasonable protection; of those who did not want advertisement tailoring, 39% responded that there was reasonable protection. Turow, *supra* at 22.

Fourth Amendment, the Supreme Court has allowed these companies to use that information for practically any use they can make of it.[6] One such use is the handing over of potentially damaging information to "fourth-parties."

Fourth-parties, such as ChoicePoint or LexisNexis, are private companies that aggregate data for the government, and they comprise the private security-industrial complex that arose after the attacks of September 11, 2001.[7] They are in the business of acquiring information, not from the information's originator (first-party), nor from the information's anticipated recipient (second-party), but from the unavoidable digital intermediaries that transmit and store the information (third-parties). These fourth-party companies act with impunity as they gather information that the government wants but would be unable to collect on its own due to Fourth Amendment or statutory prohibitions.[8]

The Supreme Court has held that the Fourth Amendment does not protect information that has been voluntarily disclosed to a third-party[9] or obtained by means of a private search.[10] Congress reacted to these holdings by creating a patchwork of statutes designed to prevent the government's direct and unfettered access to documents stored with third-parties; thus, the government's access is fettered by various statutory requirements, including, in many cases, notice of the disclosure.[11] Despite these protections, however, third-parties are not restricted from passing the same data to

[6] *See infra* Part II.

[7] *See infra* Part III.C; Mark P. Mills, *The Security-Industrial Complex*, FORBES, Nov. 29, 2004, http://www.forbes.com/forbes/2004/1129/044.html ("Security is a very big and growing tech business. Cumulative private and public sector security spending in the U.S. is forecast to exceed $1 trillion over the coming decade. . . . More than 800 companies packed exhibit aisles at the American Society for Industrial Security exhibition in Dallas in late September.").

[8] *See infra* Part III.C.3.

[9] *See infra* Part II.B.

[10] *See infra* Part II.C.

[11] *See infra* Part II.D.

other private companies (fourth-parties),[12] and after the events of September 11, 2001, the government, believing that it needed a greater scope of surveillance, turned to the fourth-parties to access the personal information it could not acquire on its own.[13] As a consequence, the fourth-parties, unrestricted by Fourth Amendment or statutory concerns, delivered—and continue to deliver—personal data *en masse* to the government.[14] Using this data, the government can, without probable cause or even an articulatable purpose, "produce a comprehensive profile on an individual, generated by only one or two queries."[15] One might argue that Congress could prevent this loophole by extending the existing statutes to fourth-parties, but as described below, such a result is unlikely.[16] While the world waits for a legislative solution that may never come, these private organizations are increasingly able to collect information about consumers, which the consumers would never anticipate being handed over to the government.

In particular, the shift to "cloud computing" is placing the very documents that were intended to be precluded from

---

[12] *See infra* Part III.C.3.

[13] Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CAL. L. REV. 901, 902 (2008) ("Private organizations can at times obtain and share information more easily and under fewer legal restrictions than the government can when it collects similar information on its own."). In addition, as the Center for Democracy & Technology describes, it is convenient to "outsourc[e]" the collection and preservation of such information. CENTER FOR DEMOCRACY & TECHNOLOGY, PRIVACY'S GAP: THE LARGELY NON-EXISTENT LEGAL FRAMEWORK FOR GOVERNMENT MINING OF COMMERCIAL DATA (2003) 2, *available at* http://www.cdt.org/security/usapatriot/030528cdt.pdf (last visited Dec. 3, 2009).

[14] For example, the Electronic Communications Privacy Act only reaches transmissions directly from a third-party to the government, not from the third-party to a fourth-party to the government. *See, infra* Part II.C.3.

[15] *CBD Notice for AutoTrack* (obtained by the Electronic Privacy Information Center from the United States Marshall's Service) *available at* http://epic.org/privacy/choicepoint/cpusms7.30.02b.pdf (last visited Dec. 3, 2009).

[16] *See infra* Part IV.B.3.

government invasion into the government's hands.[17] The term "cloud computing" is defined as the remote digital storage of information, which allows the user to access his or her document from any computer connected to the Internet.[18] A good example is Google Docs, which allows consumers to use Google's servers for the uploading and editing of documents, but also permits Google access to these documents for any purpose it chooses.[19]

This note argues that when fourth-parties disclose to law enforcement information generated as a result of searches that would be violations had the government conducted the

---

[17] *See infra* Part III.A; *see also* Jonathan Zittrain, *Lost in the Cloud*, N.Y. TIMES, July 19, 2009, at A19, *available at* http://www.nytimes.com /2009/07/20/opinion/20zittrain.html (discussing some of the dangers of cloud computing).

[18] *See* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT 123–24 (Yale Univ. Press 2008) (describing cloud computing in the context of the Google Maps API); Jon Brodkin, *Cloud Computing Hype Spurs Confusion*, NETWORK WORLD, Sept. 29, 2008, http://www.networ kworld.com/news/2008/092908-cloud-computing-definitions.html?hpg1=bn (discussing different categories of cloud computing: "one focusing on remote access to services and computing resources provided over the Internet 'cloud,' and the other focusing on the use of technologies such as virtualization and automation that enable the creation and delivery of service-based computing capabilities.").

[19] Google does not enter into an agreement with regard to use of its customers' information in its Terms of Service; instead, it has its customers agree to "the use of [their] data in accordance with Google's privacy policies," which Google can change at any time. Google Terms of Service, http://www.google.com/accounts/TOS (last visited Dec. 3, 2009); Google Privacy Policy, http://www.google.com/intl/en/privacypolicy.html (last visited Dec. 3, 2009) ("Google only shares personal information with other companies or individuals outside of Google in the following limited circumstances . . . . We provide such information to . . . trusted businesses or persons for the purpose of processing personal information on our behalf. . . . We have a good faith belief that access, use, preservation or disclosure of such information is reasonably necessary to (a) satisfy any applicable law, regulation, legal process or enforceable governmental request . . . or (d) *protect against imminent harm to the rights, property or safety of . . . the public* as required or permitted by law." (emphasis added)). *See generally* Google Docs, http://docs.google.com (last visited Dec. 3, 2009).

searches itself, those fourth-parties' actions should be considered searches by agents of the government, and the data should retain privacy protections. Part II describes the history of Fourth Amendment treatment of records that find their ways into the hands of third-parties either by disclosure or private search. Part III describes the state of technology and industry that has allowed private corporations to act as launderers for the government's acquisition of those documents. Finally, Part IV evaluates general proposals for coping with third-party disclosure and a new proposal for solving the problem of fourth-party disclosure of information gained through their quasi-private investigations.

II. THE STATE OF THE LAW: PROTECTION IS LIMITED

Although many lay people believe that there is a well-defined right to privacy, such a right, if it exists, has only been found by looking at the Bill of Rights generally.[20] When it comes to the people's right to be secured from government intrusion, it is the Fourth Amendment that provides the basis for such protection. It 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.[21]

The amendment is not self-defining, but has been construed to contain two clauses: one clause focuses on unreasonable searches and seizures, the other on when warrants shall issue. The meaning of these clauses, and

---

[20] *See, e.g.,* Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (finding that a right to privacy emanates from the penumbras of specific provisions of the Bill of Rights: the First, Third, Fourth, Fifth, and Ninth Amendments).

[21] U.S. CONST. amend. IV.

their interaction with each other, however, is unclear. Scholars have spent the better part of two centuries attempting to dissect and understand these fifty-four words.[22]

The Fourth Amendment was drafted at a time very much unlike our own. Our understanding of a person's expectations regarding privacy, of crime, and of the role of law enforcement, has necessarily changed since the Fourth Amendment's drafting. The framers were living in a world where law enforcement was so economically and technologically inefficient that there was little concern about it conducting even routine investigations. The little law enforcement that did occur was exclusively performed by part-timers and amateurs,[23] and the primary concern of

---

[22] Interestingly, the Fourth Amendment is not the most condensed amendment in the Bill of Rights; the Eighth Amendment is the shortest with 16 words.

Some of the confusion surrounding the amendment can be understood by the suggestion that the language above is not the language passed by the House of Representatives, and that an insertion was made at some point between the House vote and its report to the Senate. Thomas Y. Davies asserts that the House unanimously approved the following language:

> The right of the people to be secure in their person, houses, papers, and effects, against unreasonable searches and seizures, *shall not be violated by warrants issuing, without probable cause*, supported by oath or affirmation, and not particularly describing the places to be searched, and the persons or things to be seized.

See The Jury and the Search for Truth: The Case Against Excluding Relevant Evidence at Trial: Hearing Before the Comm. on the Judiciary, 104th Cong. 152 (1995) (statement of Thomas Y. Davies) (emphasis added, citations omitted). Davies notes that Representative Egbert Benson changed the language of the amendment after the House had voted down his proposed addition of "no warrant shall issue." *Id.* at 152, nn.20–21. However, even accepting the current language, what exactly it means remains unclear.

[23] Sam Kamin, *The Private is Public: The Relevance of Private Actors in Defining the Fourth Amendment*, 46 B.C. L. REV. 83, 89 (2004). Sheriffs were responsible for law enforcement, jails, and jury selection. However, they didn't have a staff, instead ordinary citizens rotated into positions as

Fourth Amendment jurisprudence was the general warrants that, when issued, allowed customs and tax inspectors and "officials of the Crown" to search one's home generally.[24] In fact, allegations that a search was illegal were primarily confined to civil complaints for trespass by government officials.[25] Although this view may seem odd now, one must remember that courts did not exclude evidence that was found during an illegal search until 1914.[26]

As times have changed, the Supreme Court has been called upon to interpret the Fourth Amendment. In doing so, the Court created two doctrines that now leave "the People" exposed to the very general searches that the Fourth Amendment was drafted to avoid: the third-party disclosure doctrine and the private party search doctrine.

---

constables or night watchmen. These citizens were untrained and generally unpaid. Early constables were responsible for announcing approved civil marriages, surveying land, and acting as "Sealer of Weights and Measures." Night watchmen called out the time and weather, and sometimes took care of street lamps. *See id.* at n.27.

[24] *Id.* at 90–91; *see* ANDREW E. TASLITZ, RECONSTRUCTING THE FOURTH AMENDMENT: A HISTORY OF SEARCH & SEIZURE, 1789–1868, at 17 (N.Y.U. Press 2006) (describing these "writs of assistance"). These searches were primarily conducted to search for heretical or seditious materials. TASLITZ, *supra* at 18–23; William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393, 394 (1995). As Professor Stuntz notes, the Fourth Amendment in the Eighteen Hundreds was primarily used as a check on the government's substantive power to prevent it from regulating the relevant conduct at all, as opposed to permitting regulation of the conduct, but attempting to safeguard individuals' sense of privacy. *Id.* at 395.

[25] Kamin, *supra* note 23, at 90–91.

[26] Weeks v. United States, 232 U.S. 383, 393 (1914) ("If letters and private documents can thus be seized and held and used in evidence against a citizen accused of an offense, the protection of the 4th Amendment . . . is of no value, and . . . might as well be stricken from the Constitution. The efforts of the courts . . . are not to be aided by the sacrifice of those great principles established be [sic] years of endeavor and suffering which have resulted in their embodiment in the fundamental law of the land."); *see* Mapp v. Ohio, 367 U.S. 643, 648 (1961) ("In the year 1914, in the Weeks case, this Court for the first time held that in a federal prosecution the Fourth Amendment barred the use of evidence secured through an illegal search and seizure." (internal citation omitted)).

A. Fourth Amendment Application

> *Civilization is the progress toward a society of privacy. The savage's whole existence is public, ruled by the laws of his tribe. Civilization is the process of setting man free from men.*
>
> — Ayn Rand[27]

In the modern era, the primary standard for applying the Fourth Amendment is *Katz v. United States*.[28] *Katz* turned

---

[27] AYN RAND, THE FOUNTAINHEAD 715 (Plume 2005) (1943).

[28] 389 U.S. 347 (1967). *Katz* itself was a major departure from what had been Fourth Amendment doctrine up until 1967. For years prior, Fourth Amendment analysis entailed a narrow textual reading of the amendment, as annunciated in *Olmstead v. United States*. 277 U.S. 438 (1928). *Olmstead* involved an appeal from a conviction for "conspiracy to violate the National Prohibition Act . . . by unlawfully possessing, transporting and importing intoxicating liquors." *Id.* at 455. The convicting evidence was procured by intercepting telephone calls, but these were made without trespassing on the defendants' properties. *Id.* at 456–57. The Court used a narrow textual reading and found that the Fourth Amendment only prevents official searches or seizures of people, papers, or "tangible material effects." *Id.* at 466; *see id.* at 464 ("The amendment itself shows that the search is to be of material things—the person, the house, his papers, or his effects. The description of the warrant necessary to make the proceeding lawful is that it must specify the place to be searched and the person or things to be seized.").

The Court held that the defendants' conversations were admissible, because neither (1) the area searched nor (2) the method used were protected. With regard to the area searched, to use their telephones the defendants had to send signals out of their homes and onto wires that they had no property interest in. *See id.* at 466. *Olmstead* focuses on the fact that there wasn't a physical trespass, which, as previously discussed, was also the focus of Fourth Amendment inquiries during the framing. *See* Kamin, *supra* note 23, at 90–91. As for the method used, the amendment only protects tangible items, which the messages were not. Olmstead, 277 U.S. at 464, 465 (citing Hester v. United States, 265 U.S. 57 (1924)).

