PEPPERDINE UNIVERSITY

Pepperdine Law Review

Volume 34 | Issue 4 Article 10

5-15-2007

Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too

Stephen E. Henderson

Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too

Stephen E. Henderson*

I. INTRODUCTION
II. CURRENT EVENTS
III. RELEVANT FACTORS
- A. *Factor 1. The Purpose of the Disclosure*
- B. *Factor 2. The Personal Nature of the Information*
- C. *Factor 3. The Amount of Information*
- D. *Factor 4. The Expectations of the Disclosing Party*
- E. *Factor 5. The Understanding of the Third Party*
- F. *Factor 6. Positive Law Guarantees of Confidentiality*
- G. *Factor 7. Government Need*
- H. *Factor 8. Personal Recollections*
- I. *Factor 9. Changing Social Norms and Technologies*
- J. *Irrelevant Consideration 1. The Form of the Information*
- K. *Irrelevant Consideration 2. The "Good Citizen" Motivation of a Third Party*
- L. *Irrelevant Consideration 3. The Government's Method of Acquisition*
- M. *Irrelevant Consideration 4. Expectations Created by Police Conduct*

IV. TWO PROPOSALS
V. CONCLUSION

* Associate Professor, Widener University School of Law. Yale Law School (J.D., 1999); University of California at Davis (B.S., 1995). I wish to thank Joshua Dressler, Jules Epstein, Christopher Slobogin, Leonard Sosnov, Joseph Thai, George Thomas, and Eugene Volokh for their comments on a previous draft.

I. INTRODUCTION

For at least thirty years the Supreme Court has adhered to its "third-party doctrine" in interpreting the Fourth Amendment,[1] meaning that so far as a disclosing party is concerned, information in the hands of a third party receives no Fourth Amendment protection.[2] The doctrine was controversial when adopted,[3] has been the target of sustained criticism,[4] and is the predominant reason that the "*Katz* revolution" [5] has not been the revolution many hoped it would be. Some forty years after *Katz* the Court's search jurisprudence largely remains tied to property conceptions.[6] As I have demonstrated elsewhere, however, the doctrine is not the universal constitutional rule in the United States.[7] Eleven states reject the doctrine, providing some constitutional "search and seizure" protection to information in the hands of third parties, and another eleven give some reason to believe they might reject it.[8]

But it is one thing to urge that some third-party information should be protected, and quite another to articulate *how* and *when* different information should be accessible to police. To answer this question it makes sense to turn to the most robust source of practical applications we have, namely the

---

1. The Fourth Amendment of the United States Constitution provides that:

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

U.S. CONST. amend. IV.

2. *See* United States v. Miller, 425 U.S. 435, 437 (1976) (bank records); Smith v. Maryland, 442 U.S. 735, 745-46 (1979) (telephone numbers dialed). The third party retains limited Fourth Amendment rights. *See infra* note 63 and accompanying text. For the sake of brevity this article will often nonetheless assert that under the third-party doctrine there is "no constitutional restraint." Other than in Factor 8, *infra* Part III.H, this paper focuses on the provider of information rather than the third party, the latter of which typically has less interest in restricting dissemination.

3. *See Miller*, 425 U.S. at 447-55 (Brennan, J., dissenting); *id.* at 455-56 (Marshall, J., dissenting); *Smith*, 442 U.S. at 746-48 (Stewart, J., dissenting); *id.* at 748-52 (Marshall, J., dissenting).

4. *See, e.g.*, 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE §§ 2.7(b)-(c) (4th ed. 2004).

5. Katz v. United States, 389 U.S. 347 (1967) (rejecting a trespass conception of the Fourth Amendment and adopting the reasonable expectation of privacy framework).

6. *See* Susan W. Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 MISS. L.J. 1, 31-32, 51 (2005) ("Notwithstanding [*Katz*], the Court has continued to approach Fourth Amendment privacy as if it is nothing more than a spatial concept; what I seclude from others is private, what I fail to shield is not."); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 809-15 (2004) ("Descriptively speaking, the basic contours of modern Fourth Amendment doctrine are largely keyed to property law. . . . Although no one theory explains the entire body of Fourth Amendment doctrine, property law provides a surprisingly accurate guide.").

7. *See generally* Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373 (2006).

8. *Id.* at 395. As explained *infra* notes 278-80 and accompanying text, a recent appellate decision in New Mexico demonstrates that this state should be added to the list of potential rejecters.

jurisprudence of those states that have diverged from the federal doctrine. Although state courts often employ a gestalt approach that defies precise delineation, an analysis of many cases reveals a set of relevant factors that would seem to be consistently useful in determining whether law enforcement access should be restricted, and if so, in what manner. What such analysis does not reveal is a tidy system of bright-line delineations, seemingly at odds with two thoughtful alternatives to the current federal doctrine proposed by Daniel Solove and Christopher Slobogin.[9]

Part II of this article frames the discussion via recent events. The realization that the National Security Agency has been parsing phone conversations, dialing records, and banking records since the terrorist attacks of September 11, 2001, demonstrates that the third-party doctrine is very much a contemporary concern. The decision last term in *Georgia v. Randolph*[10] demonstrates that five members of the Supreme Court are willing to depart from the doctrine, at least in the context of the home. Part III then utilizes the existing state (and to a limited extent federal) jurisprudence to determine and explain what factors are relevant in determining whether to constitutionally restrict law enforcement access. This yields an uncertain calculus that also logically challenges the essentially unrestricted ability of law enforcement to probe the recollection of a recalcitrant witness. In Part IV, I compare my approach to the seemingly more administrable proposals of Professors Solove and Slobogin. I conclude with a tentative defense of the current multi-faceted—and therefore necessarily uncertain—jurisprudence. Although its administrability is imperfect, it more appropriately distinguishes between and among different types and amounts of third-party information, and I advocate its adoption by both state and federal courts.

9. *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE (2004) [hereinafter DIGITAL PERSON]; Christopher Slobogin, *Transaction Surveillance by the Government*, 75 MISS. L.J. 139 (2005). Although Professor Solove is critical of the federal third-party doctrine, he ultimately proposes a legislative solution in his book. SOLOVE, DIGITAL PERSON at 210. However, he has elsewhere defended using the Fourth Amendment to protect against intrusions utilizing technology. *See generally* Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747 (2005). And other than his limiting independent private disclosure his proposal could be urged as a matter of constitutional interpretation. This paper will focus on the Constitution. If the reader is interested in the current statutory constraints on government accessing third-party information, I highly recommend Professor Slobogin's account. *See* Slobogin, *supra* at 149-67.

10. 126 S. Ct. 1515 (2006).

II. CURRENT EVENTS

On December 16, 2005, the New York Times revealed that the National Security Agency ("NSA") was conducting warrantless wiretaps of international telephone calls and e-mails when the Bush Administration believed one of the communicants to be affiliated with al Qaeda.[11] Begun just months after September 11, 2001, the eavesdropping had been taking place for four years and represented a dramatic shift from the Agency's foreign focus.[12] While the Administration has defended the program, the Wiretap Act requires a warrant for wiretaps in criminal investigations,[13] and the Foreign Intelligence Surveillance Act ("FISA") requires a warrant for any wiretap that constitutes "electronic surveillance."[14] To fall outside FISA's definition of "electronic surveillance" the program could not target "United States person[s]" or acquire content domestically.[15] Because the NSA has allegedly done both,[16] the program appears to be unlawful.[17]

---

11. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

12. *Id.*; Mark Hosenball & Evan Thomas, *Hold the Phone: Big Brother Knows Whom You Call*, NEWSWEEK, May 22, 2006, at 22.

13. 18 U.S.C.A. §§ 2511, 2518 (West 2004).

14. 18 U.S.C.A. § 2511(2)(f); 50 U.S.C.A. § 1805. The necessary showing differs from that required in criminal investigations, however: FISA requires that the government demonstrate probable cause to believe the target is an "agent of a foreign power." 50 U.S.C.A. § 1805(a)(3)(A).

15. 50 U.S.C.A. § 1801(f).

16. Risen & Lichtblau, *supra* note 11.

17. The President may have inherent Article II authority to conduct warrantless wiretapping for reasons of national security. *See In re* Sealed Case, 310 F.3d 717, 742 (F.I.S.A. Ct. Rev. 2002) (recognizing inherent authority); United States v. U.S. Dist. Court, 407 U.S. 297, 308 (1972) (denying such authority in the context of *domestic* security). However, it is unlikely that such authority would be exclusive such that it cannot be restricted by Congress. *See* Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 635-38 (1952) (Jackson, J., concurring) (articulating three categories of Presidential authority); Hamdan v. Rumsfeld, 126 S. Ct. 2749, 2774 n.23 (2006) ("Whether or not the President has independent power, absent congressional authorization, to convene military commissions, he may not disregard limitations that Congress has, in proper exercise of its own war powers, placed on his powers.") (citing *Youngstown*, 343 U.S. at 637). *But see* Letter from William E. Moschella, Assistant Attorney General, to F. James Sensenbrenner, Jr., Chairman, House Committee on the Judiciary, at 3-4 (Mar. 24, 2006), http://www.fas.org/irp/agency/doj/fisa/doj032406.pdf (arguing for some exclusive Presidential authority). The Administration's legal defense focuses on the Congressional Authorization for Use of Military Force ("AUMF"), passed in response to the attacks of September the 11th, Pub. L. 107-40, 115 Stat. 224 (2001). *See* Letter from William E. Moschella, Assistant Attorney Gen., to Pat Roberts, Chairman, Senate Select Comm. on Intelligence, at 3-4 (Dec. 22, 2005), http://www.fas.org/irp/agency/doj/fisa/doj122205.pdf. According to the Administration, the AUMF is a statute implicitly authorizing the surveillance given the language of FISA's proscription, namely that one is guilty of an offense if he or she "engages in electronic surveillance under color of law *except as authorized by statute*." 50 U.S.C.A. § 1809(a)(1) (2004) (emphasis added). That argument would be much stronger if not for a provision at 50 U.S.C.A. § 1811, which indicates that any such implicit authorization can only persist for 15 days.

Although the Wiretap Act includes a civil remedy, *see* 18 U.S.C.A. § 2520, the telephone companies might be exempt according to another provision of the Act:

Notwithstanding any other law, providers of wire or electronic communication

Five months later, on May 11, 2006, USA Today alleged that the National Security Agency had obtained and was parsing records identifying millions, if not billions, of telephone calls placed by Americans, creating what might be the largest database ever assembled.[18] Although the paper has since scaled back its allegations, it appears the NSA is in possession of a database containing information on a significant portion of domestic calls.[19] Again launched shortly after the attacks of September 11, the goal was to use social network analysis to detect signs of terrorist activity.[20] Because the Stored Communications Act typically does not allow public telecommunications providers to release call information to the government without a court order,[21] it appears this program may also be unlawful.[22]

> service . . . are authorized to provide information . . . to persons authorized by law to intercept wire, oral, or electronic communications . . . if such provider . . . has been provided with . . . a certification in writing by . . . the Attorney General of the United States that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required.