This reading of the Fourth Amendment, while textually accurate, failed to get at the heart of the Fourth Amendment's intended protection. As Sam Kamin recently expostulated:

> To the extent that the Fourth Amendment was written to be a check on the capacity of law enforcement officials to conduct broad, invasive investigations based on little or no

on whether evidence of the defendant's "telephone conversations, overheard by FBI agents who had attached an electronic listening and recording device to the outside of [a] public telephone booth from which he had placed his calls," would be admitted at trial.[29] Although both parties' arguments focused on whether the telephone booth was a constitutionally protected area,[30] the Court held that "the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his home or office, is not subject to Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[31] Justice Harlan's concurrence contained what would become the watchwords of Fourth Amendment doctrine: "There is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.' "[32]

When *Katz* was decided, the general consensus was that it would increase privacy, because the Court was moving from a conception based on property rights to one which focused on the individual.[33] However, since then, *Katz* has been frequently criticized as either too protective or not protective enough. One such criticism is that "if the

> suspicion, the Olmstead Court's reading does the Amendment little justice. So long as law enforcement officials snoop by means not imagined by the Founders or investigate areas not explicitly mentioned in the Amendment's text, it would seem their actions will not offend the Constitution.

Kamin, *supra* note 23, at 94. Thirty-eight years later, the Supreme Court decided *Katz* and fundamentally shifted Fourth Amendment doctrine from *Olmstead*'s focus on what constitutionally protected places the framers wanted protected to the individual's and society's expectations of privacy. 389 U.S. 347 (1967).

[29] *Katz*, 389 U.S. at 348.

[30] *Id.* at 350.

[31] *Id.* at 351–352.

[32] *Id.* at 361 (Harlan, J., concurring).

[33] Kamin, *supra* note 23, at 138.

government were simply to announce that all phones would henceforth be tapped and monitored at random . . . it would be unreasonable for [people] to presume that their conversations were private, and no search would occur when the government eavesdropped on these conversations."[34] A second criticism comes from Justice Scalia, who bemoans:

> [T]he only thing the past three decades have established about the Katz test . . . is that, unsurprisingly, those "actual (subjective) expectations of privacy" "that society is prepared to recognize as 'reasonable,' " . . . bear an uncanny resemblance to those expectations of privacy that this Court considers reasonable. When that self-indulgent test is employed . . . it has no plausible foundation in the text of the Fourth Amendment.[35]

---

[34] *Id.* at 97. This danger is particularly acute in the digital context, because as news stories are released disclosing the extent of surveillance and technologists lament the end of privacy, members of society have no choice but to believe they are constantly being surveilled. In that case, the Fourth Amendment would provide no protection.

[35] Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring) (citations omitted). In 2009, in response to a comment by Justice Scalia, an Internet privacy class taught by Fordham Law School professor Joel Reidenberg created a fifteen page dossier on the justice from only materials discoverable on the Internet. The dossier included Justice Scalia's home address and phone number, his wife's personal e-mail address and the TV shows and food he prefers. Noam Cohen, *Law Students Teach Scalia About Privacy and the Web*, N.Y. TIMES, May 17, 2009, at B3, *available at* http://www.nytimes.com/2009/05/18/technology/internet/18link.html. The Justice responded by saying that he stood by his comment: "[I]t is silly to think that every single datum about my life is private. I was referring, of course, to whether every single datum about my life deserves privacy protection in law. It is not a rare phenomenon that what is legal may also be quite irresponsible. That appears in the First Amendment context all the time. What can be said often should not be said. Prof. Reidenberg's exercise is an example of perfectly legal, abominably poor judgment. Since he was not teaching a course in judgment, I presume he felt no responsibility to display any." Kashmir Hill, *Justice Scalia Responds to Fordham Privacy Invasion!*, ABOVE THE LAW, Apr. 29, 2009, http://abovethelaw.com/2009/04/justice_scalia_responds_to_for.php; *see also* Daniel Solove, *Justice Scalia's Dossier: Joel Reidenberg Responds*, CONCURRING OPINIONS, May 1, 2009, http://www.con

Despite such criticisms, *Katz* remains the dominant precedent in Fourth Amendment cases. Even Justice Scalia has held himself to its standard. In *Kyllo v. United States*, he delivered the opinion of the Court confirming that the Court had "rejected . . . mechanical interpretation[s] of the Fourth Amendment in *Katz*."[36] In *Kyllo*, the police had used a thermal imager to determine whether a suspect was growing marijuana in his home. The Court held that when the government "uses a device that is not in general public use, to explore the details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[37] *Kyllo* underscores that once the public is aware of a device capable of invading its privacy, it must either take steps to prevent the intrusion, or acknowledge that it has knowingly exposed itself to government surveillance. Unfortunately, in a digital world it is frequently either impossible to protect oneself while remaining a member of society or simply impossible to protect oneself at all.

The next two sections describe how merely storing electronic documents on a third-party's server—for example, using Google Docs—or having a private party search one's documents has been held to be corrosive to one's expectation of privacy, and can allow third-parties to disclose those documents to the government. Later, Section D will explain how Congress has attempted to prevent such disclosures and why the government has begun using fourth-parties as intermediaries in the acquisition of such data.[38]

curringopinions.com/archives/2009/05/justice_scalias_3.html (quoting Professor Reidenberg's response to Justice Scalia).

[36] 533 U.S. 27, 35 (2001).

[37] *Id.* at 40.

[38] *See infra* Part III.

B. Third-Party Disclosures

> *[The framers] conferred . . . the right to be let alone—the most comprehensive of rights and the right most valued by civilized men.*
>
> — Justice Louis D. Brandeis[39]

> *You already have zero privacy—get over it . . . .*
>
> — Scott McNealy[40]

The Fourth Amendment has long been held not to apply when someone voluntarily discloses information, either tangible or intangible, to a third-party. A year before the Court's dogmatic change in *Katz*, it announced in *Hoffa v. United States* that even though the government had placed a secret informant in the Teamsters President Jimmy Hoffa's good graces, any statements that Hoffa voluntarily confided in the informant were not protected by the Fourth Amendment.[41] Five years later, after *Katz* was decided, the Court not only affirmed *Hoffa*,[42] it extended it, holding that "if the law gives no protection to the wrongdoer whose trusted accomplice is or becomes a police agent, neither

---

[39] Olmstead v. United States, 277 U.S. 438 (1928) (Brandeis, J., dissenting).

[40] John Markoff, *Growing Compatibility Issue: Computers and User Privacy*, N.Y. TIMES, March 3, 1999, *available at* http://www.nytimes.com/1999/03/03/business/growing-compatibility-issue-computers-and-user-privacy.html (quoting Scott McNealy, chairman and chief executive of Sun Microsystems at a news conference).

[41] 385 U.S. 293, 302 (1966). The Court couched its decision in *Olmstead*'s reasoning. It found that although a hotel room could be the object of Fourth Amendment protection, the defendant "was not relying on the security of the hotel suite when he made his incriminating statements . . . he was relying upon his misplaced confidence that [the informer] would not reveal his wrongdoing." *Id.* at 302. Furthermore, the Court stated that this is the kind of risk one assumes whenever he speaks. *Id.* at 303.

[42] United States v. White, 401 U.S. 745, 749 (1971).

should it protect him when the same agent has recorded or transmitted the conversation."[43]

In two interrelated cases, the Supreme Court extended this logic to include records kept by institutions doing business with the defendant.[44] In *Miller*, the government subpoenaed the defendant's bank records, not from the defendant, but from two banks with which the defendant had accounts. The Court held that, despite the fact that a federal statute required these bank records to be kept,[45] the defendant had no Fourth Amendment expectation of privacy in his bank records because, due to the fact that the defendant had voluntarily exposed them to the bank and its employees, the records were not *private* papers.[46] The Court then cited both *White* and *Hoffa* for the proposition 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."[47]

Similarly, in *Smith*, the Court found that the installation of a pen register, which recorded the numbers dialed from

---

[43] *Id.* at 752. Technically, there was only a majority vote for the proposition that *Katz* was not retroactive, and therefore, the Court of Appeals should have applied previous precedent, which would have yielded the same result. *Id.* at 754.

[44] United States v. Miller, 425 U.S. 435 (1976); Smith v. Maryland, 442 U.S. 735 (1979).

[45] *See* Bank Secrecy Act, 12 U.S.C. §§ 1951–59 (2006).

[46] *Miller*, 425 U.S. at 440–442.

[47] *Id.* at 443. One wonders how far the court would have been willing to allow this argument to extend. Can information that a third-party, with whom personal information has been shared for a limited and confidential purpose, has passed to a fourth-party, for an additional but limited purpose, be extracted by the government? Certainly, the defendant would have no expectation that the third-party would keep his information from the government, but would the defendant expect the third-party to hand his information to a fourth-party? Particularly if the third-party has an explicit privacy policy that appears to suggest it would not do so.

the defendant's telephone, did not implicate the Fourth Amendment, because "all telephone users realize that they must 'convey' phone numbers to the telephone company" and that "the phone company has facilities for making permanent records of the numbers they dial."[48] Again the Court, relying on *Miller*, held that there was no claim of an expectation of privacy when the defendant voluntarily conveyed the information to a third-party.[49]

The reasoning employed in *Miller* and *Smith* is not exactly the same as that in *Katz*. *Katz*, and later cases,[50] focused on "what a person knowingly expose[d] to the public."[51] *Miller* and *Smith*, on the other hand, involve the far more limited and confidential exposure of information to a single third-party.[52] Although exposure to third-parties may create a lessened expectation of privacy, it is not unreasonable for one to expect, nor for the public to protect, what little subjective expectation remains.[53] It is

[48] Smith v. Maryland, 442 U.S. 735, 742 (1979). The Court continues by saying that "[a]lthough subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret." *Id.* at 743. Interestingly, scholars have found that the public's expectations of privacy can, in fact, be tested. *See, e.g.*, Kamin, *supra* note 23, at n.80.

[49] *Smith*, 442 U.S. at 744.

[50] *See* California v. Greenwood, 486 U.S. 35, 37 (1988) (holding that garbage left for collection outside the home is not protected by the Fourth Amendment, because it was observable by any member of the public); California v. Ciraolo, 476 U.S. 207 (1986) (holding that surveillance of a fenced backyard from a private plane did not implicate the Fourth Amendment).

[51] Katz v. United States, 389 U.S. 347, 351 (1967).

[52] *Cf.* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 588 (2009) (arguing that *Miller* can be better understood as "eliminat[ing] privacy because the target voluntarily consents to the disclosure, not because the target's use of a third party waives a reasonable expectation of privacy.").

[53] For example, leave use of the information in the regular course of business unprotected, such that if disclosure to the government is ordinary for the third-party, disclosure on a specific occasion would not be protected. However, if disclosure is irregular and not part of the regular

understandable that the Court in applying the *Katz* standard would seek to create a Fourth Amendment exemption for third-party disclosure, but in doing so the Court opened a door that, in the digital age, leaves little unavailable to the government, and which utterly frustrates the purpose of the Fourth Amendment.[54] Congress has attempted to stop these

course of conducting the business involved, the document should remain protected.

[54] *See infra* Part II.B. In *United States v. Hambrick*, a police officer subpoenaed the defendant's Internet Service Provider, and the court held, citing the third-party disclosure doctrine, that the defendant had assumed the risk of disclosure by sharing his information with the ISP. 55 F. Supp. 2d 504, 507–508 (1999); *see also* Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) ("Computer users do not have a legitimate expectation of privacy in their subscriber information because they have conveyed it to another person—the system operator."); United States v. D'Andrea, 497 F. Supp. 2d 117, 120 (D. Mass. 2007) ("The *Smith* line of cases has led federal courts to uniformly conclude that internet users have no reasonable expectation of privacy in their subscriber information, the length of their stored files, and other noncontent data to which service providers must have access."); Freedman v. America Online, Inc., 412 F. Supp. 2d 174, 181 (D. Conn. 2005) ("In the cases in which the issue has been considered, courts have universally found that, for purposes of the Fourth Amendment, a subscriber does not maintain a reasonable expectation of privacy with respect to his subscriber information."); United States v. Sherr, 400 F. Supp. 2d 843, 848 (D. Md. 2005) ("The courts that have already addressed this issue . . . uniformly have found that individuals have no Fourth Amendment privacy interest in subscriber information given to an ISP.").

In *United States v. Forrester*, the court found that e-mail headers, visited website IP addresses, and the amount of data transmitted, were all sufficiently analogous to the pen registers in *Smith v. Maryland* such that their surveillance did not constitute a Fourth Amendment search. 512 F.3d 500, 510–511 (9th Cir. 2008) ("E-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information."). *But see* United States v. Cioffi, No. 08-CR-415, at 6 n.7 (E.D.N.Y. 2009) (assuming that the defendant had a reasonable expectation of privacy in the contents of his e-mail account, even though in this case that account was maintained by Google).

encroachments on privacy through legislation, but once third-party disclosure occurs, any fourth-party who can evade that legislation is free to hand such information to the government.[55]

C. Private Searches

> *This is an age where faceless informers have been reintroduced into our society in alarming ways .... Though the police are honest and their aims worthy, history shows they are not appropriate guardians of the privacy which the Fourth Amendment protects.*
>
> — Justice William O. Douglas[56]

Just as the Fourth Amendment does not protect information voluntarily disclosed to a third-party,[57] it does not apply to information searched or seized by a private party without government involvement, even if that information is given to the government to be used as evidence.[58] This doctrine provides an incentive to create companies whose purpose is to conduct searches for information that they know the government will be willing to pay to access. Thus, as discussed below, fourth-parties hire former government officials to advise them, and then they conduct searches that the government would be unable to perform itself.[59]

These decisions are troubling given that an ISP can maintain records of everything done by their users on the Internet. This means that the government can access records of all Internet-based conduct, which is as close to the general warrants the Fourth Amendment was written to prevent as possible.