18 U.S.C.A. § 2511(2)(a)(ii)(B). Given the Administration's defense of the program, there might be such a certification.

For an argument that the program is constitutional, see Letter from John C. Eastman, Professor of Law & Dir., Claremont Institute Ctr. for Constitutional Jurisprudence, Chapman University, to James Sensenbrenner, Jr., Chairman, House Judiciary Comm. (Jan. 27, 2006), http://judiciary.house.gov/media/pdfs/nsaeastmanltr.pdf. A district court has held the program unconstitutional, but it did so via an unfortunate opinion so riddled with flaws as to be unhelpful. *See* ACLU v. Nat'l Sec. Agency, 438 F. Supp. 2d 754 (E.D. Mich. 2006). For example, it erroneously asserts that "the Fourth Amendment, about which much has been written, in its few words requires reasonableness in all searches. It also requires prior warrants for any reasonable search." *Id.* at 775. Although the Bush Administration has appealed, it has also recently agreed to bring the surveillance program under the scrutiny of the Foreign Intelligence Surveillance Court, so there may be no further judicial resolution. *See In The Nation: U.S. Seeks to Drop Surveillance Case*, PHILA. INQUIRER, Jan. 26, 2007, at A7.

18. Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls: 3 Telecoms Help Government Collect Billions of Domestic Records*, USA TODAY, May 11, 2006, at A1.

19. The records were purportedly obtained from AT&T, Verizon, and BellSouth, with only Qwest refusing to participate. Cauley, *supra* note 18. Verizon and BellSouth, however, have since disputed the allegation, *see* Dionne Searcey & Anne Marie Squeo, *More Phone Firms Fight Claims They Supplied Call Data to NSA*, WALL ST. J., May 17, 2006, at A3, and USA Today has admitted it cannot confirm the participation of either entity. Susan Page, *Lawmakers: NSA Database Incomplete*, USA TODAY, June 30, 2006, at A2. But the paper continues to insist that the NSA has compiled a "massive database of phone call records." *Id.*

20. Cauley, *supra* note 18.

21. 18 U.S.C.A. §§ 2702(c), 2703(c)(1). Section 2702(c)(4) permits disclosure to the government if there is "an emergency involving danger of death or serious physical injury," but this seems a stretch in context even given that the previous statutory language (in effect for much of the program's duration) required the more stringent "*immediate* danger of death or serious physical injury." 18 U.S.C.A. § 2702(c)(4) (effective until March 8, 2006) (emphasis added). Section 2709 does permit some access via a "National Security Letter," essentially the equivalent of an administrative subpoena issued by the F.B.I., but the NSA does not have this authority. Because details of the program remain classified, however, it is possible the information was routed through

In mid-June a Congressional investigation stumbled upon a more sordid means government agents have used to obtain calling records.[23] The investigation concerns the practice of "pretexting," in which unscrupulous data brokers pose as customers in order to obtain telephone records and other data.[24] Apparently such brokers provided their services not only to private investigators and other non-government snoops (such as those involved in the Hewlett-Packard board leak debacle[25]), but also to state and federal law enforcement.[26] Repeat business by government agents would of course encourage this fraudulent activity, and some of the officers utilizing these services operate in states which constitutionally restrict law enforcement access to the acquired information.[27]

---

the F.B.I. ostensibly pursuant to these provisions.

An unrelated provision of the Communications Act restricts disclosure of "individually identifiable customer proprietary network information," which is presumably why data was communicated without names attached. 47 U.S.C.A. § 222. *See* Cauley, *supra* note 18.

22. Although lawsuits have been filed challenging both NSA programs, we will have judicial resolution of neither if the courts accept the government's assertion of the state secrets privilege. Ashbel S. Green, *Feds Want NSA Suits United for D.C. Trial*, THE OREGONIAN, June 21, 2006, at A8. So far the government has had mixed success in that regard. *See* John Markoff, *Judge Declines to Dismiss Privacy Suit Against AT&T*, N.Y. TIMES, July 21, 2006, at A13; Adam Liptak, *Judge Rejects Customer Suit Over Records From AT&T*, N.Y. TIMES, July 26, 2006, at A13. Faced with sustained criticism and proposed legislation that would transfer all such cases to the Foreign Intelligence Surveillance Court for constitutional review, *see* Chris Mondics, *Bush Agrees to Deal on Spying Program*, PHILA. INQUIRER, July 14, 2006, at A3, the Bush Administration independently decided to bring the program within the scrutiny of that court. Eric Lichtblau & David Johnson, *Court to Oversee U.S. Wiretapping in Terror Cases*, N.Y. TIMES, Jan. 18, 2007, at A1.

In an allegedly unrelated decision, one of the alleged participants, AT&T, later modified its privacy policy to indicate that all personal account information is owned by the company. Editorial, *Ma Bell's Data, And Yours*, L.A. TIMES, June 24, 2006, at A14; David Lazarus, *Personal Information Isn't That Confidential: Experts Weigh in on AT&T's Assertion That it Owns Your Data*, S.F. CHRON., June 23, 2006, at D1. "While your account information may be personal to you," says the new policy, "these records constitute business records that are owned by AT&T." *Id.*

23. Bob Sullivan, *Who's Buying Cell Phone Records Online? Cops*, MSNBC.COM, June 20, 2006, http://www.msnbc.msn.com/id/12534959/; Ted Bridis, *Lawmakers to Crack Down on Data Brokers*, Wash. Post, June 21, 2006.

24. *Feds Paid Private Brokers For Phone Records: Web-based Services Racked up $30 Million by Sometimes Violating Laws*, MSNBC.COM, June 20, 2006, http://www.msnbc.msn.com/id/11100923/.

25. Apparently at the direction of then-chairwoman Patricia Dunn, private investigators used pretexting to obtain the phone records of members of Hewlett-Packard's board of directors, journalists, and others in an attempt to determine the source of company leaks. Damon Darlin, *Ex-Chairwoman Among 5 Charged in Hewlett Case*, N.Y. TIMES, Oct. 5, 2006, at A1. The fallout not only cost Dunn her job, but has resulted in the passage of new anti-pretexting legislation, the filing of state criminal charges, a $14.5 million civil settlement, and the initiation of several federal investigations. *Id.*; Jim Hopkins & Jon Swartz, *Investigations Continue at HP: Scandal Gets Scrutiny from Several Fronts*, USA TODAY, Oct. 5, 2006, at B2; Ellen Nakashima, *HP, Calif. Settle Spying Lawsuit*, WASH. POST, Dec. 8, 2006, at D1; Jordan Robertson, *U.S. Wins First Guilty Plea in HP Boardroom Spy Probe*, PHIL. INQUIRER, Jan. 13, 2007, at C2; 18 U.S.C. § 1039.

26. *Feds Paid Private Brokers*, *supra* note 24.

27. *Id.* The article alleges use by municipal police departments in California, Colorado, and Florida, all of which recognize a constitutional right to privacy in telephone records. *See* Henderson, *supra* note 7, at 396-97.

Finally, on June 23, 2006, the New York Times and other newspapers revealed that the Central Intelligence Agency has been combing through the enormous database of banking records compiled by the Society for Worldwide Interbank Financial Telecommunications ("SWIFT").[28] Like the NSA programs, this program was instituted shortly after the attacks of September 11, and has been used tens of thousands, or even hundreds of thousands, of times.[29] Unable to extract the desired information from its enormous database, SWIFT apparently made the entire database accessible to the United States. According to Administration officials, however, the government established an audited system through which its agents would only view records of those for whom it had evidence of terrorist connections.[30] Nevertheless, those officials did pass on evidence of other crimes, such as money laundering or drug trafficking.[31] Although such access is unprecedented and the relevant laws have some ambiguity, this program appears to be lawful in the United States, though SWIFT may have violated European data protection laws.[32]

Nor is the government content to obtain existing third-party information. The United States Attorney General has requested that Internet service providers retain customer data for a period of two years, whereas most companies currently retain such data for only a matter of weeks or months.[33] Law enforcement can already request preservation of a specific user's records where that information may prove useful in an investigation,[34] but the Administration now wants companies to retain records of all customers. The retained information would be detailed, allowing a provider to identify which websites an individual visited, whom he or she exchanged e-mails

28. Eric Lichtblau & James Risen, *Bank Data Sifted in Secret by U.S. to Block Terror*, N.Y. TIMES, June 23, 2006, at A1. SWIFT routes approximately $6 trillion daily between banks, brokerages, and other institutions, but would not have records on most routine domestic transactions. *Id.* However, separate agreements with other companies might have provided such access. *Id; see also* Josh Meyer & Greg Miller, *U.S. Secretly Tracks Global Bank Data*, L.A. TIMES, June 23, 2006, at A1.

29. Lichtblau & Risen, *supra* note 28; Karen DeYoung, *Officials Defend Financial Searches*, WASH. POST, June 24, 2006, at A1; Peter Baker, *Surveillance Disclosure Denounced*, WASH. POST, June 27, 2006, at A1.

30. Lichtblau & Risen, *supra* note 28; DeYoung, *supra* note 29.

31. DeYoung, *supra* note 29.

32. Lichtblau & Risen, *supra* note 28; Editorial, *Bank Surveillance*, WASH. POST, June 24, 2006, at A20; Katrin Bennhold, *Parliament Tells Europeans to Explain What They Knew About U.S. Tracking of Bank Data*, N.Y. TIMES, July 7, 2006, at A10.

33. Saul Hansell & Eric Lichtblau, *U.S. Wants Internet Companies to Keep Web-Surfing Records*, N.Y. TIMES, June 2, 2006 at A15; Jon Swartz & Kevin Johnson, *U.S. Asks Internet Firms to Save Data*, USA TODAY, June 1, 2006, at A1.

34. 18 U.S.C.A § 2703(f) (West 2004).

with, and perhaps which searches he or she ran.[35] Concerned by the interjurisdictional nature of the Internet, the Attorneys General of forty-five states, the District of Columbia, and three territories have together urged Congress to adopt a national data retention requirement,[36] and Congressional committees are considering such legislation.[37]

The three surveillance programs and the data-retention proposal may represent good policy.[38] According to one poll, the majority of Americans are in favor of the NSA searching telephone call records.[39] But what all five programs have in common is a third-party doctrine that allows the government to access information without any federal constitutional restraint, meaning the access could be for a good reason (e.g., preventing terrorism) and include significant internal restraint, or there could be no justification (e.g., mere curiosity) and no restraint.[40] Understandably, following the attacks of September 11 there has been a dramatic increase in government access to third-party information.[41] Companies have had to establish departments that do nothing but respond to such demands, and according to some, the vast majority of the demands are legally (statutorily) unsupportable.[42] When the government begins to conduct dragnet searches of vast databases of third-party information without any required justification, we have realized the twenty-first century equivalent of the general warrants that the Fourth Amendment was specifically designed to forbid.[43] There is, more than ever before, a significant danger in permitting

---

35. Hansell & Lichtblau, *supra* note 33.

36. *See* Letter from John Suthers, Attorney General of Colorado et al. to J. Dennis Hastert, Speaker, United States House of Representatives et al. (June 21, 2006), http://www.atg.wa.gov/releases/2006/Documents/DRLetter.pdf.

37. Kurt Eichenwald, *Internet Companies Divided on Plan to Fight Pornography*, N.Y. TIMES, June 28, 2006, at C3.

38. Government support of fraudulent pretexting is obviously unacceptable.

39. *NSA's Phone-Call Program Meets Mixed Reactions: More Outrage on Capitol Hill Than Main Street*, ABC NEWS, May 12, 2006, http://www.abcnews.go.com/GMA/print?id=1953612 (finding 63 percent believe the program justified while 35 percent deem it unacceptable); Richard Morin, *Poll: Most Americans Support NSA's Phone Data Efforts*, WASH. POST, May 12, 2006. A Newsweek poll, however, found that 53 percent of Americans believe the NSA has gone "too far" in its surveillance. Mark Whitaker, *The Editor's Desk*, NEWSWEEK, May 22, 2006, at 4; Hosenball & Thomas, *supra* note 12.

40. Although the Supreme Court has not applied the third-party doctrine to the content of telephone conversations, those conversations are provided to a third party provider just like records of those calls.

41. Robert Block, *Requests for Corporate Data Multiply: Businesses Juggle Law-Enforcement Demands for Information About Customers, Suppliers*, WALL ST. J., May 20, 2006, at A4; Arshad Mohammed & Sara Kehaulani Goo, *Government Increasingly Turning to Data Mining; Peek Into Private Lives May Help in Hunt for Terrorists*, WASH. POST, June 15, 2006, at D3.

42. *See* Block, *supra* note 41 (quoting John Ryan, AOL's Vice President and Associate General Counsel, as saying that "for every five requests that come in maybe one will fit the standard to a certain level and will be honored").

43. *See* Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 669-71 (1995) (O'Connor, J., dissenting) (recognizing primary purpose of forbidding general warrants); Stanford v. Texas, 379

completely unfettered government access to information in the hands of third parties.

Last term five members of the Supreme Court departed from the third-party doctrine in a different context, namely the search of a place "given" to a third party.[44] On July 6, 2001, police were called to the home of Scott and Janet Randolph.[45] The fractured couple parried allegations of drug use, culminating in Janet's revelation that there were "items of drug evidence" in the house.[46] When Scott refused an officer's request for permission to search the home, the officer merely made the same request of Janet, which she granted.[47] Her tour led officers upstairs to Scott's bedroom, where they found a drinking straw containing cocaine residue.[48]

While it was settled doctrine that consent searches were constitutional,[49] including those based on consent by one with common authority[50] (and even on reasonable but erroneous belief that one has such authority[51]), Scott argued that Janet's consent was ineffective as to him given his contemporaneous refusal.[52] Despite unanimous federal appellate doctrine and a majority of state decisions to the contrary, five members of the Court agreed with Scott, holding the search unconstitutional.[53] According to these Justices, societal expectations were contrary to the officers' actions: If one tenant invites in a guest but another contemporaneously refuses admission, the expectation is that the guest will not enter.[54] "The constant element in assessing Fourth Amendment reasonableness in the consent cases . . . is the great significance given to widely shared social expectations,"[55] and "there

---

U.S. 476, 481-82 (1965) (same); Brenner, *supra* note 6, at 63.

44. *Georgia v. Randolph*, 126 S. Ct. 1515, 1519 (2006).

45. *Id.*

46. *Id.*

47. *Id.*

48. *Id.* By the time the officer returned to the house after walking to his vehicle to obtain an evidence bag, Janet had decided to withdraw her consent. *Id.* A subsequent search of the home pursuant to a search warrant yielded further evidence of drug use. *Id.*

49. *See* Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973).

50. *See* United States v. Matlock, 415 U.S. 164, 170-71 (1974).

51. *See* Illinois v. Rodriguez, 497 U.S. 177, 186 (1990).

52. *Randolph*, 126 S. Ct. at 1519.

53. *Id.* at 1520 n.1.

54. *Id.* at 1522. According to the Court,

> [I]t is fair to say that a caller standing at the door of shared premises would have no confidence that one occupant's invitation was sufficiently good reason to enter when a fellow tenant stood there saying "stay out." Without some very good reason, no sensible person would go inside under those conditions.

Id. at 1522-23.

55. *Id.* at 1521.

is no common understanding that one co-tenant generally has a right or authority to prevail over the express wishes of another, whether the issue is the color of the curtains or invitations to outsiders."[56]

Of course, whether this is indeed the societal expectation in this instance, and how these five members of the Court came to know it, can be debated.[57] The Court once again urged and applied an empirical conception of the Fourth Amendment without any empirics.[58] And social expectations and a "balancing of competing individual and governmental interests"[59] often do not make for bright line rules.[60] But I agree with Justice Breyer that "the Fourth Amendment does not insist upon bright-line rules. Rather, it recognizes that no single set of legal rules can capture the ever changing complexity of human life. It consequently uses the terms 'unreasonable searches and seizures.' And [the] Court has continuously emphasized that reasonableness is measured by examining the totality of the circumstances."[61]

Scott Randolph voluntarily shared information, and in this case access to a private location, with his wife Janet. But despite Janet's eager acceptance of law enforcement's request to enter that location, the Court refused to permit such access without legal process or a recognized exception thereto.

---

56. *Id.* at 1523. Why this indicates that the naysayer trumps the tenant desiring entry is not clear, as Chief Justice Roberts pointed out in dissent: "Does the objecting cotenant accede to the consenting cotenant's wishes, or the other way around? The majority's assumption about voluntary accommodation simply leads to the common stalemate of two gentlemen insisting that the other enter a room first." *Id.* at 1532.

57. Justice Roberts assailed the majority's "assumption" / "hunch" in his dissent. *Id.* He also asserted that the majority erred by considering societal expectations in determining reasonableness, urging that such expectations are only relevant to whether a search occurred. *Id.*

58. Although the Court has now opined for forty years on when people do and do not have a "reasonable expectation of privacy," it has never seriously considered how it should go about determining societal views. One scholar who has taken this seriously is Christopher Slobogin, who has conducted two empirical studies. *See generally* Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society,"* 42 DUKE L.J. 727 (1993); Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 275-78 (2002). Although neither survey focused on third-party searches, "[p]erusing bank records" ranked as the thirteenth most intrusive of Slobogin and Schumacher's fifty proposed government actions. Slobogin & Schumacher, *supra* at 738-39.

59. *Randolph*, 126 S. Ct. at 1523.

60. Justice Roberts emphasized this lack of clarity in his dissent. *Id.* at 1532.

61. *Id.* at 1529 (Breyer, J., concurring) (internal quotation marks and ellipses omitted). Interestingly, Justice Breyer also signed onto a recent dissent that objected to the use of such a totality reasonableness balance in deciding whether to permit the suspicionless search of parolees. *See* Samson v. California, 126 S. Ct. 2193, 2202 (2006) (Stevens, J., dissenting). But the majority in *Samson* strongly rearticulated the reasonableness criterion: "Under our general Fourth Amendment approach we examine the totality of the circumstances to determine whether a search is reasonable within the meaning of the Fourth Amendment. Whether a search is reasonable is determined by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate government interests." *Id.* at 2197 (internal citations and quotation marks omitted).

As the Chief Justice explained in his dissent, this is contrary to a broad understanding of the Court's third-party doctrine.[62] If one retains no reasonable expectation of privacy in information or location given to a third party, then access could only infringe on that third party's Fourth Amendment rights. Thus, for example, when third-party recipients of National Security Letters recently contested certain provisions of their use, both the government and the courts recognized that the third party had some Fourth Amendment rights even though the true party in interest had none under the federal third-party doctrine.[63] If that third party consents, then the Fourth Amendment should be satisfied. But in *Randolph* the Court instead insisted that societal expectations are relevant in determining what is reasonable, and I posit that the Court was at least correct in this: society expects some constraint on law enforcement accessing some information in the hands of third parties.[64] It remains to determine when law enforcement should be constrained and what that constraint should be.

III. RELEVANT FACTORS

A good place to begin is with bank records, which played a critical role in the development of the federal doctrine.[65] In the waning days of 1974, a unanimous California Supreme Court declared in *Burrows v. Superior Court*[66] that law enforcement could not access bank records absent some legal process.[67] Perhaps anticipating that the United States Supreme Court might ultimately hold to the contrary,[68] the California court relied on its state

62. *Randolph*, 126 S. Ct. at 1533-35 (Roberts, C.J., dissenting).

63. *See* Doe v. Ashcroft, 334 F. Supp. 2d 471, 494 n.118, 527 (S.D.N.Y. 2004) (holding National Security Letter provision unconstitutional based on a provision seeming to prevent third-party challenge, while recognizing that no challenge by accountholder was constitutionally necessary), *vacated based on intervening statutory change*, Doe v. Gonzales, 449 F.3d 415 (2d. Cir. 2006).

64. There is no reason why societal expectations should play a role unique to consent cases. However, the Court's "common authority" consent cases rely on the same "assumption of risk" the Court has used to justify its third-party doctrine. *See Randolph*, 126 S. Ct. at 1522 (majority opinion) (quoting United States v. Matlock, 415 U.S. 164, 171 (1974)); *id.* at 1533-35 (Roberts, C.J., dissenting) (equating doctrines). Thus, there is an explicit linkage in these contexts.

65. *See* United States v. Miller, 425 U.S. 435, 435 (1976) (holding that so far as the customer is concerned, the Fourth Amendment places no restriction on law enforcement access to bank records).

66. 529 P.2d 590 (Cal. 1974).

67. *Id.* at 594-95.

68. Earlier in the year the United States Supreme Court had decided *California Bankers Ass'n. v. Shultz*, 416 U.S. 21 (1974), in which a divided Court (6-3) upheld the recording and reporting requirements of the Bank Secrecy Act of 1970 against a constitutional challenge. Based on the opinions in *Shultz* it was not clear whether the Court would find any Fourth Amendment restriction on accessing bank records. *See Burrows*, 529 P.2d at 595-96.

constitutional analog, Article I, section 13.[69] The opinion is important, not only because it was to become the dissent of Justice Brennan in *United States v. Miller*,[70] but because it has been the basis upon which other states have rejected the federal doctrine.[71]

California had adopted *Katz'* reasonable expectation of privacy criterion, so the *Burrows* court had to determine whether a customer retained a "reasonable expectation of privacy" in bank records.[72] According to the court, "[i]t cannot be gainsaid that the customer of a bank expects that the documents, such as checks, which he transmits to the bank in the course of his business operations, will remain private, and that such an expectation is reasonable."[73] The unanimous court did not think it necessary to support this proposition with reasoning or empirics—it was simply self-evident. The court did note that the assumed expectation was generally shared by the relevant third party.[74]

But slightly over a year later the United States Supreme Court rejected this "undeniable" truth and deemed it inconsequential that a recipient promises to use information only for a limited purpose.[75] Assuming the proposition is therefore not undeniable—although both courts would have done well to give some justification for their assumption in that regard—what other support did the California Supreme Court provide for restricting law enforcement access? The court began by articulating a potential distinction that it deemed irrelevant, namely whether law enforcement seeks disclosed information or records created by the third party that incorporate that information: "That the bank alters the form in which it records the information transmitted to it by the depositor . . . does not diminish the depositor's anticipation of privacy in the matters which he confides to the bank."[76]

---

69. *Burrows*, 529 P.2d at 592-93, 595.

70. With the exception of a few explanatory paragraphs, Justice Brennan's entire dissent consists of passages quoted from *Burrows*. *See Miller*, 425 U.S. at 447-55. Of the approximately 1800 words exclusive of footnotes in Justice Brennan's opinion, approximately 1300 are Justice Mosk's of the California Supreme Court. *See id.*

71. *See* Charnes v. DiGiacomo, 612 P.2d 1117, 1121 (Colo. 1980); People v. Jackson, 452 N.E.2d 85, 88-89 (Ill. App. Ct. 1983); State v. McAllister, 875 A.2d 866, 874-75 (N.J. 2005); Commonwealth v. DeJohn, 403 A.2d 1283, 1289-91 (Pa. 1979).