[55] *See infra* Part III.C.

[56] Jones v. United States, 362 U.S. 257, 273 (1960) (Douglas, J., dissenting in part).

[57] *See supra* Part II.B.

[58] *See* Coolidge v. New Hampshire, 403 U.S. 443, 489 (1971) (holding that when the private party produced evidence, without coercion or dominance, "it was not incumbent on the police to stop her or avert their eyes.").

[59] *See infra* Part III.C.

The seminal private search case is *Burdeau v. McDowell*, in which the Court held that papers stolen from the plaintiff's office by a private party and subsequently delivered to the government did not need to be returned to their owner.[60] The Court reasoned that "[the Fourth Amendment's] origin and history clearly show that it was intended as a restraint upon the activities of sovereign authority, and was not intended to be a limitation upon other than governmental agencies."[61]

1. Scope of the Search

A more modern example involved a search conducted by Federal Express employees, pursuant to a company policy, when a package they were carrying was damaged by a forklift and a white powdery substance was observed.[62] The package had been wrapped as well as possible to avoid disclosing its contents,[63] but the employees cut through multiple layers of packaging, including a basement duct tube—which for all they knew was what was being transported—until they discovered Ziploc bags of white powder.[64] They then notified the Drug Enforcement Administration, but before an agent arrived, they repackaged the parcel.[65] Upon arrival, the agent re-opened the box, tested the white powder within, and determined that it was cocaine.[66] The Court found:

---

[60] 256 U.S. 465, 475–76 (1921).

[61] *Id.* at 475.

[62] United States v. Jacobsen, 466 U.S. 109, 111 (1984).

[63] *Id.* ("The container was an ordinary cardboard box wrapped in [eight layers of] brown paper. Inside the box five or six pieces of crumpled newspaper covered a tube about 10 inches long; the tube was made of the silver tape used on basement ducts. . . [Inside were] a series of four zip-lock plastic bags, the outermost enclosing the other three and the innermost containing about six and a half ounces of white powder.").

[64] *Id.*

[65] *Id.*

[66] *Id.* at 111–12.

> [T]he fact that agents of the private carrier independently opened the package and made an examination that might have been impermissible for a government agent cannot render otherwise reasonable official conduct unreasonable. The reasonableness of an official invasion of the citizen's privacy must be appraised on the basis of the facts as they existed at the time that invasion occurred.[67]

Because the defendant delivered the package to a third-party who frustrated his expectation of privacy by conducting a private search,[68] and "the Government did not exceed the scope of the private search" with its subsequent invasions,[69] the Court held that the government action was not a search within the meaning of the Fourth Amendment.[70] It did, however, reject the "suggestion that [the] case [was] indistinguishable from one in which the police simply learn from a private party that a container contains contraband, seize it from its owner, and conduct a warrantless search."[71] The Court suggests that such a warrantless search would have been unconstitutional and that "the precise character of the white powder's visibility to the naked eye [was] far less significant than the facts that the container could no longer support any expectation of privacy, and that it was virtually certain that it contained nothing but contraband."[72] Therefore, the Court's decision turned not on the private party's possession of a container he believed contained contraband, nor on any probable cause the agents had at the time of the search, but on the frustration of the defendant's reasonable expectation of privacy. Without a private search, the Court suggested that a container that otherwise retained

---

[67] *Id.* at 114–15.

[68] *Id.* at 117 (citing United States v. Miller, 425 U.S. 435, 443 (1976)).

[69] *Id.* at 116 (quoting Walter v. United States, 447 U.S. 649 (1980)). The Court treated each of the subsequent invasions separately: seizing the package, viewing the powder inside the plastic bags, and testing the substance.

[70] *Id.* at 126.

[71] *Id.* at 120 n.17.

[72] *Id.*

a reasonable expectation of privacy could not be subjected to a warrantless search.[73]

Jacobsen is a worrisome decision because it stands for the proposition that despite making every attempt to maintain the privacy of a parcel, one's reasonable expectation of privacy may be frustrated by actions completely out of his or her control. After *Jacobsen*, the only means to transport a package containing items the sender wishes to keep from being disclosed to the government is for the sender to transport the package herself, thus avoiding the opportunity for private-party searches.[74] Yet, while this may be a satisfying result in the context of a package and a mail carrier where personal transportation is possible, it is quite a different matter in the digital context where there is no reasonable alternative to transmission through third-parties.[75]

The Court's opinion indicates that one can retain a legitimate expectation of privacy after a private search is conducted, but that expectation is limited by the scope of the private search.[76] The Court, however, has never clarified how to determine the scope of a private search of physical

---

[73] *Id.*

[74] This is not to say that drug trafficking should be encouraged. However, what may be a search revealing cocaine today, may be a search revealing seditious materials tomorrow.

[75] *See* Smith v. Maryland, 442 U.S. 735, 749–50 (1979) (Marshall, J., dissenting) ("Implicit in the concept of assumption of risk is some notion of choice [and] some discretion in deciding who should enjoy his confidential communications. . . . By contrast here, unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance. . . . It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative." (citations omitted)); *cf.* James Harkin, *Is access to the internet now a human right?* TIMES ONLINE, Nov. 4, 2009, http://technology.timesonline.co.uk/tol/news/tech_and_web/article6901504.ece (describing an ISP's threat of a lawsuit against the British Business Secretary under human rights legislation due to the Secretary's announcement that he would disconnect "persistent [I]nternet pirates").

[76] Therefore, once a fourth-party has infiltrated a source of information, the government is free to access that source within the scope of the fourth-party's search.

materials, much less digital works, which has left such determinations to the circuit courts. For example, the Fifth Circuit has determined that while a private search of a given computer disk destroys the expectation of privacy in all files on that disk regardless of how the files are organized,[77] a private search of some computer disks in a collection does not frustrate an expectation of privacy with regard to all the disks in that collection.[78] Therefore, once a private party has searched a computer disk in a collection, law enforcement's investigation of that computer disk, but not the others, does not constitute a Fourth Amendment search in the Fifth Circuit.[79]

---

[77] United States v. Runyan, 275 F.3d 449, 465 (5th Cir. 2001).

[78] *Id.* at 464.

[79] Another area where the circuits have been left to their own devices is the determination of when a private party becomes a government agent, which would in turn implicate the Fourth Amendment. In the Ninth Circuit and several others, the critical factors are "(1) whether the government knew of and acquiesced in the intrusive conduct, and (2) whether the party performing the search intended to assist law enforcement efforts or [alternatively] to further his own ends." United States v. Miller, 688 F.2d 652, 657 (9th Cir. 1982) (citing United States v. Walther, 652 F.2d 788, 791–92 (9th Cir. 1981). *See also* United States v. Paige, 136 F.3d 1012, 1017–18 (5th Cir. 1998) (affirming application of the two-part *Miller* test); United States v. Feffer, 831 F.2d 734, 739 (7th Cir. 1987) (applying the same two-factor test). In *Miller*, the government conceded the first factor, but the court determined that the second factor was not satisfied, because (a) the private actor was acting out of a desire to recover his stolen property, (b) it was his plan and not the officers', and (c) his plan was not illegal and so the officers had no reason to restrain him. 688 F.2d at 657.

In contrast, the Tenth Circuit, which uses the same factors, has determined that the second prong does not require evaluating "the private person's state of mind—whether his motive to aid law enforcement preponderates. . . . [because] [a]lmost always a private individual making a search will be pursuing his own ends—even if only to satisfy curiosity-although he may have a strong intent to aid law enforcement." United States v. Leffall, 82 F.3d 343, 347 (10th Cir. 1996). Instead, the Tenth Circuit requires the court to consider the government's role, and whether an agent was involved "either directly as a participant—not merely as a witness—or indirectly as an encourager of the private person's search." *Id.*

2. Standing Idly By

In certain circumstances, government involvement may be found when it does not request or direct a search, but is merely aware of an illegal search by a private person and fails to prevent the intrusion.[80] For example, an officer that follows a private party to a suspect's apartment and remains in the hallway while the private party conducts a search of the apartment, despite their being no indication of inducement,[81] will be held to have participated in the search, and the private party an agent of the government.[82] The doctrine merely requires that the official have a "hand in it," with the decisive factor being "the actuality of a share . . . in the total enterprise of securing and selecting evidence by other than sanctioned means. It is immaterial whether a federal agent originated the idea or joined in it while the search was in progress. So long as he was in it before the

---

Hawai'i, on the other hand, found these factors completely unworkable. In *Kahoonei*, the Supreme Court of Hawai'i determined that the motivation of the private party was irrelevant, and instead focused on the totality of the circumstances "to determine whether the *governmental* involvement [was] significant or extensive enough to objectively render an otherwise private individual a mere arm, tool, or instrumentality of the state." State v. Kahoonei, 925 P.2d 294, 300 (Haw. 1996) (emphasis added).

The factors used by the First Circuit are: "[1] the extent of the government's role in instigating or participating in the search, [2] its intent and the degree of control it exercises over the search and the private party, and [3] the extent to which the private party aims primarily to help the government or to serve its own interests." United States v. Momoh, 427 F.3d 137, 141 (1st Cir. 2005) (quoting United States v. Pervaz, 118 F.3d 1 (1st Cir. 1997)).

[80] Stapleton v. Superior Court, 447 P.2d 967, 970 (Cal. 1968) ("[T]he police stood silently by while [the private party] made the obviously illegal search . . . . [T]he police need not have requested or directed the search in order to be guilty of 'standing idly by'; knowledge of the illegal search coupled with a failure to protect the petitioner's rights against such a search suffices."); *but see* People v. North, 629 P.2d 19, 23 (Cal. 1981) (narrowing *Stapleton* to cases involving a joint operation where a request is made or the government knowingly allows the search to occur).

[81] Moody v. United States, 163 A.2d 337, 339 (D.C. App. 1960).

[82] *Id.* at 340.

object of the search was completely accomplished, he must be deemed to have participated in it."[83]

On the other hand, in *United States v. Steiger*, an anonymous computer hacker contacted officials with information of potential sexual abuse and child molestation;[84] information which he accessed using a Trojan horse virus.[85] Though law enforcement asked for any additional information the hacker possessed, including the accused's IP address,[86] the court held that "even assuming *arguendo* that [law enforcement] tacitly encouraged further nonconsensual searches,"[87] the information acquired before contact with law enforcement was not protected by the Fourth Amendment.[88] After the accused was indicted, an FBI agent informed the hacker that he would not be prosecuted, thanked him for his assistance, and told him, "If you want to bring other information forward, I am available."[89]

A year later, the hacker contacted law enforcement with evidence of another potential child molester.[90] Although the government conceded the second prong of the *Miller* test,[91] the court held that the conversations that occurred between the first and second search were insufficient to establish government acquiescence[92] because the communications were too temporally remote[93] and tenuous.[94] Furthermore, the

[83] *Id.* (quoting Lustig v. United States, 338 U.S. 74, 78–79 (1949)).

[84] 318 F.3d 1039, 1042 (11th Cir. 2003).

[85] *Id.* at 1044.

[86] *Id.* at 1042.

[87] *Id.* at 1045.

[88] *Id.*

[89] United States v. Jarrett, 338 F.3d 339, 341 (4th Cir. 2003).

[90] *Id.* at 341–42.

[91] *Id.* at 345.

[92] *Id.* at 347.

[93] *Id.* at 346 ("[A]ll of these exchanges were brief and took place seven to twelve months before the Jarrett search.").

[94] *Id.* ("[T]hese exchanges consisted of nothing more than perfunctory expressions of gratitude for [the hacker's] assistance in the Steiger investigation, assurances that [the hacker] would not be prosecuted should

court found that even though the government did not discourage the hacker, this did not make the hacker an agent, because "more explicit representations and assurances . . . that [the government] was interested in furthering its relationship with [the hacker] and availing itself of the fruits of any information that [the hacker] obtained" were necessary.[95] Interestingly, the court conceded that a post-search exchange, which it characterized as "the proverbial 'wink and a nod,' "[96] "probably" would have constituted sufficient government participation had it been made before the hacker's search.[97]

D. Statutory Scheme

> *Voice mail? I don't even know what that is. How can you mail a voice?*
>
> — Will & Grace[98]

Since *Katz* opened the door for the government to remove the public's reasonable expectation of privacy by merely announcing its ability to search, the people's exposure has been compounded by the extension of the third-party disclosure doctrine and the government's use of private parties to obtain information that is at the heart of living in

---

he decide to testify as a witness in the Steiger trial, and a vague offer of availability to receive more information in the future.").

[95] *Id.* at 347.

[96] *Id.* at 343 (An email from law enforcement to the hacker read: "I can not ask you to search out cases such as the ones you have sent to us. That would make you an agent of the Federal Government and make how you obtain your information illegal and we could not use it against the men in the pictures you send. But if you should happen across such pictures as the ones you have sent to us and wish us to look into the matter, please feel free to send them to us. We may have lots of questions and have to email you with the questions. But as long as you are not 'hacking' at our request, we can take the pictures and identify the men and take them to court. We also have no desire to charge you with hacking. You are not a U.S. citizen and are not bound by our laws.").

[97] *Id.* at 346.