72. *Burrows*, 529 P.2d at 593.

73. *Id.*

74. *Id.* "Representatives of several banks testified at the suppression hearing that information in their possession regarding a customer's account is deemed by them to be confidential." *Id.*

75. *Miller*, 425 U.S. at 443.

76. *Burrows*, 529 P.2d at 593. The court stated:

> In *Katz v. United States*, it was said that the "premise that property interests control the right of the Government to search and seize has been discredited." The mere fact that the bank purports to own the records which it provided to the detective is not, in our view, determinative of the issue at stake. The disclosure by the depositor to the bank is made for the limited purpose of facilitating the conduct of his financial affairs; it seems evident that his expectation of privacy is not diminished by the bank's retention of a record of

Next, the court asserted that completely discretionary access is disfavored, because it would allow officers to gather information on a mere whim: "If this search may be deemed reasonable, nothing could prevent any law enforcement officer from informally requesting and obtaining all of a person's or business entity's records which had been confided to a bank, though such records might have no relevance to a crime, if any, under investigation."[77] Nevertheless, unfettered access might be reasonable where there is legitimate need, but here the government failed to make any such claim:

> The People advance no governmental justification for such a sweeping exploratory invasion into an individual's privacy. Their primary assertion is not that it is essential to effective law enforcement to obtain bank records without judicial process, or even that the interests of a person in the confidentiality of his financial affairs is outweighed by the advantages to society in disclosure of the information.[78]

Instead, the government argued that the court should not interfere with the desire of a bank to assist law enforcement.[79] Whether beneficent or intended to improve its public image, the court quite properly deemed irrelevant a *bank's* desire to comply with a law enforcement request: "However laudable these motives may be, we are not here concerned with the conduct or reputation of banks, but with whether the police violated [the customer's] rights . . . ."[80]

The court did consider relevant that in modern society the "choice" to convey information to a bank is not voluntary in any meaningful sense.[81]

---

such disclosures.

Id. at 594 (internal citation omitted). *Cf. Miller*, 425 U.S. at 440 ("[R]espondent can assert neither ownership nor possession. Instead, these are the business records of the banks.").

77. *Burrows*, 529 P.2d at 593.

78. *Id.*

79. *Id.*

80. *Id.* The court further asserted:

> [T]he fact that the bank voluntarily acceded to a police officer's request . . . cannot serve to validate the governmental conduct. It is not the right of privacy of the bank but of the [customer] which is at issue, and thus it would be untenable to conclude that the bank, a neutral entity with no significant interest in the matter, may validly consent to an invasion of its depositors' rights.

Id. at 594.

81. *Id.* at 596. "For all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account." *Id.* "In this complex

Moreover, the information, at least when considered *en masse*, includes "many aspects of [one's] personal affairs, opinions, habits and associations" so as to constitute a "virtual current biography."[82] This important point would later be entirely neglected by the United States Supreme Court in *Miller*.[83] Even if most individual exchanges were disclosed not only to the bank but additionally to another third party (e.g., checks drawn on the account), the privacy implication in obtaining a log of every such transaction is much more dramatic.

Finally, the California court recognized the need to account for changing technology and social norms:

> Cases are legion that condemn violent searches and invasions of an individual's right to the privacy of his dwelling. The imposition upon privacy, although perhaps not so dramatic, may be equally devastating when other methods are employed. Development of photocopying machines, electronic computers and other sophisticated instruments have accelerated the ability of government to intrude into areas which a person normally chooses to exclude from prying eyes and inquisitive minds. Consequently judicial interpretations of the reach of the constitutional protection of individual privacy must keep pace with the perils created by these new devices.[84]

Thus the *Burrows* analysis begins by asserting an "undeniable" truth, but in its entirety it provides a rather rich discussion of why government access to bank records should be restricted, and I agree with that analysis and its conclusion. Other state and federal decisions both reiterate the *Burrows* factors and introduce other relevant considerations. In all I have identified nine factors that I believe are relevant to whether law enforcement access should be constitutionally restricted and four considerations that I believe are not relevant. Table I contains a list of these factors and considerations, following which is an explanation of each. While each

---

society, few people can live or conduct business without a bank account." People v. Chapman, 679 P.2d 62, 67 (Cal. 1984) (describing *Burrows*).

82. *Burrows*, 529 P.2d at 596.

> In the course of [banking], a depositor reveals many aspects of his personal affairs, opinions, habits and associations. Indeed, the totality of bank records provides a virtual current biography. While we are concerned in the present case only with bank statements, the logical extension of the contention that the bank's ownership of records permits free access to them by any police officer extends far beyond such statements to checks, savings, bonds, loan applications, loan guarantees, and all papers which the customer has supplied to the bank to facilitate the conduct of his financial affairs upon the reasonable assumption that the information would remain confidential.

Id.

83. United States v. Miller, 425 U.S. 435 (1976).

84. *Id.* at 596.

individual factor considers information essentially as disclosed, Factor 3 includes a discussion of the relevance of aggregating that information into databanks.

TABLE 1

RELEVANT FACTORS:
1. THE PURPOSE OF THE DISCLOSURE
2. THE PERSONAL NATURE OF THE INFORMATION
3. THE AMOUNT OF INFORMATION
4. THE EXPECTATIONS OF THE DISCLOSING PARTY
5. THE UNDERSTANDING OF THE THIRD PARTY
6. POSITIVE LAW GUARANTEES OF CONFIDENTIALITY
7. GOVERNMENT NEED
8. PERSONAL RECOLLECTIONS
9. CHANGING SOCIAL NORMS AND TECHNOLOGIES

IRRELEVANT CONSIDERATIONS:
1. THE FORM OF THE INFORMATION
2. THE "GOOD CITIZEN" MOTIVATION OF A THIRD PARTY
3. THE GOVERNMENT'S METHOD OF ACQUISITION
4. EXPECTATIONS CREATED BY POLICE CONDUCT

A. Factor 1. The Purpose of the Disclosure

If a disclosure is necessary to participate in society, this weighs in favor of restricting government access. In what could be considered the most extreme case, no disclosure is intended and the disclosure cannot reasonably be prevented. For example, the human body and computers emit electromagnetic radiation, but this unintended "leakage" would be costly or impossible to prevent.[85] That a "transfer" did occur and that it could be (but is typically not) obtained by a third party should play no role in Fourth Amendment analysis. Taken alone, advancing technology gives no justification for limiting or abdicating Fourth Amendment interests.[86]

85. *See* Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 535-36, 537-38 (2005).

86. This does not mean technology is irrelevant. It could, for example, lead to general public consumption, *see* Factor 4, *infra* Part III.D, in the absence of restricting legislation, *see* Factor 6, *infra* Part III.F.

A less extreme case is when one desires to provide the relevant information, but only because the third party is serving as a conduit, as when one sends electronic mail via an Internet service provider.[87] Such a third party has no need, or reason, to examine the content itself. Here too the transfer should not weaken existing Fourth Amendment protections.[88] Not only do conduits provide critical avenues of socially beneficial communication, such as telephone, mail, and the Internet, but there is typically a recipient for whom the content is intended, and therefore to whom any legitimate third-party doctrine would apply. I have previously referred to both of these limitations as a "limited" third-party doctrine.[89]

A closer case is when one does desire to disclose the content, but only because doing so is necessary to participate in ordinary society. This necessity should weigh in favor of restricting government access. Thus in *Burrows* the California Supreme Court relied on the necessity of having a bank account,[90] and when the same court was called upon to decide whether to constitutionally restrict law enforcement access to unlisted information disclosed to a telephone company, the court held in the affirmative: "[D]isclosure of the information . . . is not entirely volitional. Doing without a telephone is not a realistic option for most people."[91] Four justices of the

---

87. *See* Henderson, *supra* note 85, at 522-28.

88. The best judicial exposition of this claim is probably in *State v. Hempele*, 576 A.2d 793 (N.J. 1990), in which the New Jersey Supreme Court required a warrant supported by probable cause for searches of garbage left for collection:

> Conveying information to another is different from conveying an opaque bag containing information. People do not compromise their privacy interest in the contents of a container when they turn that container over to a third party: "Were it otherwise, a letter or package would lose all Fourth Amendment protection when placed in a mail box or other depository with the 'express purpose' of entrusting it to the postal officer or a private carrier; those bailees are just as likely as trash collectors (and certainly have greater incentive) to 'sor[t] through' the personal effects entrusted to them, 'or permi[t] others, such as police to do so.'" Materials given to public or private carriers for delivery are constitutionally protected . . . . That principle suggests that garbage does not lose constitutional protection merely because it is handed over to a collector.
>
> Here, defendants did not inform the collector of the contents of their garbage. The only information conveyed was the number, type, and weight of the bags.

Id. at 806-07 (quoting California v. Greenwood, 486 U.S. 35, 55 (1988) (Brennan, J., dissenting)) (other internal citations omitted).

89. Henderson, *supra* note 85, at 528.

90. Burrows v. Superior Court, 529 P.2d 590, 596 (Cal. 1974).

91. People v. Chapman, 679 P.2d 62, 67 (Cal. 1984) (internal quotation marks and citation omitted). Other justices and courts have similarly relied upon the necessity of having a bank account and telephone service. With respect to bank accounts, see *People v. Jackson*, 452 N.E.2d 85, 89 (Ill. App. Ct. 1983) ("Since it is virtually impossible to participate in the economic life of contemporary society without maintaining an account with a bank, opening a bank account is not entirely volitional and should not be seen as conduct which constitutes a waiver of an expectation of privacy.") (citing *Burrows*); *State v. McAllister*, 875 A.2d 866, 874 (N.J. 2005) ("[I]n contemporary society, it is the rare citizen who 'socks away' cash in the proverbial mattress. Instead, citizens customarily deposit money in bank accounts, which have become an indispensable part of modern commerce. As a consequence, numerous participants in our nation's economic life leave behind detailed financial dossiers."). With respect to telephone service, see *Smith v. Maryland*, 442 U.S. 735, 746 (Stewart,

Washington Supreme Court would have reached a similar result with respect to records of electricity consumption,[92] and some courts have so held with respect to garbage left for collection.[93]

Likewise, if a disclosure is for a limited purpose, this weighs in favor of restricting unrelated access.[94] As Justice Marshall urged in his dissent in *Smith*, "[p]rivacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."[95] Only when the

---

J., dissenting) ("In *Katz v. United States* the Court acknowledged the 'vital role that the public telephone has come to play in private communications.' The role played by a private telephone is even more vital. . . . A telephone call simply cannot be made without the use of telephone company property and without payment to the company for the service.") (internal citation omitted). *See also id.* at 750 (Marshall, J., dissenting) ("[U]nless 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.") (internal citation omitted); People v. Sporleder, 666 P.2d 135, 141 (Colo. 1983) ("A telephone is a necessary component of modern life. It is a personal and business necessity indispensable to one's ability to effectively communicate in today's complex society."); People v. DeLaire, 610 N.E.2d 1277, 1282 (Ill. App. Ct. 1993) ("[The phone company] is a monopoly and a utility, and it records customers' [dialing information] automatically and involuntarily."); State v. Hunt, 450 A.2d 952, 955-56 (N.J. 1982) ("The telephone has become an essential instrument in carrying on our personal affairs.").