[98] *Will & Grace: Bully Wully* (NBC television broadcast February 3, 2005).

the twenty-first century. Recognizing this exposure, Congress passed a patchwork of statutes designed to protect against disclosure, each of which protects to an extent specific types of information, including: communications, child privacy, financial information, medical records, and various other types of information.[99]

For example, bank records are not protected by the Fourth Amendment, because the Court in *Miller* found that they had been disclosed to a third-party: the bank.[100] Congress attempted to resolve this by passing the Right to Financial Privacy Act,[101] which purports to prevent the government from accessing "copies of, or the information contained in the financial records" of a financial institution's customers "*from* a financial institution."[102] There is no provision, however, preventing the financial institution from disclosing that information to a fourth-party, who could then pass it on to the government.[103]

---

[99] A description of these statutes is beyond the scope of this piece. See the Center for Democracy & Technology's *Guide to Online Privacy*, http://www.cdt.org/privacy/guide/protect/laws.php, for more information on individual statutes.

Because the United States' privacy laws are sectoral (covering specific information use) instead of omnibus (covering a wide array of information uses), there are various uses of information that are not currently covered by privacy laws. *See generally* Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902 (2009) (arguing that adopting a Federal omnibus privacy law that preempted federal and state sectoral laws would be a mistake, and describing differences between sectoral and omnibus privacy laws). For example, if the government wanted to conduct research using social network information similar to the research discussed *supra* note 5, there are currently no privacy laws in the United States that would prohibit them from doing so, assuming that they do not seize the underlying content. *See infra* notes 104 & 105 and accompanying text (describing that non-content information is subject to less protection).

[100] United States v. Miller, 425 U.S. 435 (1976); *see supra* Part II.B.

[101] 12 U.S.C. §§ 3401–22 (2006).

[102] 12 U.S.C. § 3402 (2006) (emphasis added). Similarly, the financial institution is restricted from voluntarily providing the government relevant records. *Id.* at § 3403.

[103] In fact, the JPMorgan Chase & Co. Privacy Policy explicitly states that Chase shares information about its customers within its "family as

Similarly, while the Electronic Communications Privacy Act provides some protection against the disclosure of wired, electronic, and stored communications to the government,[104] it also allows service providers to disclose consumer records to "any person other than a governmental entity,"[105] such as

required or permitted by law," and with outside companies, including marketing firms and other financial companies, but also with "retailers, auto dealers, auto makers, direct marketers, membership clubs and publishers." Furthermore, Chase reserves the right, even if its customers take the affirmative step of contacting Chase and telling them not to share their information, to share the information. Privacy Policy – Chase Security Center, https://www.chase.com/index.jsp?pg_name=ccpmapp/privacy_security/protection/page/privacy_policy (last visited Dec. 3, 2009).

Also, the FBI's National Security Law Unit believes that the FBI's use of fourth-party information need not comply with the Fair Credit Reporting Act because "Choicepoint [a fourth-party described below] does not collect 'public record information' for any of the [FCRA] purposes" and is not acting as a consumer reporting agency when it does so. Memorandum from the Federal Bureau of Investigation, Guidance Regarding the Use of ChoicePoint for Foreign Intelligence Collection or Foreign Counterterrorism Investigations at 12–14 (Sept. 17, 2001), *available at* http://epic.org/privacy/publicrecords/cpfcimemo.pdf [hereinafter FBI Memorandum].

Furthermore, disclosure of financial records that are not identifiable as being from a particular customer is not restricted at all. 12 U.S.C. § 3413(a) (2006). Of course, what constitutes "personally identifiable" information may be a point of contention for privacy groups. Seth Schoen, *What Information is "Personally Identifiable"?*, ELECTRONIC FRONTIER FOUNDATION (Sept. 11, 2009), http://www.eff.org/deeplinks/2009/09/what-information-personally-identifiable (describing a 1997 study that purports to show that with only a gender, zip code, and date of birth, one can identify individually about 87% of the United States population); Nate Anderson, *"Anonymized" data really isn't—and here's why not*, ARSTECHNICA, Sept. 8, 2009, http://arstechnica.com/tech-policy/news/2009/09/your-secrets-live-online-in-databases-of-ruin.ars. Similarly unrestricted is disclosure of financial records to certain government agencies, 12 U.S.C. at § 3413, including foreign counterterrorism organizations and the secret service, which may use special procedures to keep such disclosure secret. *Id.* § 3414.

[104] *See infra* Part III.B.1.

[105] 18 U.S.C. § 2702(c)(6) (2006); *see also* Michaels, *supra* note 13, at 918. It is important to note that § 2702(c) does not allow for the disclosure of the contents of stored communications. However, "contents" is defined as "information concerning the substance, purport, or meaning of that

a fourth-party, and there is no provision preventing the fourth-party from giving that information to the government in turn. Therefore, the government can avoid requesting a warrant or waiting 180 days and issuing a subpoena, both of which would eventually require disclosure of the search and seizure, by using a fourth-party as a go-between.

Despite the public's understandable expectations of non-disclosure of their documents in the hands of third-parties and the statutes that Congress has passed to protect those expectations, the courts have held that such statutes do not establish an expectation of privacy cognizable under the

---

communication," 18 U.S.C. § 2510(8) (2006), which does not include metadata or subscriber information. Metadata includes all information other than the actual substance of the communication; therefore, providers are free to disclose the identities of the first- and second-parties, their IP addresses, when the messages were sent, and various other useful information. Subscriber information may include a party's name, address, credit card number, telephone number, and other similar information. *See* Freedman v. America Online, Inc., 412 F. Supp. 2d 174, 181 (D. Conn. 2005) (noting a distinction between "the content of electronic communications, which is protected, and non-content information . . . which is not").

In addition, there are a number of exceptions to the non-disclosure of the contents of stored communications requirement, including with the consent of the first- or second-parties, and, in the case of a remote computing service, the subscriber. 18 U.S.C. § 2702(b). Courts have interpreted this exception to apply broadly to both express and implied consent. Griggs-Ryan v. Smith, 904 F.2d 112, 116 (1st Cir. 1990) (holding that the continued use of a telephone, having received "unambiguous, unqualified notice" of monitoring, was implied consent to the disclosure of any and all content of any communications); United States v. Amen, 831 F.2d 373, 378 (2d Cir. 1987) (noting that Congress intended the provision to allow for implied consent in a variety of settings, including monitoring of banks and apartment houses). These cases suggest that if a user has explicitly accepted privacy policy terms that provide for disclosure at a third-party's whim, *see infra* Part III.B.2, a court would find that the user had consented to any such disclosures.

Also, third-parties may disclose the contents of a subscriber's communications or stored communications when done "incident to the rendition of his service or to the protection of the rights or property of the provider." 18 U.S.C. at § 2511(2)(a)(i) (2006). This would also appear to open a rather large hole for third-parties to disclose information to others.

Fourth Amendment.[106] Therefore, "[e]ven if . . . information is disclosed to a single entity for a narrow purpose, . . . [and] that information is protected by a privacy statute if accessed by a private actor, and . . . the government conduct in question would violate that statute, the courts are unlikely to find a reasonable expectation of privacy."[107]

As discussed in Part III, the reality is that neither the current legislative hodgepodge nor appeals for judicial intervention are able to protect against government intrusion and investigation of nearly all aspects of a citizen's—or non citizen's—life.

III. THE TECHNOLOGICAL REALITY

The impetus for drafting the Fourth Amendment was a concern that grew out of the Crown's ability to issue general warrants that permitted inspectors and other officials to search people's homes generally.[108] The framers were offended by the idea that government officials could trespass on their private property and rummage through their personal effects without any semblance of a reason.[109] Out of these anxieties grew the Fourth Amendment and cases that were designed to hold the state to a standard of conduct when conducting searches and seizures of its people and their property.

Unfortunately, due to technological shifts and government obfuscation of the purpose behind the Fourth Amendment, the people's persons, houses, papers, and effects are now available for government search and scrutiny without regard to judicial process. Section A lays out the

---

[106] United States v. Hambrick, 55 F. Supp. 2d 504, 507 (W.D. Va. 1999) ("Although Congress is willing to recognize that individuals have some degree of privacy in the stored data and transactional records that their ISPs retain, the ECPA is hardly a legislative determination that this expectation of privacy is one that rises to the level of 'reasonably objective' for Fourth Amendment purposes.").

[107] Kamin, *supra* note 23, at 130.

[108] *See id.*

[109] *Id.*

state of technology and how third-party intermediaries are able to retain data on millions of consumers. Section B describes how those "trusted" intermediaries have handed over that information to the government, and which laws make it less convenient for the government to get that data from third-parties. Section C assesses the fourth-party problem and why the government has turned to these companies in an effort to access information it is unable to gather otherwise.

A. The State of Technology

> *Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and . . . expose . . . the most intimate occurrences of the home.*
>
> — Justice Louis D. Brandeis[110]

In the 20th century, there were major societal shifts caused by changes in technology. When computers were first introduced to the market, they merely displaced the customary desktop functions of creating, storing, and distributing documents. Now we are seeing the introduction of cloud computing in the consumer marketplace, which goes beyond what users do themselves; it encompasses what they want their computers to be able to do, and how they want it done. Cloud computing is a form of computing where, instead of providing computing power as a product that allows you to create content locally, content and computing power are provided as a centrally administered service. An example of cloud computing is Google Docs, where Google maintains a user's document on their servers while creating an interface that, in all other respects, acts like a conventional word processor.[111] Professor Richard C. Picker argues that the shift to cloud computing is natural, because (1) users are bad at performing their own tech support,

[110] Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

[111] Google Docs, http://docs.google.com (last visited Dec. 3, 2009).

(2) computers are complicated, (3) poorly run computers are used by hackers to harm everyone else, and (4) users cannot buy additional computing power as it is needed.[112] Furthermore, he notes that, like electricity, users may one day rely on companies providing cloud computing services to do the "hard work" while they merely plug in.[113]

In addition to cloud computing, people ask more of the computers they interact with than mere desktop publishing: they want them to match and coordinate.[114] This, however, has created a group of intermediaries with access to every click users make,[115] whose business model is either to charge transaction fees—such as eBay and Craigslist—or support advertising content—such as Google and Facebook. These businesses have every incentive to find new ways of exploiting the prodigious amount of data they have about their users:

> The new Web intermediaries . . . have access to an enormous datastream about their users . . . . These data are the[ir] lifeblood . . . and could play a similarly important role as a cloud infrastructure emerges. The advertising that supports much of the content on the Internet is much more valuable if it can be matched to [one's] actual interests.[116]

This leaves society with two major questions. First, can these intermediaries be trusted with this information? The information accrues naturally from the tasks these agents

---

[112] Randal C. Picker, *Competition and Privacy in Web 2.0 and the Cloud*, 103 NW. U. L. REV. COLLOQUY 1, 5 (2008).

[113] *Id.* ("Most people wouldn't consider for a second generating their own electricity; they expect to get it from a socket and want to rely on the local electricity company to do the hard work. We may be headed in that direction on computing power, both for calculation and storage.").

[114] Picker, *supra* note 112, at 3 ("eBay is explicitly about creating a marketplace to match buyers and sellers. Craigslist matches everything under the sun . . . . Social networking sites like mySpace and Facebook match individuals to define new groups. And Google matches people looking for content with the websites where the content is stored.").

[115] *Id.* at 5.

[116] *Id.* at 3.

are asked to perform. However, if they cannot be trusted, society can create regulations requiring the destruction of the information, "but throwing away the information requires a deliberate engineering design choice by the intermediaries."[117] If the *intermediaries* can be trusted to retain consumer data, the second question is whether they should be able to turn around and disclose that information to whomever they wish.[118]

Every time a user uses the Internet, whether moving information about herself online or merely using Internet-based applications, the service-providing intermediaries develop their cache about her. For many, this kind of monitoring is itself troubling.[119] Some may be comforted by the patchwork of statutes meant to restrict the intermediaries' ability to collect and disclose information about their users.[120] However, built into those statutory restrictions, there are frequently sufficient exceptions and work arounds to allow an intermediary to sell data about its

---

[117] *Id.* at 5.

[118] For example, should these intermediaries be permitted to disclose our information to our government, other governments, advertisers, and data mining companies? To an extent, these questions have been answered. For example, with the passage of the Electronic Communications Privacy Act in 1986, Congress limited the ability of electronic communication services to divulge stored communications. 18 U.S.C. § 2702 (2006). However, as discussed below, the ECPA provides insufficient protection against government intrusion.

Some commentators argue that as individuals shift to cloud computing, law enforcement will be driven to working with third-parties to gather information. ZITTRAIN, *supra* note 18, at 186 ("The movement of data from the PC means that warrants served upon personal computers and their hard drives will yield less and less information as the data migrates onto the Web, driving law enforcement to the networked third parties now hosting that information. When our diaries, e-mail, and documents are no longer stored at home but instead are business records held by a dot-com, nearly all formerly transient communication ends up permanently and accessibly stored in the hands of third parties, and subject to comparatively weak statutory and constitutional protections against surveillance.").

[119] *See* Picker, *supra* note 112, at 5–6.

[120] *See supra* Part II.D.

consumers. For example, the Cable Communications Policy Act limits what a cable operator can do without written or electronic consent from its subscribers: the Act limits its ability to use the cable system to collect personally identifiable information,[121] and disclose that information.[122] However, the Act allows acquisition of information as necessary to operate the services the cable company provides,[123] and allows disclosure as necessary to conduct legitimate business activities related to the company's services.[124] This means that if the cable company vertically integrates and takes on greater responsibilities, it can render the restrictions largely ineffective, because these provisions do not bar disclosure within the company.[125] Additionally, in many circumstances, there is no reason for a company to make an actual disclosure because they are able to sell a user's information inside a "black box."[126]

These concerns for user privacy, however, pale in comparison to the greater concern raised when the

---

[121] *See* 47 U.S.C. § 551(b)(1) (2006).

[122] *Id.* § 551(c)(1).

[123] *Id.* § 551(b)(2)(A).

[124] *Id.* § 551(c)(2)(A). In this modern age, however, a legitimate business activity could include disclosure to a credit rating agency or credit investigator to ensure the reliability of the service recipient. Such disclosures would be legitimate business activities, but the statute places no restrictions on the use of the information beyond the cable operator's activities. This is particularly striking when one realizes that most fourth-parties began as components of credit reporting companies. *See* discussion *infra* Part III.C.1.

[125] *See* Picker, *supra* note 112, at 10. Another industry where this is relevant is banking. In 1999, the Gramm-Leach-Bliley Act repealed part of a previous Act—the Glass-Steagall Act—which prevented one corporation from providing any combination of investment banking, commercial banking, and insurance service. Allowing mergers of these once separated companies means that they will be able to share the information.

[126] Picker, *supra* note 112, at 11 ("Google's ad placement server . . . does not disclose any information to facilitate matches between content and consumers. For Google's advertisers the information will be in a black box . . . . No disclosure of the datastream, just use on the advertiser's behalf.").

government attempts to obtain access to that information, especially when it does so outside of the judicial process.

B. Government Relationships with Third-Parties

> *Examples of the information we collect and analyze include the Internet protocol (IP) . . . login; e-mail address; password; computer and connection information . . . operating system, and platform; purchase history . . . the full Uniform Resource Locator (URL) clickstream to, through, and from our Web site, including . . . products you viewed or searched for . . . we may . . . measure and collect session information, including page response times . . . length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), and methods used to browse away from the page.*
>
> — Amazon.com[127]

Whereas traditional intermediaries are somewhat restricted in the ways they can exploit their users' information,[128] "the emerging financial infrastructure for financing Web 2.0—free content paid for by on-line advertising supported by rich databases—is largely unregulated."[129] Furthermore, the government has established relationships with third-parties, which it is able to use to gain access to information that most people would consider private.

---

[127] Amazon.com Privacy Notice, http://www.amazon.com/gp/help/customer/display.html/ref=footer_privacy/181-3755122-6051147?nodeId=468496 (last visited Dec. 3, 2009).

[128] Picker, *supra* note 112, at 3 ("Banks, cable companies, phone companies—even your local video store—face strong restrictions on how they can use the information seen as they process many of our transactions. Laws disable them—wholly or partially—from using that information.").

[129] *Id.*

1. Asking Third-Parties

Under current law there are limited protections from disclosure of stored communications to the government. Under the Electronic Communications Privacy Act, a warrant is required to access electronic communications in storage.[130] However, those communications are only protected for 180 days; after that point, the government can subpoena communications and delay notice of their search and seizure for three months, with indefinite extensions.[131] Thus the government may be granted access to a user's documents stored in a cloud computing system if the documents are nothing more than "relevant and material to an ongoing criminal investigation."[132] Futhermore, in a recent case, a court held that the notice requirement for stored communications is satisfied by notifying only the ISP and not the user.[133] If a user has shifted their computing experience completely into "the cloud," such a government action would destroy the very protections that the Fourth Amendment was designed to provide: namely, unfettered

[130] 18 U.S.C. § 2703(b)(1)(B) (2006). In *United States v. Perrine*, a Yahoo! chat room user reported to police that another user had sent him videos containing child pornography. 518 F.3d 1196, 1199 (10th Cir. 2008). After reviewing a log of the chat room conversation, the police officers sought and received a disclosure order directed at Yahoo! requiring the disclosure of subscriber information for the user; the officers then used that information to get a disclosure order for the Internet Service Provider associated with the user's IP address. *Id.* at 1199–1200. The Tenth Circuit held that a police officer's affidavit describing his conversation with the reporting user and that he had read the chat room log was sufficient to meet the "specific and articulable facts" standard required by the ECPA. *Id.* at 1203–04.

[131] 18 U.S.C. § 2705(a)(1)(B) (2006).

[132] 18 U.S.C. § 2703(d) .

[133] *In re* United States, 2009 WL 3416240 (D. Or. 2009). The court held that the federal rules of criminal procedure apply to warrants issued under 18 U.S.C. § 2703(a), and therefore officers executing those warrants need only give notice to the person from whom the property was taken. *Id.* at 5; *see* Fed. R. Crim P. 41(f)(1)(C).

access to the user's personal papers for nothing more than a generalized search.[134]

Some statutes are more restrictive. For example, the Right to Financial Privacy Act prevents the government from accessing "copies of, or the information contained in the financial records" of a financial institution's customers.[135] Furthermore, while this Act too has a provision for an administrative subpoena, the subpoena must be served on the customer, and the customer has ten to fourteen days to object.[136] These scenarios, however, assume that the government attempts to gain access to a user's communications directly.

2. Third-Parties Volunteering

In many cases, the government will not need to ask for the information involved. Instead, third-parties will volunteer it after conducting their own searches. As discussed above in Part II.C, Federal Express has contacted the government when searches conducted by its employees have revealed contraband.[137] Similarly, the United Parcel Service conducts regular searches of its packages, and notifies the government when even non-contraband is transported.[138] Cooperation may occur even when there are

---

[134] Furthermore, courts have held that "violations of the ECPA do not warrant exclusion of evidence," because the rule itself provides for remedies in § 2707. Perrine, 518 F.3d at 1202 (citing United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003); United States v. Smith, 155 F.3d 1051, 1056 (9th Cir. 1998); Bansal v. Russ, 513 F. Supp. 2d 264, 282–83 (E.D. Pa. 2007); United States v. Sherr, 400 F. Supp. 2d 843, 848 (D. Md. 2005); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000)).

[135] 12 U.S.C. § 3402 (2006).

[136] *Id.* § 3405.

[137] *See supra* Part II.C.1.

[138] United States v. Parker, 32 F.3d 395, 397 (8th Cir. 1994) (UPS found $4000 cash during a regular inspection of a package insured for more than $1000. UPS contacted the DEA, which asked UPS to deliver the package and notify them again if a return package was received); United States v. Livesay, 983 F.2d 135, 136 (8th Cir. 1993) ($3200 cash found during a search for hazardous chemicals).

no such policies: when a computer repair company employee observed child pornography on the computer of one of his customers, he contacted law enforcement.[139] Finally, there is evidence of third-party volunteerism as far back as the Civil War and World War II, when Western Union "forwarded copies of all international cables to U.S. intelligence operatives."[140]

In the modern era, it is entirely likely that a company like Google would be willing to volunteer similar information. When DoubleClick, a company that marketed advertisements based on users' browsing habits, announced plans to combine its vast database with that of other companies it had acquired, privacy advocates and negative publicity brought down the intended information coup.[141] However, Google has since purchased DoubleClick and it is able to combine all of the information DoubleClick had acquired with the immense amount of information Google

[139] United States v. Hall, 142 F.3d 988, 995 (7th Cir. 1998) (holding that the employee's search was not conducted as a government agent, and therefore the Fourth Amendment was inapplicable).

[140] Michaels, *supra* note 13, at 914 ("This partnership, dubbed Operation Shamrock, outlasted the war by approximately thirty years, over which time the government reviewed countless confidential diplomatic and military dispatches, as well as personal and business communiqués. Once publicly exposed in the 1970s, Operation Shamrock was brought to an abrupt end." However, "[t]he Western Union-government partnership is evidently back in business.").

[141] Andrea Petersen, *DoubleClick Reverses Course After Privacy Outcry*, WALL ST. J., Mar. 3, 2000, at B1 (describing DoubleClick's decision in the context of a Federal Trade Commission probe, a lawsuit, which was eventually dismissed, and a general "firestorm" about Internet privacy); *see also In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001) (granting a motion to dismiss a class action in which the plaintiffs claimed violations of (1) 18 U.S.C. § 2701, et seq. (2006); (2) 18 U.S.C. § 2510, et seq. (2006); (3) 18 U.S.C. § 1030, et seq. (2006); (4) common law invasion of privacy; (5) common law unjust enrichment; (6) common law trespass to property; and (7) §§ 349(a) and 350 of Article 22A of the New York General Business Law).

possesses about search habits, e-mail, and other documents stored in its "cloud."[142]

When a user signs up for a Google account, he signs Google's Terms of Service, which include an agreement "to the use of [his] data in accordance with Google's privacy policies."[143] Those policies may be changed by Google at any time, and the current policy states that Google shares information to "satisfy any applicable law, regulation, legal process or enforceable *governmental request*," or to "protect against imminent harm to the rights, property or safety of . . . the public as required or *permitted* by law."[144]

---

[142] *See* Letter to FTC Chair Deborah Platt Majoras from Mindy Bockstein, Chairperson and Executive Director, State of New York, State Consumer Protection Board regarding "Double Click Inc. and Google Inc. Merger" (May 1, 2007) ("The combination of DoubleClick's Internet surfing history generated through consumers' pattern of clicking on specific advertisements, coupled with Google's database of consumers' past searches, will result in the creation of 'super-profiles,' which will make up the world's single largest repository of both personally and non-personally identifiable information."), *available at* http://www.epic.org/privacy/ftc/google/CPB.pdf.

[143] Google Terms of Service, http://www.google.com/accounts/TOS (last visited Dec. 3, 2009); *see also,* Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commerical Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595, 621–622 (2004) ("[S]ome private businesses have crafted 'law enforcement-friendly' policies that exploit the Miller case in order to provide data to government. In a closed-door conference in February 2003, eBay, the world's largest Internet auction site, revealed that it had crafted its privacy policy to maximize efficiency in responding to law enforcement requests for personal data. eBay described in detail how the company 'is willing to hand over everything it knows about visitors to its web site that might be of interest to an investigator.' eBay's Joseph Sullivan, director of the company's Law Enforcement and Compliance Department, specified that law enforcement only need to ask for the information they wish to obtain: 'There's no need for a court order.'").

[144] Google Privacy Policy, http://www.google.com/intl/en/privacypolicy.html (emphasis added) (last visited Dec. 3, 2009).

On the other hand, in 2006, Google resisted a request by the Department of Justice to turn over its records of the search queries of its users. The DOJ's purported purpose was to enforce the Child Online Protection Act, which was subsequently held an unconstitutional

Furthermore, Google makes no apology for the fact that it shares "aggregated, non-personal information,"[145] which is so well indexed that in 2008 it boasted that based on its users' searching habits, it could determine when a flu outbreak occurs nearly as accurately as the United States Centers for Disease Control.[146] If such non-personal information was

---

restriction of free speech, and many of Google's competitors (Yahoo!, Microsoft, and America Online) acquiesced to the request. Google, however, resisted and forced the DOJ to file a motion to compel. Katie Hafner & Matt Richtel, *Google Resists U.S. Subpoena of Search Data*, N.Y. TIMES, Jan. 21, 2006, at C1, *available at* http://www.nytimes.com/2006/01/20/technology/20google.html. The trouble is, as Professor Timothy Wu points out, "By asserting its power over search engines, using threats of force, the government can directly affect what the Internet experience is. For while Google is fighting the subpoena, it's clear that if they lose, they will comply." *Id.*

In the end, Judge Ware of the Northern District of California did grant the DOJ's motion to compel in part:

> Google is ordered to . . . develop a protocol for the random selection . . . of a listing of 50,000 URLs . . . on the following conditions: 1. . . . Google shall not be required to disclose proprietary information with respect to its database; 2. . . . The Government shall pay the reasonable cost incurred by Google . . . ; 3. Any information disclosed in response to this Order shall be subject to the protective order in the underlying case; To the extent the motion seeks an order compelling Google to disclose search queries of its users the motion is DENIED.

Gonzales v. Google, Inc., 234 F.R.D. 674, 688 (N.D. Cal. 2006). While it is laudable that Google attempted to resist the DOJ's request, the issue would not have been nearly as concerning to privacy advocates had Google not maintained its users' records with such specificity and for such a lengthy time. In addition, Google does not always resist the government. In a recent case it was revealed that after Google had informed law enforcement that they could not produce a user's e-mail, and the government had proceeded to trial without them, Google contacted law enforcement on the eve of trial with a copy of the user's account as it existed two years before. United States v. Cioffi, No. 08-CR-415, at 5 (E.D.N.Y. 2009).

[145] Google Privacy Policy, *supra* note 145.

[146] *See* Miguel Helft, *Google Uses Searches to Track Flu's Spread*, N.Y. TIMES, Nov. 12, 2008, at A1 *available at* http://www.nytimes.com/2008/11/12/technology/internet/12flu.html.

used by the government in a pattern-matching search, the government could then use a subpoena or warrant to force Google to provide the corresponding personal information. Imagine what a similar company could do if instead of merely seeing the information shared by its users with its own online interface, it could see everything they do on the Internet—for example, ISP-side advertisers like NebuAd, Phorm and FrontPorch.

C. Fourth-Party Acquisition and Analysis of User Information

> *LexisNexis is committed to . . . protecting individual privacy rights. In recognition of this commitment, LexisNexis has adopted the LexisNexis Data Privacy Principles. . . . LexisNexis reserves the right to not apply its Data Privacy Principles . . . upon request of law enforcement . . .*
>
> — LexisNexis[147]

Thus far, I have only described situations where the government either requests information from or is volunteered information by third-parties. There is, however, another way the government is able to acquire information about "the people." It does so through the use of private companies that aggregate and analyze data *on behalf of* the government: the so called fourth-parties. One group of these private companies, including LexisNexis, ChoicePoint, and Acxiom, maintain private databases of personal information that, unlike the third-parties discussed above who garner people's personal data within their own system as "a byproduct of the exchange of goods and services," are acquired from an assortment of public and private sources.[148] A second group, which includes Science Applications International Corporation, takes the personal data acquired

[147] LexisNexis Data Privacy Principles, http://www.lexisnexis.com/privacy/data-privacy-principles.aspx (last visited Dec. 3, 2009).