92. *See In re* Maxfield, 945 P.2d 196, 200-01 (Wash. 1997). Justice Johnson, writing for four justices who would have granted constitutional protection, asserted that "[e]lectricity, even more than telephone service, is a 'necessary component' of modern life, pervading every aspect of an individual's business and personal life. . . . A requirement of receiving this service is the disclosure to the power company . . . of one's identity and the amount of electricity being used." *Id.*

93. *See* State v. Boland, 800 P.2d 1112, 1117 (Wash. 1990) ("The proper and regulated collection of garbage, as evidenced by ordinances . . . is as necessary to the proper functioning of modern society as is the telephone company."); State v. Morris, 680 A.2d 90, 95 (Vt. 1996) ("As a practical matter, the regulated collection of garbage is necessary for the proper functioning of our complex society. Most people today have little choice but to place their garbage at curbside for collection by public or private trash haulers.").

A California court held to the contrary with respect to information conveyed to a locksmith in the context of changing the combination of a safe, asserting that such hiring of a locksmith is "entirely volitional" because "[r]etaining a locksmith's services is certainly not a prerequisite to participating in contemporary society." People v. Abbott, 162 Cal. App. 3d 635, 640 (1984). The court's assertion is questionable, because having a safe (and therefore sometimes hiring a locksmith) would seem to be essential in many contexts.

94. *See Chapman*, 679 P.2d at 66 ("[P]eople disclose the information contained in these records to the bank for very limited purposes. The clear expectation is that those limits will be honored.").

95. *Smith*, 442 U.S. at 749 (Marshall, J., dissenting). Other courts have so held. *See Hunt*, 450 A.2d at 956 ("The telephone caller . . . is entitled to assume that the numbers he dials in the privacy of his home will be recorded solely for the telephone company's business purposes. . . . This disclosure has been necessitated because of the nature of the instrumentality, but more significantly the disclosure has been made for a limited business purpose and not for release to other persons for other reasons."); Mont. Human Rights Div. v. City of Billings, 649 P.2d 1283, 1288 (Mont. 1982) ("The [state] argues that because an employee knows information concerning his employment may

government's motivation to access information is related to the purpose of disclosure does this weigh in favor of unrestricted access. Thus the Supreme Court of Pennsylvania refused to restrict law enforcement access to information given to an insurance company in the course of an arson claim investigation, because the purpose of that investigation was to determine whether the insured was entitled to payment, necessarily including whether the insured committed a criminal act.[96] And the Washington Supreme Court refused to restrict access to driver's license records, explaining that "in this case the government is accessing records kept by a government entity expressly for use by that agency and law enforcement."[97]

However, the government cannot use this as a loophole to acquire all sorts of information in lieu of traditional investigation. If the third party obtaining the information is effectively law enforcement, or if that party is obtaining or retaining the information for law enforcement, and it is obtained or retained solely for a law enforcement purpose, unfettered collection and/or access is likely to be unreasonable. Hence in *Ferguson v. City of Charleston*,[98] a hospital urine test was an unconstitutional search where the hospital administration had worked closely with the police in crafting a drug testing regime that relied upon threats of criminal prosecution.[99] The decision is consistent with a "necessary to disclose" or "limited purpose" criterion,[100] but it also demonstrates that law enforcement will not be permitted to take advantage of a sham third-party transfer. Although three dissenters argued that the holding was contrary to the established third-party doctrine,[101] the majority was right to consider government involvement in the transfer, and it should have played a similar role in *United States v. Miller* (in which banks were required by federal statute to retain the relevant banking records precisely because they were often useful in criminal and

---

be sought by prospective employers in the future, he may not reasonably expect it will never be divulged to anyone else. It may well be unreasonable for an employee to expect that this information will never be divulged to prospective employers. It does not necessarily follow that, therefore, this information is unprotected by the right of privacy under all other circumstances . . . . The right of privacy turns on the reasonableness of the expectation, which may vary, even regarding the same information and the same recipient of that information.").

96. Commonwealth v. Efaw, 774 A.2d 735, 738-39 (Pa. 2001).

97. State v. McKinney, 60 P.3d 46, 50-51 (Wash. 2002); *accord* State v. Richter, 765 A.2d 687, 688 (N.H. 2000).

98. 532 U.S. 67 (2001).

99. *Id.* at 81-85.

100. For an illuminating argument in this regard, see Joseph T. Thai, *Is Data Mining Ever a Search Under Justice Stevens's Fourth Amendment?*, 74 FORDHAM L. REV. 1731, 1746-50 (2006). Perhaps as to the drug information the transfer could also be considered "unintended leakage" that would be difficult or impossible to prevent, in that it was information the patient did not wish to disclose to anyone, including the physician. The physiology of the human body dictated that in giving what information *was* desired, this information was necessarily communicated as well.

101. *Ferguson*, 532 U.S. at 94-95 (Scalia, J., dissenting).

civil investigations)[102] and *California v. Greenwood* (in which homeowners were required to dispose of their garbage via an authorized collector).[103] Thus, if the government decides to require that Internet service providers retain records,[104] that requirement would weigh in favor of constitutionally restricting government access.

B. Factor 2. The Personal Nature of the Information

There is a definite benefit to a legal rule that does not require courts to distinguish between "more personal" and "less personal" information. It will often be contentious which of two things is more personal and, if so, whether there is a significant enough difference to affect the legal rule.[105] Thus it is not surprising that the Supreme Court in *Kyllo v. United States*[106] refused to develop "a jurisprudence specifying which home activities are 'intimate' and which are not."[107] But the Court was only able to decline such a jurisprudence because it could hold that the use of sense-enhancing technology to determine *any* information regarding the interior of the home constitutes a search typically requiring a warrant supported by probable cause.[108] Because it would unduly cripple law enforcement to apply the same rule to all third-party information outside of the home, it is impossible to avoid making distinctions based on the personal nature of information.[109]

---

102. *See* United States v. Miller, 425 U.S. 435, 436, 443 (1976); Cal. Bankers Assn. v. Schultz, 416 U.S. 21, 26 (1974).

103. *See* California v. Greenwood, 486 U.S. 35, 54-55 (1988) (Brennan, J., dissenting).

104. *See supra* notes 33-37 and accompanying text.

105. Privacy is a complicated notion, and for a court to distinguish among different types of information it will have to adopt a conception of what is "more personal." As Professor Solove has demonstrated, different constructions of privacy are commonplace, *see* Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087 (2002), and I certainly do not minimize the difficult questions this engenders. Although it is unusual, courts will sometimes take a stab at articulating a conception. *See, e.g.*, Shaktman v. State, 553 So. 2d 148, 150-51 (Fla. 1989) (requiring judicial determination of reasonable suspicion for installation of pen register). "[The Florida constitutional] right ensures that individuals are able to determine for themselves when, how and to what extent information about them is communicated to others. One of its ultimate goals is to foster the independence and individualism which is a distinguishing mark of our society and which can thrive only by assuring a zone of privacy into which not even government may intrude without invitation or consent. . . . A fundamental aspect of personhood's integrity is the power to control what we shall reveal about our intimate selves, to whom, and for what purpose." *Id.* (internal citations and quotation marks omitted).

106. 533 U.S. 27 (2001).

107. *Id.* at 38-39.

108. *Id.* at 34.

109. The other bright-line alternative, requiring little or no justification for access to all third-party information, is just as unacceptable to legitimate privacy interests.

Some information provided to third parties is so banal that there should be no restriction on government access. Thus, the Supreme Court of Pennsylvania refused to restrict government access to name and address information held by a bank, despite that court's policy of generally restricting access to bank records: "A person's name and address do not, by themselves, reveal anything concerning his personal affairs, opinions, habits, or associations."[110] Other courts have held that the same is true of power consumption records[111] and driver's license records.[112] The opposite is true of garbage left for collection, and several courts have relied on this personal nature in granting it constitutional protection.[113]

---

110. Commonwealth v. Duncan, 817 A.2d 455, 463 (Pa. 2003) (internal quotation marks omitted); *accord* State v. Chryst, 793 P.2d 538, 542 (Alaska Ct. App. 1990) (refusing to restrict government access to name and address information held by utility company); State v. Faydo, 846 P.2d 539, 541 (Wash. Ct. App. 1993) (refusing to restrict government access to name held by phone company because "[h]is identity is not 'private' in the same sense as is a record of the phone numbers dialed on a subscriber's phone").

Some courts have restricted access to *unlisted* name and address information. *See, e.g.*, People v. Chapman, 679 P.2d 62, 71 (Cal. 1984); State v. Butterworth, 737 P.2d 1297, 1301 (Wash. Ct. App. 1987). The distinction is probably not how personal the information is—although perhaps that does vary when a telephone number is affirmatively not disclosed—but rather that other factors come into play, such as contractual guarantees and a disclosing party's expectations. *See* Factor 4, *infra* Part III.D; Factor 5, *infra* Part III.E; Factor 6, *infra* Part III.F.

111. *In re* Maxfield, 945 P.2d 196, 207 (Wash. 1997) (Guy, J., dissenting) (Justice Guy wrote for a majority of five justices refusing to restrict access to power consumption information: "A statement that power consumption at a particular address appears to be high discloses no discrete information about an individual's activities, not even the individual's name. . . . The information did not provide any intimate details of the [defendants'] lives or identify their friends or political and business associates. Electrical consumption information, unlike telephone or bank records or garbage, does not reveal discrete information about a customer's activities."); State v. Kluss, 867 P.2d 247, 254 (Idaho Ct. App. 1993); People v. Dunkin, 888 P.2d 305, 308 (Colo. Ct. App. 1994) (adopting reasoning of *Kluss*); Samson v. State, 919 P.2d 171, 173 (Alaska Ct. App. 1996). Although it left the ultimate issue undecided, the New Jersey Supreme Court recently recognized this distinction as well. *See* State v. Domicz, 907 A.2d 395, 403 (N.J. 2006).

112. State v. McKinney, 60 P.3d 46, 51 (Wash. 2002) ("[T]he information kept in the drivers' license records does not reveal intimate details of the defendants' lives, their activities, or the identity of their friends or political and business associates. The only information accessed by police from the . . . records were the names and addresses of the registered owners associated with license plate numbers, physical descriptions, and license status.").