[148] *See* Michaels, *supra* note 13, at 917–18.

by LexisNexis and Acxiom and analyzes it for the government.[149]

Today, data aggregators are able to cross-index various sources of information to produce incredibly extensive—and invasive—lists for practically any purpose.[150] For example, many can "provide lists of people who take Prozac for depression, believe in the Bible, gamble online, or buy sex toys. Another outfit maintains a 700,000-name list called 'the Gay America Megafile.'"[151] These lists are compiled using unlisted telephone numbers; retailer reports of those admitting or convicted of shoplifting; birth, death, marriage, and divorce records; child custody orders; registrations for boats, aircrafts, and automobiles; E-ZPass, criminal, and credit-card records; arrest warrants; concealed-weapons and hazardous-materials handling permits; eviction notices; appliance warranty cards; insurance claims; Social Security numbers; book purchases; and employment histories.[152]

---

[149] *See* SAIC: Services and Products, http://www.saic.com/business/ (last visited Dec. 3, 2009).

[150] How did this happen? In his book, NO PLACE TO HIDE, Robert O'Harrow, Jr. traces the history of these companies from their early inception to the present. He points out that, "Almost everyone you do business with collected information about you, sold it to someone else, or sifted it for their own mercantile ends. In some cases, you eagerly sought out the benefits and conveniences they offered in exchange for your information." This information was used by companies such as retailers, banks, and drug companies to focus their direct mail campaigns, as well as to target individuals who might be more inclined to use the companies' services, as well as to screen people for jobs and track down debtors. "By now those bargains are being transformed, usually without your input, into a public-private security infrastructure, the likes of which the world has never seen." O'HARROW, *supra* note 1, at 6, 37.

[151] Paul Magnuson, *They're Watching You*, BUS. WK., Jan. 24, 2005. The "Gay America Megafile" is just one of the many lists in the *SRDC Direct Marketing List Source*, which contains information about people's reading and buying habits, including the books they buy, the magazines they read, and the cars they own. Other lists include the users of Prozac, online gamblers, sex toy purchasers, the religious, and political donors. O'HARROW, *supra* note 1, at 47.

[152] *Id.*; Robert O'Harrow, Jr., *In Age of Security, Firm Mines Wealth of Personal Data*, WASH. POST, Jan. 20, 2005, at A1; Shane Harris, *FBI,*

In 2007, the United States government's intelligence budget was $43.5 billion—not including military services.[153] Just one federal intelligence agency spent over $1 billion paying private contractors to "conduct core intelligence tasks of analysis and collection over [a period of] five years."[154] As Peter Swire, former Clinton advisor and law professor at Ohio State University's Mortiz School of Law, has said: "After 9/11 we have seen the rise of the security-industrial complex"[155] which involves public security agencies, such as the Department of Homeland Security, creating relationships with private industry to sell citizens' information to the government. In addition, the government is funding companies that conduct "open source intelligence," which involves tracking publicly available information—for

Pentagon Pay for Access to Trove of Public Records, NAT'L JOURNAL, Nov. 11, 2005. In addition, information aggregators receive data from retailers, financial institutions (including banks), direct marketers, mail-order companies, banks, credit card companies, automobile manufacturers, telephone companies, drugmakers, and computer software and hardware companies. O'HARROW, *supra* note 1, at 43. Other sources include telephone directories, warranty cards, catalogue buyer behavior information, and product registration forms. *Id.* at 51–52. In one instance, Merck & Co. used a booklet about heart disease promoted by former football player and coach of the Denver Broncos and Atlanta Falcons Dan Reeves to draw in potential customers. To get the booklet, callers were asked to provide their names, addresses, and information about their "age, health history, insurance coverage, and smoking and exercise habits—all of which went into a database." *Id.* at 51–52.

[153] Mark Mazzetti, *$43.5 Billion Spying Budget for Year, Not Including Military*, N.Y. TIMES, Oct. 31, 2007, *available at* http://www.nytimes.com/2007/10/31/washington/31intel.html?_r=1&oref=slogin.

[154] Walter Pincus, *Defense Agency Proposes Outsourcing More Spying*, WASH. POST, Aug. 19, 2007, at A3. In 1998, it was revealed that Image Data, a company involved in adding photographs to the existing profiles of American consumers, had received nearly $1.5 million in federal funds and technical assistance from the U.S. Secret Service. O'HARROW, *supra* note 1, at 66–67. In 2000, ChoicePoint, described *infra* Part III.C.1., had an $8 million contract with the Justice Department, and another for $8–12 million with the IRS. SOLOVE, *supra* note 1, at 169.

[155] Paul Harris, *How US Merchants of Fear Sparked a $130bn Bonanza*, THE OBSERVER, Sept. 10, 2006.

example, blog posts, twitter feeds, Facebook accounts, and YouTube videos.[156]

1. ChoicePoint, a LexisNexis Company

One such company, ChoicePoint, which was recently acquired by the UK-based Reed Elsevier Group and merged into the LexisNexis Risk & Information Analytics group,[157] was originally a part of Equifax, a credit reporting company.[158] Its original mission was to sell credit data to the insurance industry, but over the years "[it] became an all-purpose commercial source of personal information about Americans, with billions of details about their homes, cars, relatives, criminal records and other aspects of their

---

[156] *See* Noah Shachtman, *Exclusive: U.S. Spies Buy Stake in Firm That Monitors Blogs, Tweets*, WIRED, Oct. 19, 2009, http://www.wired.com/dangerroom/2009/10/exclusive-us-spies-buy-stake-in-twitter-blog-monitoring-firm/ (reporting that In-Q-Tel—a venture capital firm wholly owned by the CIA—has invested an undisclosed sum in Visible Technologies, a software firm specializing in the monitoring of "social media").

[157] ChoicePoint was acquired on September 19, 2008. *See* About ChoicePoint, http://www.choicepoint.com/about/overview.html (last visited Dec. 3, 2009). This merger is of particular concern as it means that ChoicePoint and LexisNexis will be able to merge their databases together and further their cross-indexing of every aspect of people's lives. However, it is not the first company that LexisNexis has assimilated. In 2004, Seisint, discussed *infra* note 210, was acquired for $775 million in cash. O'HARROW, *supra* note 1, at 124.

[158] Bob Sullivan, *Selling 'Insurance' After the ID Theft Flood*, MSNBC, Mar. 21, 2005, http://www.msnbc.msn.com/id/7231738/. Even before ChoicePoint, Equifax was a major force in information gathering: "It had some seven thousand investigators who compiled information on some 45 million adults. . . . One credit report, for instance, described a retired Army lieutenant colonel as 'a rather wild-tempered, unreasonable, and uncouth person who abused his rank and wasn't considered a well-adjusted person.'" O'HARROW, *supra* note 1, at 41. In addition, Equifax and other companies like it worked with "banks, retailers, landlords, car dealerships, and an array of other enterprises" to collect information about American consumers. *Id.* at 76.

lives .... transforming itself into a private intelligence service for national security and law enforcement tasks."[159]

By 2005, ChoicePoint was a "national data and analysis clearinghouse" with 50,000 clients, including the CIA, FBI, Justice Department, and Defense Department.[160] ChoicePoint's government contracts range from solving a series of rapes[161] to working with the FBI's Foreign Terrorist Tracking Task Force.[162] The work with the task force is particularly interesting because the task force was set up to locate and track foreign terrorists and their supporters in the United States, but government agencies "can't maintain records of U.S. persons without opening an official investigation," so the task force "relie[d] on ChoicePoint to augment the intelligence that the government collect[ed] through legal channels."[163] Specifically, the FBI had an "urgent need to acquire high-volume public record data."[164]

In 2003, the government requested Internet-based services, which allowed the government to connect to ChoicePoint's databases directly through their desktop computers; a product designed to locate "people and assets", and a service that listed personal information, including pilot licenses, about an individual or his known associates and

---

[159] O'HARROW, *supra* note 152. ChoicePoint grew by acquiring other companies, including companies making use of credit reports, and demographic and lifestyle records. O'HARROW, *supra* note 1, at 131. Later, it acquired a drug testing company, employee screening businesses, and eventually a private forensic DNA laboratory. *Id.* at 131–32. These were just the beginning, however: ChoicePoint began working with retailers, such as Target and the HomeDepot, to set up a database of employees who had stolen from their stores because most of these thefts do not end up in public criminal records and the retailers wanted a method by which they could blacklist those convicted of shoplifting (as well as those referred to the authorities but not prosecuted). *Id.*

[160] *Id.*; *see also* S. HARRIS, *supra* note 152.

[161] O'Harrow, *supra* note 152.

[162] S. Harris, *supra* note 152.

[163] *Id.*

[164] *Id.* (quoting FBI contract documents acquired through a Freedom of Information Act request).

relatives.[165] One such website allows the government to "obtain a comprehensive dossier on almost any adult."[166] Additionally, in the post-9/11 era, ChoicePoint created a special system for identifying terrorism suspects.[167]

ChoicePoint executives consider the company to be a private intelligence agency doing the government's spying[168] by "gathering data, [and] applying analytics."[169] Government agents, however, admit that, unlike the government, private companies like ChoicePoint are able to conduct searches and collect information without the restrictions that would bind a government intelligence agency.[170] The large amount of cooperation between ChoicePoint and the government raises serious questions about whether ChoicePoint's searches can legitimately be considered private, and whether ChoicePoint has, in fact, become an agent of the government.

This problem is aggravated by the revolving door to employment between the highly regulated government intelligence agencies and ChoicePoint's largely unregulated "private intelligence agency."[171] In late 2003, ChoicePoint

---

[165] *Id.*

[166] Hoofnagle, *supra* note 143, at 595–96.

[167] Another company generated a list of individuals with a "High Terrorist Factor," and 1200 names of people they deemed to be the biggest threats. O'HARROW, *supra* note 1, at 102.

[168] P. Harris, *supra* note 155.

[169] O'Harrow, *supra* note 152.

[170] *See id.* ("Pasquale D'Amuro, an assistant director at the FBI and head of its New York office . . . expressed qualms about whether ChoicePoint and other information services operate with enough supervision. 'There are all kinds of oversight and restrictions to the federal government, to Big Brother, going out there and collecting this type of information,' he said. 'Yet there are no restrictions in the private sector to individuals collecting information across this country, which potentially could be a problem for the citizens of this country.'").

[171] It is unclear how President Obama's Executive Order regarding Ethics Commitments by Executive Branch Personnel will affect potential lobbying activities, but one is reminded of the old adage "money and politics is like water on cement, it finds every crack." Furthermore, Section 3 of the Order provides for waiver particularly in "exigent circumstances relating to national security." Exec. Order No. 13490, 74

hired William P. Crowell Jr., former deputy director of the National Security Agency; Dale Watson, former FBI executive assistant director of counter-terrorism and counterintelligence; and Viet D. Dinh, former assistant attorney general and primary author of the USA Patriot Act, as homeland security advisors.[172] Furthermore, ChoicePoint was one of the clients of former Attorney General John Ashcroft's lobbying firm.[173] This relationship was forged immediately after Ashcroft secured the company a $67 million no-bid contract.[174]

2. Science Applications International Corporation

SAIC provides private analysis to the government, often using data collected by companies like ChoicePoint. For example, in 2006, SAIC developed a service bureau called ADAM ("Automated Data Analysis and Mining"), which used data from the "electronic data-warehouses of ChoicePoint" and ran searches against the data.[175] SAIC claimed: "ADAM

C.F.R. 4673 (2009), *available at* http://www.usoge.gov/laws_regs/exec_orders/eo12834.html (last visited Dec. 3, 2009).

[172] *See* O'Harrow, *supra* note 152. In addition, Jeff Jonas, whose company Systems Research & Development received millions of dollars from the Central Intelligence Agency's private not-for-profit In-Q-Tel, and who himself was an advisor at the Homeland Security Department, the Defense Department, and other intelligence agencies, was a major player with ChoicePoint thanks to his analytical software program, NORA (Non-Obvious Relationship Awareness). O'HARROW, *supra* note 1, at 145–46. Interestingly, there are some that argue that because In-Q-Tel's CEO and founder sat on the board of a venture capital trade association with the managing partner of one of venture capital firms funding Facebook, Facebook is working with or for the CIA. *See Facebook a CIA Front?*, AboveTopSecret.com, July 14, 2007, http://www.abovetopsecret.com/forum/thread291893/pg1.

[173] P. Harris, *supra* note 155.

[174] Greg Palast, *Will The Gang That Fixed Florida Fix the Vote in Caracas this Sunday*? COMMONDREAMS.ORG, Aug. 11, 2004, http://www.commondreams.org/views04/0811-02.htm.

[175] SAIC: Data Mining & Data Warehousing: Data Analysis, http://web.archive.org/web/20060209120733/www.saic.com/datamining/data-analysis.html (last visited Dec. 3, 2009).

provides clients with the ability to obtain and analyze enormous amounts of data to create explicit profiles of target groups and collect critical data on each of the individual members of that group."[176] Today, SAIC offers a product called Pathfinder, which is "extensively used for data mining and knowledge discovery."[177] SAIC states that the program is being used in traditional military intelligence, as well as in "[i]nformation warfare, computer forensics, law enforcement investigative case management, terrorism link analysis, litigation support, and financial investigations and money laundering."[178] In 2002, SAIC was chosen by the NSA to build a tool to discover national threats from within the collection of worldwide communications.[179]

Like ChoicePoint, SAIC also has a revolving door to employment with the government agencies it works with.[180] The San Diego, California based company is generally known as "NSA West," and does two-thirds of its work for the federal government. The SAIC board has included Bobby Ray Inman, former NSA director; John M. Deutch, former CIA director; Melvin R. Laird and William J. Perry, former Defense Secretaries; and Robert M. Gates, former CIA director and current Secretary of Defense.[181]

---

[176] *Id.*

[177] SAIC: Products: Software: Pathfinder, http://www.saic.com/products/software/pathfinder/ (last visited Dec. 3, 2009).