113. State v. Granville, 142 P.3d 933, 941 (N.M. Ct. App. 2006) ("The contents of a person's garbage are evidence of his most private traits and intimate affairs. A search of one's garbage can reveal eating, reading, and recreational habits; sexual and personal hygiene practices; information about one's health, finances, and professional status; details regarding political preferences and romantic and other personal relationships; and a person's own private thoughts, activities, beliefs, and associations. Almost every human activity ultimately manifests itself in waste products, and any individual may understandably wish to maintain the confidentiality of his refuse.") (internal quotation marks and citation omitted), *cert. granted*, 2006 N.M. Lexis 379 (Aug. 22, 2006) (No. 29,890); State v. Tanaka, 701 P.2d 1274, 1276-77 (Haw. 1985); *Hempele*, 576 A.2d at 802-03; State v. Morris, 680 A.2d 90, 94 (Vt. 1996); *see also* People v. Hillman, 834 P.2d 1271, 1281 (Colo. 1992) (Quinn, J., dissenting). The intimate nature of our garbage is well demonstrated by an Oregon investigation in which police utilized a garbage pull to obtain a blood-soaked tampon which they tested for drugs, DNA, and seminal fluid. *See* State v. Galloway, 109 P.3d 383, 384 (Or. Ct. App. 2005). *Cf.* People v. Abbott, 162 Cal. App. 3d 635, 640 (Cal. Ct. App. 1984) ("Dealing with a

Illinois employs a bifurcated approach that explicitly requires courts to distinguish between and among information based on its "private" nature. Illinois' constitutional analog is textually similar to the Fourth Amendment with the addition of explicit protection against "invasions of privacy."[114] The courts therefore apply a "limited lockstep" approach for "ordinary" search and seizure situations,[115] but grant greater protection than the Fourth Amendment when the government seeks to acquire "private records or documents or information of the type typically contained therein."[116] Therefore not all third-party information will be protected, but only that deemed sufficiently private, and increasing restrictions will be imposed as the government seeks increasingly personal information.[117]

The Fourth Amendment should likewise account for this differing personal nature. Of course it does not follow that there must be a different standard for every different type of information. Large classes of information may be able to be considered together, such as the recognized distinction between less personal internal records of business organizations and their more personal private counterparts.[118]

C. *Factor 3. The Amount of Information*

Although it may be difficult to determine which of two types of information is more personal, it should be less controversial to assert that it is a greater invasion to obtain them both. Although it does not necessarily follow that the difference is sufficient to justify a greater government restraint, it is clear one relevant factor is the amount of information the government wishes to acquire. It was important to the *Burrows* court that "the totality of bank records provides a virtual current biography,"[119] and

---

locksmith, one does not reveal many aspects of his [or her] personal affairs, opinions, habits, and associations.") (internal quotation marks omitted).

114. ILL. CONST. art. I, § 6.

115. *See* People v. Caballes, 851 N.E.2d 26, 44 (Ill. 2006).

116. *Id.* at 52-53.

117. *Id.* at 49. Thus in a non-third-party context in which a grand jury was seeking varied information from a suspect, the Illinois Supreme Court "established a continuum of privacy protections—from mere relevance, to relevance plus individualized suspicion, to probable cause—depending on the degree of intrusiveness of the grand jury's inquiry." *Id.*

118. *See* Slobogin, *supra* note 9, at 170-73 (describing and agreeing with the Supreme Court's differentiation).

119. Burrows v. Superior Court, 529 P.2d 590, 596 (Cal. 1974); *see also* People v. Blair, 602 P.2d 738, 745 (Cal. 1979) (noting that credit card statements can similarly provide a "virtual current biography"). *Cf.* People v. Abbott, 162 Cal. App. 3d 635, 640 ("We cannot conclude the location of a safe has anything to do with providing government a 'virtual current biography.'").

other courts have followed suit with respect to searches of bank records[120] and telephone dialing records,[121] location tracking,[122] garbage pulls,[123] and searches of employment records.[124] Illinois courts have expressed the concern that absent constitutional constraint the government would establish a "general information bank" into which more and more information could be stored.[125]

This factor is intimately tied to the previous one, because typically the more information that is obtained, the more the government will be able to

120. People v. Jackson, 452 N.E.2d 85, 89 (Ill. App. Ct. 1983) ("We believe that it is reasonable for our citizens to expect that their bank records will be protected from disclosure because in the course of bank dealings, a depositor reveals many aspects of her personal affairs, opinion, habit and associations which provide a current biography of her activities."); State v. McAllister, 875 A.2d 866, 874 (N.J. 2005) ("[B]ank records are simply a collection of numbers, symbols, dates, and tables. They are a veritable chronicle of the mundane . . . . However, when compiled and indexed, individually trivial transactions take on a far greater significance. . . . 'Indeed, the totality of bank records provides a virtual current biography.'") (quoting *Burrows*, 529 P.2d at 596); State v. Domicz, 907 A.2d 395, 403 (N.J. 2006) (distinguishing bank records from utility records on this basis).

121. People v. DeLaire, 610 N.E.2d 1277, 1282 (Ill. App. Ct. 1993) ("[T]he [dialing] records revealed personal associations and dealings which create a 'biography' which should not be subject to an unreasonable search or seizure."); People v. Sporleder, 666 P.2d 135, 142 (Colo. 1983) ("[A] pen register record holds out the prospect of an even greater intrusion in privacy when the record itself is acquired by the government, which has a technological capacity to convert basic data into a virtual mosaic of a person's life.").

122. People v. Oates, 698 P.2d 811, 817 (Colo. 1985) ("Knowing the movements of an item and its possessor may permit the government to reconstruct a virtual mosaic of a person's life, including one's habits, habitats and associates.") (internal quotation marks and citation omitted); State v. Jackson, 76 P.3d 217, 223 (Wash. 2003) ("Moreover, the intrusion into private affairs made possible with a GPS device is quite extensive as the information obtained can disclose a great deal about an individual's life. For example, the device can provide a detailed record of travel to doctors' offices, banks, gambling casinos, tanning salons, places of worship, political party meetings, bars, grocery stores, exercise gyms, places where children are dropped off for school, play, or day care, the upper scale restaurant and the fast food restaurant, the strip club, the opera, the baseball game, the 'wrong' side of town, the family planning clinic, the labor rally. In this age, vehicles are used to take people to a vast number of places that can reveal preferences, alignments, associations, personal ails and foibles. The GPS tracking devices record all of these travels, and thus can provide a detailed picture of one's life.").

123. State v. Hempele, 576 A.2d 793, 802-03 (N.J. 1990) ("A plethora of personal information can be culled from garbage.").

124. Mont. Human Rights Div. v. City of Billings, 649 P.2d 1283, 1287 (Mont. 1982) ("Employment records would reasonably contain, among less sensitive information, references to family problems, health problems, past and present employers' criticism and observations, military records, scores from IQ tests and performance tests, prison records, drug or alcohol problems, and other matters, many of which most individuals would not willingly disclose publicly.").

125. People v. Caballes, 851 N.E.2d 26, 47 (Ill. 2006) ("The clause creating an additional right to privacy . . . was added to [the state analog] in response to a concern that the government might use newly available technology to develop 'a general information bank' that would collect and monitor personal information."); Small v. Kusper, 513 N.E.2d 1108, 1110 (Ill. App. Ct. 1987) ("[W]e have now the concept of a general information bank whereby the state government or the federal government can take certain pertinent information about each and every one of us based on, for instance, our social security number—know our weight, height, family ages, various things about us—and this . . . was not acceptable to the majority of our committee in approving [the additional right].")

discern about the target's life, and therefore the more personal the information considered in totality. Thus the Washington Supreme Court has "noted that the nature *and* extent of information obtained by the police . . . is relevant."[126] The two factors are complementary, and often will be applied together.

So far this assumes that police are requesting data relating to a single person from the third party to which it was disclosed, and that the third party need not sort through other information to produce it. To produce a suspect's bank statements a bank need not sort through unrelated information on the suspect, nor banking or other information relating to other persons, because the bank already catalogs the relevant information by individual. Thus the type and amount of information are readily discerned. However, none of these constraints are necessarily true of a government request.

What if police want to know who received deposits of $100,000 or more in the last year, or the names of all people purchasing Bruno Magli shoes? Is the "amount" of information greater? In one sense, the answer must be in the affirmative. It is intrusive of more persons' privacy to obtain a list of all persons who have purchased such shoes than to inquire whether one particular person has made such a purchase. But it is also a more focused inquiry. Rather than request all records relating to a single person, the police have requested information on one particular transaction. I believe both considerations are relevant and that courts should be willing to constitutionally regulate such "event-based" searches.[127] Obviously police cannot be required to have or demonstrate a belief that a known person committed an offense, as that is what this type of search is intended to yield. But courts can require that police have reason to believe a crime has been committed and that the information will assist in that investigation.[128]

What if police want to know whether a particular suspect received a large deposit within the past year, purchased Bruno Magli shoes, and had cellular service? If three officers split the tasks, one traveling to the bank, one to the shoe store, and one to the phone company, the "type" and

126. *Jackson*, 76 P.3d at 222 (emphasis added).

127. I take the term "event-based" from Professor Slobogin, whose proposal I consider *infra* Part IV. The alternative is the "target-based" search, in which police seek information relating to a known person.

128. Thus where police require evidence (such as a DNA sample) from a non-supect to prove a suspect's guilt, courts have required that the government demonstrate "probable cause to believe a crime was committed, and that the sample will probably provide evidence relevant to the question of the [suspect's] guilt." Commonwealth v. Draheim, 849 N.E.2d 823, 829 (Mass. 2006). Massachusetts courts also consider "the seriousness of the crime, the importance of the evidence, and the unavailability of less intrusive means of obtaining it . . . ." *Id.*

"amount" of information is clear in each case, and the requisite restraint might vary accordingly. Imagine that there becomes a single source from which police can obtain all three pieces of information, either a private or government data broker. Obviously the restraint on utilizing that service cannot be less than the greatest individual restraint on the three independent acquisitions. But could it ever be more? I believe it could on appropriate facts. The acquisition of a large amount of individually-less-intrusive information might go a long way to creating a "virtual current biography." That police could avoid such an "extra" restraint by compiling the information from disparate sources is not troubling, because there are resource constraints limiting such multiple acquisitions.[129]

Finally, what if the police seek very limited information, but its derivation requires mining significant information? Government entities and private companies are developing massive databases that aggregate diverse and disparate information on vast numbers of people.[130] If the broker uses artificial intelligence software to compile a list of suspects based on known facts of a crime,[131] is the search minimally intrusive because it yields only names and addresses, which are typically unprotected? Or is it instead dispositive that the system searched through real estate, banking, credit card, retail, and other records?

Typically we are concerned about searches because of the information they look through, not because of the information they seek. Although search and seizure jurisprudence no longer has a "mere evidence" limitation,[132] it is of course still commonplace to search for fruits of crime, contraband, and instrumentalities of crime. It is not those things that are private, but rather what the police might have to look through to find them. Thus searching for a gun in a home is more restricted than searching for a gun in a car, only the former being protected by a warrant requirement.[133] The gun does not become more private upon entering the home; instead what would be searched through in order to locate the gun is considered more private. Thus if police want to search *through* private information, it is the characteristics of that information (via the factors discussed in this article) that are to be considered in formulating the requisite government restraint.

---

129. *See* William J. Stuntz, *The Distribution of Fourth Amendment Privacy*, 67 GEO. WASH. L. REV. 1265, 1277 (1999) (recognizing both resource and legal restraints on police conduct).

130. *See generally* ROBERT O'HARROW, JR., NO PLACE TO HIDE (2005) (describing in significant detail the rise of the modern data broker); Henderson, *supra* note 7, at 390-92; Thai, *supra* note 100, at 1736-41.

131. For a description of such software in action see O'HARROW, *supra* note 130, at 56-57, 100-02.

132. *Warden v. Hayden*, 387 U.S. 294, 301-02, 309-10 (1967).

133. *See Payton v. New York*, 445 U.S. 573, 602-03 (1980) (generally requiring warrant supported by probable cause for entrance to home); *California v. Acevedo*, 500 U.S. 565, 579 (1991) (requiring only probable cause to search automobile).