[178] *Id.*

[179] Siobhan Gorman, *Little-known Contractor Has Close Ties with Staff of NSA*, BALTIMORE SUN, Jan. 29, 2006, at 13A.

[180] *Id.*

[181] *Id.* In one case, however, the NSA did take actions to minimize the appearance of a conflict of interest. When William B. Black Jr. retired from the NSA's cryptologic executive service, he became an SAIC assistant vice president. When he was called back to the NSA, he sold his SAIC stock and "recused himself for a year from 'involvement in any matter affecting the financial interests' of the company." Gorman, *supra* note 179. Black's recusal once returning to the NSA may be of little comfort, because during his three years with SAIC he was likely able to steer the company toward producing products and gathering information that the NSA wanted. *See id.* (quoting an SAIC executive vice president: "We do a much

3. Data Laundering and Lack of Sanctions

A major concern with these two companies and those like them is that, as individuals move back and forth between government intelligence positions and positions in the private sector, these individuals are able—and have a monetary incentive—to direct their private employers to "independently" conduct searches that could not be conducted by government agencies. Therefore, ChoicePoint can situate itself between third-parties and the government and pass information, otherwise restricted by the Constitution or statutes, between the two. In other words, ChoicePoint makes itself quite useful by building a database of stored communications and other information that *might* be useful should the government *happen* to want to see them.

Related to the current legislative and judicial regimes, which fail to establish rules against this kind of data acquisition and laundering, is the lack of realistic sanctions in the foreign intelligence arena. In the Fourth Amendment context, the method of deterrence is generally exclusion at trial, but for this to have a deterrent effect the government must actually intend information to be used at trial. If the government merely uses the information in an intelligence setting, there may be no reason to have a trial, [182] or any evidence discovered may be laundered and used to get the requisite warrant.[183]

---

better job for our customers if we have people in the company who really know the customers.").

[182] *See* Matthews, *supra* note 140, at 925–26 ("In the counterterrorism context, where criminal prosecutions are rare and generally take a back seat to national-security investigations and military detentions . . . there is no comparable built-in mechanism for deterring officials from engaging in unreasonable practices."). In fact, the Federal Bureau of Investigation has stated that it recognizes differences between the requirements involved with foreign intelligence information and those involved with criminal prosecutions. *See* FBI Memorandum, *supra* note 103, at 3, n.7.

[183] *Id.* at 930 ("Government agents who receive intelligence through, for example, warrantless eavesdropping, have reportedly funneled that information back through the proper, formal channels. These agents may

In conclusion, since the drafting of the Fourth Amendment, there have been radical changes in the way that people retain their papers and effects which makes them susceptible to government searches in a way that no one at the Framing could have seen possible. Furthermore, the judicial determinations concerning the limited scope of Fourth Amendment protection have left citizens with little in the way of privacy from, not only government working directly with those who are trusted with their data, but also the fourth-party data aggregators and analyzers who are able to extract, re-assemble, and search their data with impunity. Part IV describes ways in which the judiciary and the legislature can protect those whom they are supposed to serve from these attacks on individual privacy.

IV. SALVAGING THE SITUATION

The relationship between third- and fourth-parties and the government allows law enforcement to obfuscate both federal statutes and the clear intent of the framers of the Fourth Amendment. This is a grave issue, but privacy advocates have thus far been unable to suggest a new legal regime that would adequately protect people from the government's intrusions. Section A discusses general commentator proposals on how to cope with the third-party disclosure doctrine in a digital world. Then, section B proposes a solution to target the insecurity created by the agreements between fourth-parties and the government.

---

have reused the information to obtain faster FISA authorization . . . or, the laundering may be done to re-run the same search, this time with the requisite court order in place."); *see also* Kim Zetter, *NSA-Intercepted E-Mails Helped Convict Would-Be Bombers*, WIRED, Sept. 8, 2009, *available at* http://www.wired.com/threatlevel/2009/09/nsa-email/ (last visited Dec. 3, 2009) (describing e-mails intercepted by the United States National Security Agency that were divulged to the British government, but not used to convict their authors in British trials related to an attempt to bomb several transcontinental flights).

A. General Proposals

> *The mere possibility that unwelcome meddlers might open and rummage through the containers does not negate the expectation of privacy in their contents any more than the possibility of a burglary negates an expectation of privacy in the home; or the possibility of a private intrusion negates an expectation of privacy in an unopened package; or the possibility that an operator will listen in on a telephone conversation negates an expectation of privacy in the words spoken on the telephone. What a person . . . seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.*
>
> — Justice William J. Brennan[184]

One viable solution is to have Congress define places where individuals have reasonable expectations of privacy.[185] However, courts have consistently found that statutes protecting privacy do not automatically provide for such an expectation,[186] and even if a statute were to explicitly provide for such an expectation, there is no guarantee that the Supreme Court would endorse Congress's legislative findings.[187] It is, however, possible that if Congress were to lay out fundamental areas where they believed people should have a reasonable expectation of privacy, and people started to expect that privacy, the courts would have no choice but to concede that a subjective belief in that privacy had been created.[188] Then again, the third-party disclosure doctrine

---

[184] California v. Greenwood, 486 U.S. 35, 54 (1988) (Brennan, J., dissenting) (citation omitted).

[185] *See supra* Part II.D.

[186] *Id.*

[187] *See* Kamin, *supra* note 23, at n.210 (discussing the Supreme Court's overturning of Congress's interpretation of the Commerce Clause). On the other hand, a constitutional amendment establishing the right to privacy would force the courts to respect statutes passed by Congress in furtherance thereof.

[188] Such a statute would need to be passed by Congress, because the states are unable to do so by virtue of the Supremacy Clause. However,

might still counsel against such an interpretation,[189] and if a court found the search to be a private one, it would still negate any Fourth Amendment protections established.

Jon D. Michaels advocates a different legislative solution. He would require companies to inform Congress whenever they disclose information to law enforcement, with failure to do so penalized and compliance providing immunity from later lawsuits.[190] Such a system would set up third-parties as government watchdogs who would have incentives to betray not only their consumers, but also the government agencies they work with. On the other hand, such a system would leave enforcement in the hands of Congress, which has traditionally been anemic when battling the Executive on intelligence-gathering matters. Furthermore, given the mass of background dealings between third- and fourth-parties and the government, and between third-parties and fourth-parties with each other, it seems unlikely that even if disclosure were to occur Congress would be sufficiently able to analyze the swarms of data for potential privacy violations.

A judicial alternative would be to recognize that *Katz* has outlived its usefulness and to abandon it.[191] In abandoning the "assumption of risk"-based reading of the Fourth Amendment, however, the Supreme Court would need to adopt a new interpretation. One option would be to concede Justice Scalia's complaint in *Minnesota v. Carter*,[192] and return to a textual reading of the Fourth Amendment as applied in *Olmstead*.[193] Such a reversal, however, seems unlikely given the vested interests in maintaining a doctrine

---

Kamin argues that if the states were to pass such statutes, the statutes should be included in any *Katz* analysis. *Id.* at 142–43.

[189] *See supra* Part II.B.

[190] *See, e.g.*, Michaels, *supra* note 13.

[191] *See* Kamin, *supra* note 23, at 137–38.

[192] 525 U.S. 83, 92–93 (1998) (Scalia, J., concurring). *See* discussion *supra* note 35 and accompanying text.

[193] 277 U.S. 438 (1928).

that merely turns on convincing a majority of the Supreme Court that your vision of privacy is the reasonable one.[194]

Instead, Sam Kamin advocates a more promising approach. He argues that the Supreme Court should overturn the third-party disclosure doctrine and instead focus on the actual expectations that society has developed for its privacy, which can be determined with "survey research, public referenda, and [the public's] actual practices:"[195]

> Had the Court applied these "everyday expectations of privacy" to the Miller and Smith cases, the result would likely have been very different. For example, the Court might reasonably conclude from the fact that nearly all people with the means to do so keep their money in bank accounts that they reasonably expect their privacy in their banking information to be respected.[196]

Sam Kamin, however, did not address the problem of fourth-parties, and his solution would be insufficient on its own, because even if the Fourth Amendment protection was determined based on one's subjective expectation of privacy, a fourth-party's search and aggregation would permit government access under current doctrine.[197]

Not all scholars, however, believe that the third-party doctrine has outlived its usefulness. Orin Kerr recently argued that although the third-party doctrine is "widely criticized as profoundly misguided"[198] and "decisions applying the doctrine 'top[] the chart of [the] most-criticized fourth amendment cases,' "[199] the doctrine serves two important purposes: (1) preserving technological neutrality, and (2)

---

[194] *See supra* Part II.A.

[195] Kamin, *supra* note 23, at 140.

[196] *Id.* at 139–40.

[197] *See supra* Part II.C.

[198] Kerr, *supra* note 52, at 563.

[199] *Id.* at 563–64; *see id.* at n.5 ("A list of every article or book that has criticized the doctrine would make this the world's longest law review footnote.").

providing ex ante clarity.[200] To support his claim that the doctrine must exist to preserve technological neutrality, Kerr argues that the rule ensures that a criminal receives "the same degree of privacy protection regardless of whether [she] commits crimes on her own or uses third-parties."[201] His argument, however, does not account for the fact that by observing the public activities of third-parties, police can, in most cases, solve the same percentage of crimes that they would have solved had the criminal committed the crime herself.[202] He uses *Smith*[203] and *Miller*[204] as examples to substantiate his argument, but in *Smith*, law enforcement could just have easily monitored the recipient of the harassing phone calls;[205] in *Miller*, the prosecutors used bank records that would not have existed had the transaction been conducted in cash. Had the authorities monitored the exchange of the check instead of using the bank records, they

[200] *Id.* at 564–65.

[201] *Id.* at 577.

[202] Kerr asks the reader to "[c]onsider how a person might use third parties to commit crimes from the protection of his own home. A mob boss might summon his underlings to his house to give them orders. A stalker might call his victim on his home phone rather than lying in wait outside the door. A computer hacker might hack into computers thousands of miles away without leaving his bedroom." *Id.* at 576. However, in all of these hypotheticals, the third-parties' actions are easily observable by law enforcement. The underling can be monitored when he leaves the house to carry out orders. The stalker's victim might permit law enforcement to access the records on her own phone. The computer hacker's activities can be logged by the computers of his victim. Without the third-party doctrine, observation must occur differently, but it can occur. Furthermore, one could argue that, without the third-party doctrine, in none of the situations described by Professor Kerr does the first-party maintain a subjective expectation of privacy under *Katz*: the underling moves around in public, and the stalker and hacker make connections with individuals with whom they do not have a relationship of trust.

[203] 442 U.S. 735 (1979).

[204] 425 U.S. 435 (1976).

[205] Kerr argues that due to technology Smith no longer needed to leave his home, and that the police needed a pen register to get "the equivalent of the previously public information about what he was doing." Kerr, *supra* note 198, at 578.

would have observed substantially the same public components.[206]

B. Coping with Fourth-Parties

> *There is something terribly wrong with this country . . . . [C]ruelty and injustice, intolerance and oppression. And where once you had the freedom to object, to think and speak as you saw fit, you now have censors and systems of surveillance coercing your conformity and soliciting your submission . . . . Who's to blame? . . . . If you're looking for the guilty, you need only look into a mirror. I know why you did it. I know you were afraid. Who wouldn't be? War, terror, disease. There were a myriad of problems which conspired to corrupt your reason and rob you of your common sense.*
>
> — V for Vendetta[207]

To adequately cork the hole in Fourth Amendment protections with regard to fourth-parties, courts must resolve the difficulties created by the third-party disclosure doctrine and the private-party search doctrine. To achieve this goal, courts should take two steps. First, courts should refuse to treat disclosure to fourth-parties as corrosive to an individual's expectation of privacy, and instead apply the same requirements to the government in accessing the information from a fourth-party as they would from a third-party. Second, courts must recognize that fourth-parties are agents of the government, and as such, their searches cannot be excused by the private party search doctrine.

---

[206] Kerr argues that the checking account replaced a transaction with "substantial public components with a transaction that would normally occur entirely in private." *Id.* at 579.

[207] V FOR VENDETTA (Silver Pictures 2005).

1. Fourth-Party Disclosure Not Corrosive to Privacy

The third-party disclosure doctrine was created in recognition of the fact that when someone discloses something to a confederate, she assumes the risk that her confederate will betray her secrets to the government.[208] This argument need not be applied to fourth-party aggregators who reach out to third-parties for information generally and then later conduct searches that will disclose the third-party's consumers' secrets. Your bank handing your information over to a non-governmental body is completely unlike someone you have shared a secret with turning out to be an informant, and therefore should not disentitle you, the consumer, to your expectations with respect to the government.

Specifically, while someone might be charged with subjectively understanding that her bank records and web searches are in the possession of a third-party, she may not understand that the third-party might pass these records on to a fourth-party. Therefore, the government should not be immunized because it conducts its searches on the fourth-party's databases, unless the user understood in providing the information to the third-party intermediary that the intermediary would disclose the information in the ordinary course of business.[209] Instead, the government should be

---

[208] *See supra* Part II.A.