The one exception to this rule is reflected in existing jurisprudence. Although a canine sniff might search "through" private things (by detecting odors that emanate from them), an accurate sniff detects only contraband.[134] Humans gain no information about other contents, neither through direct exposure nor indirectly through knowledge of a search algorithm combined with the results it produced. Thus it is not surprising that some states that have rejected the federal third-party doctrine nonetheless have agreed that a dog sniff of inanimate objects does not constitute a search.[135]

D. Factor 4. The Expectations of the Disclosing Party

According to the Supreme Court, Fourth Amendment protections depend upon expectations of privacy, and, as discussed above,[136] "[e]xpectations of privacy are established by general social norms"[137] or "societal understanding[s]."[138] Thus in initially refusing to find a reasonable expectation of privacy in a workplace computer, the Ninth Circuit looked to the prevalence of workplace monitoring and concluded that "[s]ocial norms suggest that employees are not entitled to privacy in the use of workplace computers . . . ."[139] Although I am not in favor of the duplicative expectation of privacy framework,[140] I agree that one factor in the reasonableness inquiry should be what persons typically expect when making the relevant disclosure.[141]

---

134. *See* United States v. Place, 462 U.S. 696, 707 (1983) (holding canine sniff does not constitute a Fourth Amendment search); Illinois v. Caballes, 543 U.S. 405, 409 (2005) (same).

135. *E.g.*, State v. Scheetz, 950 P.2d 722, 727-28 (Mont. 1997) (sniff of luggage); People v. Mayberry, 644 P.2d 810 (Cal. 1982) (sniff of luggage); People v. Caballes, 851 N.E.2d 26, 55 (Ill. 2006) (sniff of vehicle exterior); State v. Cancel, 607 A.2d 199, 203 (N.J. Super. Ct. App. Div. 1992) (sniff of luggage). Other jurisdictions nonetheless deem canine sniffs to be regulated searches, but typically allow them upon reasonable suspicion given their "inherently less intrusive" nature. *See, e.g.*, Commonwealth v. Rogers, 849 A.2d 1185, 1190-91 (Pa. 2004).

136. *See supra* note 54 and accompanying text.

137. Robbins v. California, 453 U.S. 420, 428 (1981) (plurality opinion), *overruled on other grounds*, United States v. Ross, 456 U.S. 798 (1982).

138. California v. Greenwood, 486 U.S. 35, 43 (1988).

139. United States v. Ziegler, 456 F.3d 1138, 1145-46 (9th Cir. 2006). Given Supreme Court jurisprudence that an employee has a reasonable expectation of privacy in an office, however, the Ninth Circuit panel withdrew this opinion, held that the employee *did* have an expectation of privacy, and instead permitted the search based on employer consent. United States v. Ziegler, 474 F.3d 1184 (9th Cir. 2007).

140. I am in favor of a dictionary definition of "search" accompanied by an encompassing "reasonableness" determination. The current formulation instead artificially restricts the definition of "search" but smuggles a portion of the reasonableness determination into the "reasonable expectation of privacy" criterion. *See* Henderson, *supra* note 85, at 544-46.

141. However, even a negative expectation (meaning people do *not* expect information to remain private) should not necessarily be determinative. The last five years have made it is easy to see how,

I part with the High Court, however, on its refusal to determine those expectations in any rational manner. Rather than grapple with the complications of surveys or other evidence, the Court has been content to declare societal expectations without any foundation or support. Even if it were true that "subjective expectations cannot be scientifically gauged,"[142] surely the attempt would come closer to the mark than Justices reading phone books and asserting what people take from that text[143] or merely assuming how people react when faced with conflicting invitations to enter a dwelling.[144] Either courts should look to academic empirical studies like those done by Professor Slobogin[145] (in which case we need more like them), or litigants should prepare relevant surveys as they do in other areas of law, such as trademark. Ideally both should occur.

The Court has engaged in a limited form of empirics in that it will look to the decisions of state and lower federal courts. For example, in holding that there is no Fourth Amendment protection for garbage left for collection, the Court relied in part on "the unanimous rejection of similar claims by the

---

in a world of significant danger and aggressive police, people might begin to expect less than they should of a democratic society.

> It is always somewhat dangerous to ground exceptions to constitutional protections in the social norms of a given historical moment. The purpose of the Fourth Amendment's requirement of reasonableness "is to preserve that degree of respect for the privacy of persons and the inviolability of their property that existed when the provision was adopted--even if a later, less virtuous age should become accustomed to considering all sorts of intrusion 'reasonable.'"

Richard v. Wisconsin, 520 U.S. 385, 392 n.4 (1997) (quoting Minnesota v. Dickerson, 508 U.S. 366, 380 (1993) (Scalia, J., concurring)).

Although I deem current expectations relevant, Justice Harlan was correct that "[s]ince it is the task of the law to form and project, as well as mirror and reflect, we should not . . . merely recite the expectations and risks without examining the desirability of saddling them upon society." United States v. White, 401 U.S. 745, 786 (Harlan, J., dissenting); *accord* Smith v. Maryland, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting) ("In my view, whether privacy expectations are legitimate within the meaning of *Katz* depends not on the risks an individual can be presumed to accept when imparting information to third parties, but on the risks he should be forced to assume in a free and open society."); State v. Butterworth, 737 P.2d 1297, 1298-99 (Wash. Ct. App. 1987) ("The privacy protections of our state constitution encompass more than the defendant's merely subjective expectations, which may depend on such things as advances in surveillance technology, and may, moreover, be subject to manipulation by police and other agents of the state. Instead, the appropriate analysis . . . focuses on those privacy interests which citizens of this state have held, and should be entitled to hold, safe from governmental trespass absent a warrant.") (internal citation and quotation marks omitted). To the extent people's expectations are formed by police conduct, see *infra* Part III.M.

142. *Smith*, 442 U.S. at 743.

143. *See id.* at 742-43 (concluding that telephone users "typically know" information such that they do not harbor any expectation that the numbers they dial will remain private). Justice Marshall chided the majority for this baseless assertion: "Lacking the Court's apparently exhaustive knowledge of this Nation's telephone books and the reading habits of telephone subscribers . . . . I decline to assume general public awareness of how obscene phone calls are traced." *Id.* at 749 n.1 (Marshall, J., dissenting).

144. *See supra* note 57 and accompanying text.

145. *See* Slobogin & Schumacher, *supra* note 58; Slobogin, *supra* note 58.

Federal Courts of Appeals" and a similar rejection by "the vast majority" of state appellate courts.[146] Of course, for this type of "empirical analysis" to be sound, those state and federal decisions should be based on more than mere judicial assertion, and they typically are not. For example, when New Jersey diverged from the federal doctrine, the court asserted that "many would be upset to see a neighbor or stranger sifting through their garbage."[147] This is my intuition and experience as well, but neither is a satisfactory ground for asserting what is the *typical* societal expectation.

A related inquiry that should be reflected in the results of an empirical study is whether information is accessible to, and accessed by, private persons. If unrelated private parties routinely access the relevant information, perhaps because it is in plain view in an area they frequent, because they carry a certain device,[148] or because they look up certain information on the Internet, then I agree with the Court that police officers need not "shield their eyes"[149] from that same information. The paradigm of this category might be name and address information[150] or vehicle license plates.[151] Both types of information are routinely acquired by the public, and hence there is no restriction on law enforcement doing the same. Thus the *Kyllo* Court was right to consider "general public use" when deciding whether to restrict government use of technologies,[152] despite its having

146. California v. Greenwood, 486 U.S. 35, 41-42 (1988). For three other examples of the Supreme Court looking to state decisions and trends therein, see Henderson, *supra* note 7, at 374-75.

147. State v. Hempele, 576 A.2d 793, 803 (N.J. 1990). This type of assertion is not at all unusual. Note the similarly unfounded assertion in the Montana Supreme Court's grant of constitutional protection to employer records: "[W]hile, as far as we know, [the employers] gave their employees no specific assurances of confidentiality, we believe that employees would reasonably expect such communication normally would be kept confidential." Mont. Human Rights Div. v. City of Billings, 649 P.2d 1283, 1287-88 (Mont. 1982). How do they know?

148. For example, a thermal imager, *see* Kyllo v. United States, 533 U.S. 27, 29-30 (2001), or a passive millimeter wave camera, *see* Henderson, *supra* note 85, at 535-36.

149. *Kyllo*, 533 U.S. at 32 (quoting California v. Ciraolo, 476 U.S. 207, 213 (1986)).

150. *See* Commonwealth v. Duncan, 817 A.2d 455, 465-66 (Pa. 2003) ("[I]t is all but impossible to live in our current society without repeated disclosure of one's name and address, both privately and publicly. . . . In this day and age where people routinely disclose their names and addresses to all manner of public and private entities, this information often appears in government records, telephone directories, and numerous other documents that are readily accessible to the public, and where customer lists are regularly sold to marketing firms and other businesses, an individual cannot reasonably expect that his identity and home address will remain secret . . . ."); *accord* State v. Chryst, 793 P.2d 538, 542 (Alaska App. 1990) (refusing to restrict government access to name and address information held by utility company); State v. Faydo, 846 P.2d 539, 541 (Wash. Ct. App. 1993) (refusing to restrict government access to name held by phone company).

151. *See* State v. Richter, 765 A.2d 687, 688 (N.H. 2000) (allowing random computer checks of license plates so read).

152. *Kyllo*, 533 U.S. at 40 (holding that "[w]here . . . the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable

been criticized by the dissenters[153] and some commentators.[154] Indeed, this is the proper interpretation of *Katz*' construct that "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection,"[155] rather than the Court's tortured interpretation in cases like *Miller*.[156]

For example, flashlights are significantly publicly available *and* publicly used such that law enforcement's use should not be restricted, and the Supreme Court has so recognized.[157] But the Court has at times left out a critical portion of this criterion, as evidenced by its language in *Greenwood* that "the police cannot reasonably be expected to avert their eyes from evidence of criminal activity that *could have been observed* by any member of the public."[158] It is not sufficient that members of the public *could* observe the information. Instead, it is necessary that members of the public *do* observe the information. When private persons could, but do not, access given information, such practical obscurity renders it effectively private. If private persons in fact do not regularly rifle through others' garbage, this weighs in favor of restricting government access.[159] If fellow travelers do not regularly feel others' carry-on bags "in an exploratory manner,"[160] this weighs in favor of restricting law enforcement from doing the same. If private persons do not regularly approach homes at midnight and shine

---

without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant.").

153. *See id.* at 39 n.6, 46-47 (Stevens, J., dissenting).

154. *See* Christopher Slobogin, *Peeping Techno-Toms and the Fourth Amendment: Seeing Through* Kyllo*'s Rules Governing Technological Surveillance*, 86 MINN. L. REV. 1393, 1394 (2002). Despite our different conclusion, there is much in Slobogin's article with which I agree, such as his emphasis on better defining what constitutes "general public use." *See id.* at 1402-06.

155. Katz v. United States, 389 U.S. 347, 351 (1967).

156. United States v. Miller, 425 U.S. 435, 442 (1976).

157. United States v. Dunn, 480 U.S. 294, 304-05 (1987); *accord* State v. Jackson, 76 P.3d 217, 222 (Wash. 2003). The Supreme Court of Washington relies on whether a technological enhancement is a "particularly intrusive method of viewing," which in my mind would equate to whether it is in general public use, at least when positive law prohibitions are considered. *See id.*

158. Greenwood v. California, 486 U.S. 35, 41 (1988) (emphasis added). The Court concluded "that society would not accept as reasonable respondents' claim to an expectation of privacy in trash left for collection in an area accessible to the public." *Id.* The Court should have required that it be accessible to *and often accessed by* the public.