[209] The court in *Miller* associated the disclosure to a third-party that happens to be an informant with the disclosure to a third-party company that provides your information to the government. United States v. Miller, 425 U.S. 435, 440–42 (1976) (citing Hoffa v. United States, 385 U.S. 293, 301–02 (1966)). As Kate Vershov points out, however, the Court may have failed to appreciate the difference between the expectations one has of an acquaintance and those one has of a business: "Acquaintances may well betray or turn out to be informants, but companies are not acquaintances and it is more reasonable to have concrete expectations about companies, entities which exist by the grace of legal recognition, than it is about acquaintances." Kate Vershov, *US v. Miller and "Voluntary" Data Handover, c. 2009*, COLUM. SCI. & TECH. L. REV., April 20, 2009, http://www.stlr.org/2009/04/us-v-miller-and-voluntary-data-handove

required to get the information itself and provide it to the fourth-party for aggregation, which means that all relevant statutes and protections would be implicated.[210] Alternatively, when the government seeks information from a fourth-party, the government's actions should be treated as if it had gotten the information directly from the third-party.

When a bank customer stores documents in a safe deposit box, he does not lose Fourth Amendment protection even though he has given those documents to the bank and the bank can access them and give them to the government.[211] He should not lose that protection simply because the bank hands his documents to a fourth-party before they reach the government. Likewise, when a third-party intermediary can access documents stored in the cloud, government access should not be sanitized because a fourth-party stands in the breach.[212]

---

r-c-2009. Ms. Vershov also highlights the difference between information provided to someone directly, and information acquired by virtue of being an intermediary. *Id.*

[210] Shortly after the attacks of September 11, 2001, a company called Seisint, Inc. (short for seismic intelligence)—which is partly financed by Equifax and received information from it—created a "surveillance engine" called Matrix (Multi-state Anti-Terrorism Information Exchange). In order to supply Matrix with better identity information, federal prosecutors issued subpoenas for various information, including financial records and credit card activity. O'HARROW, *supra* note 1, at 104, 106–07. Privacy advocates can argue about their concerns with this information being aggregated or with the laws protecting its collection, but by forcing the government to get the information, all of the relevant constitutional and statutory protections, at least initially, retain their effectiveness. One wonders, however, whether once a given investigation has ended, the information gained by government subpoena is disconnected from Matrix.

[211] *See* United States v. First Nat'l City Bank, 568 F.2d 853, 858 (2d Cir. 1977); *id.* at n. 13 (finding that the third-party disclosure doctrine is not dispositive and that a safe deposit box user has a greater "interest in, or expectation of privacy with respect to, the records kept by a bank").

[212] One Sixth Circuit panel felt that even seeking the information from the third-party intermediary in the first place would implicate the Fourth Amendment, unless the intermediary "actually relies on and utilizes [their] access in the normal course of business, sufficient to establish that the user has waived his expectation of privacy with respect to that entity." Warshak v. United States, 490 F.3d 455, 476 (6th Cir. 2007), *rev'd en banc*

Similarly, in *Minnesota v. Olson*, the Court held that an overnight guest retained a legitimate expectation of privacy, because of the "everyday expectations of privacy that we all share."[213] Furthermore, the court found that such a houseguest should only expect his privacy to be disturbed by his host and those that the host allows inside, none of whom would "want[] to see or meet with the guest over the objection of the guest," who himself is entitled to a "legitimate expectation of privacy despite the fact that [he has] no legal interest in the premises and do[es] not have the legal authority to determine who may or may not enter the household."[214] Therefore, "just as the overnight guest is aware of a risk that his host will betray him, yet nonetheless enjoys a reasonable expectation of privacy in another's home, so [a] patron, aware of the . . . risk of betrayal, ought to be

on other grounds, 532 F.3d 521 (6th Cir. 2008) ("It is true . . . that by sharing communications with someone else, the speaker or writer assumes the risk that it could be revealed to the government by that person . . . . The same does not necessarily apply, however, to an intermediary that merely has the ability to access the information sought by the government. Otherwise phone conversations would never be protected, merely because the telephone company can access them; letters would never be protected, by virtue of the Postal Service's ability to access them; the contents of shared safe deposit boxes or storage lockers would never be protected, by virtue of the bank or storage company's ability to access them."). *Contra* United States v. Miller, 425 U.S. 435, 443 (1976) ("[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 confidence placed in the third party will not be betrayed.").

See also ZITTRAIN, *supra* note 18, at 188 ("[T]he happenstance of where data are actually stored should not alone control the constitutional assessment of which standard the government must meet.").

[213] 495 U.S. 91, 98 (1990). Note that *Olson* involved a seizure, and not a search of the defendant's materials. However, the case remains a situation where the Supreme Court recognized an expectation of privacy in a location not controlled by the defendant.

[214] *Id.* at 99.

entitled to a reasonable expectation of privacy in his . . . records."[215]

2. Fourth-Party Searches Not Private

Additionally, courts should recognize that when a fourth-party data aggregator is the source of government information, the fourth-party's acquisition and search of data should be treated as a government action. These companies cooperate with the government in ways that were not imagined by the Court when it created the private party search doctrine.[216] Fourth-parties increasingly seem to act as the government's private intelligence service.[217] Additionally, when the activities of fourth-parties are directed by former members of the very intelligence agencies with which they are working, current members of the government need not request fourth-parties to acquire data, because they know that like-minded individuals inside the companies will direct the companies' surveillance in that direction.

Furthermore, even if the relationship does not initially merit agency status, once the government pays a fourth-party for information, any future information that is provided should be considered tainted. In *United States v. Walther*, the Ninth Circuit found that an airline employee who conducted a search for contraband without a business motive and with the reasonable expectation of receiving a government reward had the requisite intent to be an "instrument or agent" of the government.[218] Furthermore,

---

[215] Kamins, *supra* note 23, at 139–40.

[216] *See supra* Part II.C.; Part III.C.

[217] In 2004, the United States General Accounting Office determined that 52 agencies were using or planning to use data mining, and that 62% of these agencies used personal information and 27% used private sector data. U.S. Gen. Accounting Office, GAO-04-548, *Data Mining: Federal Efforts Cover a Wide Range of Uses* 3 (2004), http://www.gao.gov/new.items/d04548.pdf. Of the programs involving national security and law enforcement, all but four use personal data. *Id.* at 8, 10; *see also supra* Part III.C.

[218] 652 F.2d 788, 792 (9th Cir. 1981).

the court found that the employee's prior experiences with the government provided proof of the government's acquiescence, even though the government had no prior knowledge of this particular search and had not directly encouraged the employee to search the particular bag.[219] Having established these two factors, the court held that "the government cannot knowingly acquiesce in and encourage directly or indirectly a private citizen to engage in activity which it is prohibited from pursuing where that citizen has no motivation other than the expectation of reward for his or her efforts."[220]

When the government agrees to pay fourth-parties billions of dollars in exchange for the information that they can gather and the government cannot, [221] the fourth-party data aggregators, who have no independent business reason for conducting such searches, should be considered instruments of the government for the purposes of Fourth Amendment and statutory analysis. If fourth-parties are treated as agents of the government, their searches could be interpreted as government actions under relevant privacy statutes, and they could not be used to work around statutes such as the ECPA.[222]

3. Counterargument: Legislation

One might argue that the problem of law enforcement gaining access to data through fourth-parties is better resolved by comprehensive legislation passed by Congress. However, Congress has proved incapable or unwilling to pass legislation that would effectively protect against the

---

[219] *Id.* at 793 ("While the [government] had no prior knowledge that this particular search would be conducted and had not directly encouraged [the employee] to search this overnight case, it had certainly encouraged [the employee] to engage in this type of search. [The employee] had been rewarded for providing drug-related information in the past. He had opened [packages] before, and did so with no discouragement from the [government].").

[220] *Id.*

[221] *See supra* Part III.C.

[222] *See supra* Part III.C.3.

disclosure of personal information. As discussed in Part II.D., the Electronic Communications Privacy Act and the Right to Financial Privacy Act both contain loopholes that allow fourth-parties to acquire and launder data for law enforcement.

Even the Health Insurance Portability and Accountability Act ("HIPAA"), which is partly intended to prevent disclosure of health information and which is arguably one of the most comprehensive pieces of privacy legislation, is staggeringly inadequate. HIPAA merely stated that if Congress did not enact privacy legislation before 1999, the Secretary of Health and Human Services would be required to do so,[223] as the Secretary did in 2000.[224] This approach, however, leaves the creation of privacy protections in the hands of the Executive, from whom the information is, at least in part, meant to be kept secret. Although the Privacy Rule that was adopted by HHS provides comprehensive protection, it leaves law enforcement several avenues by which it can gather medical information. These include: (a) requesting information from an exempted public health authority;[225] and (b) in certain

---

[223] Summary of HIPAA Privacy Rule 1 (May 2003), http://www.hhs.gov/ocr/privacysummary.pdf. HIPPA was adopted after a company called Elensys collected prescription records directly from pharmacies. O'HARROW, *supra* note 1, at 69.

[224] Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82,462.01 (Dec. 28, 2000) (to be codified at 45 C.F.R. pt. 160).

[225] 45 C.F.R. § 164.512(b)(1)(i) (2002). "Public health authority means an agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency . . . that is responsible for public health matters as part of its official mandate." 45 C.F.R. § 164.501 (2002). In other words, public health authorities include federal public health agencies, such as the Centers for Disease Control (CDC), the Food and Drug Administration (FDA), the Health Resources and Services Administration (HRSA), the National Institutes of Health (NIH), the Occupational Safety and Health Administration (OSHA), and the Substance Abuse and Mental Health Services Administration (SAMHSA); tribal health agencies; state public health agencies, such as public health departments, state cancer registries, and vital statistics departments; local public health agencies;

situations, requesting the information directly[226]—for example, when law enforcement is conducting lawful intelligence, counter-intelligence, and other national security activities.[227]

In addition to Congress's general reluctance and the Executive's conflict of interest, there is pressure from the fourth-parties themselves to allow them to continue doing business. In 2005, six fourth-party companies spent $2.4 million lobbying Congress; ChoicePoint alone spent $970,000.[228] In addition, former government employees now working for fourth-party companies pressure their former agencies for support.[229]

Given the political and financial reasons not to create legislation to control the activities of the fourth-party companies, it would be more reliable to adopt an interpretation of the Fourth Amendment that leaves the power in the hands of the courts and changes the question from whether the investigation is one that is exempted by statute to whether the investigation violates an individual's expectation of privacy.[230]

---

and anyone performing public health functions under a grant of authority from a public health agency. *See* HIPAA, *HIPAA Privacy Rule and Public Health* (Apr. 11, 2003), *available at* http://www.cdc.gov/mmwr/preview/mmwrht ml/m2e411a1.htm (last visited Dec. 3, 2009).

[226] 45 C.F.R. § 164.512(d)(1) (investigations related to heath care); 45 C.F.R. § 164.512(f) (various law enforcement activities).

[227] 45 C.F.R. § 164.512(k)(2).

[228] Evan Perez & Rick Brooks, *Data Providers Lobby to Block More Oversight*, WALL ST. J., Mar. 4, 2005, at B1, *available at* http://www.rmi.gsu.edu/rmi/faculty/klein/RMI_3500/Readings/Other/Data providers_BlockOversight.htm. Image Data, discussed *supra* note 154, lobbied state and federal legislators through the Rasky/Baerlein Group. O'HARROW, *supra* note 1, at 68.

[229] *See supra* Part III.C.

[230] There may be some question as to judicial competency in this regard, but a case-by-case inquiry is what was originally contemplated in *Katz*, and is the only way to determine whether an individual's expectation of privacy has been invaded, and whether it was an expectation society was willing to recognize as reasonable. *See* 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

If courts consider fourth-party searches government actions and disclosure to fourth-parties not to be corrosive to the people's expectations of privacy, the information that people are forced to share with third-parties in an evolving technological world will be far better secured against government searches and seizures.

V. CONCLUSION

In a world where technology is developing rapidly and the government is applying more scrutiny to every piece of data it can acquire, the focus of privacy advocates must be on both the methods the government uses to acquire data and the uses it can make of that data once acquired. Due to the Supreme Court's jurisprudence, much of the information that a lay person would assume is protected from disclosure to the government is no longer protected by the Fourth Amendment and despite Congress's attempts to prevent such disclosure statutorily, government agents have the information readily at their disposal. Fourth-parties acquire and aggregate information that the government would be unable to collect on its own and deliver it to the government en masse. The government is then able to use this data without ever being asked to show probable cause or even an articulable purpose.

This note has argued that when fourth-parties disclose to law enforcement information generated as a result of searches that would be constitutional violations had the government conducted the searches itself, those fourth-parties' actions should be considered searches by agents of the government, and the data should retain privacy protections. Specifically, it has recommended two changes to Fourth Amendment jurisprudence. First, the government should be required to acquire the information itself and provide it to the fourth-party for aggregation, thereby implicating all relevant statutes and protections, or alternatively, when the government gets information from a fourth-party, that action should be considered as though the government had received the information directly from its source. Second, fourth-parties should be treated as agents of

the government, and their searches should be considered government actions not covered by the private search doctrine.

This proposal limits data acquisition in a way that retains the original intentions of the framers. Had they been aware of the possibility that searching and analyzing the people's papers could be done so efficiently that general searches would be commonplace in criminal and foreign intelligence investigation, there is no doubt that they would be concerned, and rightfully so. Yet, that is exactly what has occurred as the people have moved their information simultaneously into "the cloud" and the government's hands. The Fourth Amendment was originally drafted as an attempt to curb the government's use of general search warrants for contraband. It is consistent with the reasoning behind its drafting to curb the government's general acquisition through the use of fourth-parties of both contraband and non-contraband.