159. As the New Jersey Supreme Court has pointed out, with respect to garbage left for collection in opaque bags, what is relevant is not the "knowingly exposes" language of *Katz* but instead the very next sentence of that opinion, namely that "what a person . . . seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." State v. Hempele, 576 A.2d 793, 807 (N.J. 1990) (quoting *Katz*, 389 U.S. at 351); *see also Greenwood*, 486 U.S. at 54 (Brennan, J., dissenting) ("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.").

160. Bond v. United States, 529 U.S. 334, 339 (2000) (holding such a squeeze unconstitutional).

flashlights in vehicles left on a driveway, this weighs in favor of restricting law enforcement from that conduct.[161] To risk a glib example, one's undergarments are "accessible" to the public—it often would not be hard to yank down someone's pants—but apart from the Harlem Globetrotters and perhaps Dennis Rodman, people refrain from doing so because it is normatively unacceptable. Therefore undergarments remain effectively private.[162] Because the government has reasons and resources to look where others do not, the mere potential for private consumption is not sufficient.

This criterion is reflected in state court opinions concerning garbage. Although the Colorado Supreme Court had previously diverged from federal doctrine with respect to electronic tracking,[163] telephone records,[164] and bank records,[165] a divided court decided not to restrict police access to garbage.[166] According to the majority, contrary to these other instances, people are aware that fellow members of the public might snoop in their garbage.[167] In fact, according to the court "it is 'common knowledge' that members of the public often sort through other people's garbage."[168] In the words of the Connecticut Supreme Court, "[a] person's reasonable expectations as to a particular object cannot be compartmentalized so as to restrain the police from acting as others in society are permitted or suffered to act."[169] Although in my experience in suburban locales such access is thankfully rare,[170] if such access were known to be commonplace it would

161. *Cf.* United States v. Carter, 360 F.3d 1235, 1239 (10th Cir. 2004) (asserting that such conduct "do[es] not implicate the Fourth Amendment").

162. As should activity undertaken in public restroom stalls, even though private persons *could* peer inside.

163. People v. Oates, 698 P.2d 811, 815-18 (Colo. 1985).

164. People v. Timmons, 690 P.2d 213, 215 (Colo. 1984); People v. Corr, 682 P.2d 20, 26-27 (Colo. 1984); People v. Sporleder, 666 P.2d 135, 144 (Colo. 1983).

165. People v. Lamb, 732 P.2d 1216, 1220-21 (Colo. 1987); Benson v. People, 703 P.2d 1274, 1278 (Colo. 1985); Charnes v. DiGiacomo, 612 P.2d 1117, 1120 (Colo. 1980).

166. People v. Hillman, 834 P.2d 1271 (Colo. 1992). The state of Idaho later adopted the reasoning of *Hillman* in *State v. Donato*, 20 P.3d 5, 9-10 (Idaho 2001).

167. *Hillman*, 834 P.2d at 1277 n.14.

168. *Id.* at 1275 (quoting United States v. Hedrick, 922 F.2d 396, 399 (7th Cir. 1991)). The Seventh Circuit cited *Greenwood* for this proposition. *Id.*; *see also* State v. 1993 Chevrolet Pickup, 116 P.3d 800, 804 (Mont. 2005) ("While garbage bags oftentimes remain intact until their contents are collected by a designated hauler, it is also common to see homeless people, stray pets and wildlife, curious children, and scavengers rummaging through trash set out for collection."). An appellate court in Colorado similarly declined to restrict access to utility records in part because "unlike telephone and bank records, utility records can be obtained by other members of the public such as real estate salespersons or a prospective purchaser of a home." People v. Dunkin, 888 P.2d 305, 308 (Colo. App. 1994).

169. State v. DeFusco, 620 A.2d 746, 752 (Conn. 1993).

170. The experience of some justices is nearer to my own: "[T]he Court similarly overstates its

weigh in favor of similarly unfettered government access.[171] "[I]n applying the Fourth Amendment we take societal expectations as they are, not as they could or (some think) should be."[172]

To be relevant, however, the private access should be as intrusive as that desired by law enforcement. A mere glance by the public should not be equated to an exhaustive search by the government. Thus in *Bond v. United States*[173] the Court distinguished an agent's probing squeeze of carry-on luggage from that contact to be expected from fellow travelers.[174] And there may be circumstances in which law enforcement should be restricted where only a limited class of private persons has access to the information. In the words of an Oregon appellate court,

> A person may not expect privacy in his open field or backyard as against children at play or parents looking for lost or tardy children. Yet he may subjectively expect and objectively be entitled to expect privacy as against policemen making a "dragnet" search of a whole group of private fields or a whole neighborhood of backyards in the

---

case when it claims that garbage cans '[r]outinely . . . are knocked over' and their contents 'strewn across streets and alleyways.' Our cities' thoroughfares are not, I am happy to report, awash in garbage." *1993 Chevrolet Pickup*, 116 P.3d at 809 (Leaphart, J., dissenting). In restricting government access to utility records an appellate court in New Jersey did not believe the state's "unsupported assertion" that members of the public could freely inspect such records. State v. Domicz, 873 A.2d 630 (N.J. App. 2005), *rev'd on other grounds*, 907 A.2d 395 (N.J. 2006).

171. The Supreme Court of Montana has applied this factor to the luggage of an airplane traveler:

> [T]he luggage that a person brings to the airport is generally subject to observation by the public or the state . . . . For example, a person cannot expect to conceal completely from the public the odor of the luggage or its contents, its color, or even its weight since it must be handled by others. Accordingly, we conclude that a person lacks a reasonable expectation of privacy in the smell of luggage that he or she brings to an airport in the same way that he or she lacks an expectation of privacy in the color or weight of the luggage. . . . Accordingly, we conclude that a person does not maintain a sufficient expectation of privacy in luggage entrusted to an airline that the Montana Constitution prohibits inspection of that luggage by a dog trained to detect the presence of drugs by sniffing the luggage.

State v. Scheetz, 950 P.2d 722, 727 (Mont. 1997). As the dissent in this case pointed out, however, this is a poor application of this principle because unlike color or weight, a person's olfactory senses are not sensitive enough to detect the relevant contraband, and therefore that information will not be obtained by other persons. *Id.* at 729-30 (Leaphart, J., dissenting). The court seemed to recognize this mistake in time, because it later held that a canine sniff of a vehicle exterior in a publicly accessible location was nonetheless a search requiring reasonable suspicion. State v. Tackitt, 67 P.3d 295, 300-02 (Mont. 2003).

172. United States v. Ziegler, 456 F.3d 1138, 1145 (9th Cir. 2006) (finding no reasonable expectation of privacy in workplace computer), *withdrawn by* 474 F.3d 1184 (finding expectation of privacy but also sufficient employer consent). However, a negative expectation should not always be determinative. *See* discussion *supra* note 147.

173. 529 U.S. 334 (2000).

174. *Id.* at 338-39.

> assumption that if they search long enough and far enough they will find some evidence of some crime.[175]

Although I believe it will typically be sufficient under this factor to restrict law enforcement access to the level of scrutiny given privately,[176] there may be some circumstances in which government access should be even more restricted, as in an office context in which only a limited number of coworkers enjoy access.[177]

Finally, even consistent access by private persons to the same degree desired by law enforcement would not always be dispositive. That private persons gain *unlawful* access to information, perhaps via computer hacking or traditional thievery, should not be relevant. We should be able to expect law enforcement to obey positive law, despite the Supreme Court's declaration to the contrary with respect to trespassing on fenced and posted private property that the Court nonetheless considers "open fields."[178]

E. Factor 5. The Understanding of the Third Party

If the third party generally considers the information confidential, this weighs in favor of restricting government access. In an obvious example, courts have distinguished between access to a listed name held by a phone company from access to an unlisted name.[179] Moreover, it is erroneous to

---

175. State v. Stanton, 490 P.2d 1274, 1279 (Or. App. 1971) (nonetheless finding no restriction because the area of interest was open to a "substantial segment of the public"), *overruled to the extent inconsistent by* State v. Walle, 630 P.2d 377 (Or. App. 1981) (holding one can have a legitimate expectation of privacy in open fields).

176. *See* State v. Hempele, 576 A.2d 793, 805 (N.J. 1990) ("Although a person may realize that an unwelcome scavenger might sort through his or her garbage, such expectations would not necessarily include a detailed, systematized inspection of the garbage by law enforcement personnel.") (internal quotation marks omitted).

177. *See id.* at 804 (discussing O'Connor v. Ortega, 480 U.S. 709 (1987)).

178. *See* Oliver v. United States, 466 U.S. 170, 183-84 (U.S. 1984) (holding there is no restriction on police entry to "open fields" despite the contrary law of criminal trespass). The Supreme Court of Hawaii has rejected a determinative "general public use" criterion, but recognizes that it might be a relevant factor in its state constitutional determination. State v. Detroy, 72 P.3d 485, 494 n.11 (Haw. 2003). Professor Slobogin, who is critical of the "general public use" limitation, agrees that positive law can ameliorate what he believes are its negative effects. *See* Slobogin, *supra* note 154, at 1433-37.

179. *See* State v. Faydo, 846 P.2d 539, 541 (Wash Ct. App. 1993). "[I]n this day and age in which private businesses routinely sell customer lists to other businesses, it is unreasonable to believe a customer's name and the names of others he lists at his residence for billing purposes will be kept private." *Id.*; *accord* Commonwealth v. Duncan, 817 A.2d 455, 465-66 (Pa. 2003) (refusing to restrict access to name and address information); State v. Chryst, 793 P.2d 538, 542 (Alaska Ct. App. 1990) (same).

The *Chryst* court asserted that "[t]he trial court's reliance on the internal policies adopted by

presume a third party does not consider information confidential merely because it complied with a law enforcement request. In *Burrows* at least one bank released the information upon mere oral request despite bank representatives' apparently uniform testimony that they deemed such customer information confidential.[180] Such compliance is probably typical of law-abiding persons and companies. Although not required,[181] express promises of confidentiality are obviously relevant to this inquiry.[182]

F. Factor 6. Positive Law Guarantees of Confidentiality

Violation of an explicit restriction on law enforcement conduct should rarely be "reasonable."[183] More generally, all statutory and common-law guarantees of confidentiality weigh in favor of constitutionally restricting government access.

For example, that some municipal ordinances permit only licensed collectors to acquire garbage left for collection, and sometimes restrict what those collectors may do with the refuse, weighs in favor of restricting access by law enforcement.[184] Even if the impetus for such laws was not to protect privacy but rather to further cleanliness or maintain an existing government monopoly, the laws affect people's perception of the privacy of garbage.[185]

[the utility] . . . is questionable. While [the utility's] disclosure policies would certainly be relevant to the issue of [a customer's] subjective expectations and might affect [a customer's] contractual rights . . . they cannot determine the scope of the constitutional right to privacy." *Id.* at 542 (Bryner, J., concurring). I agree that such policies are not determinative, but they are relevant. If nothing else, they give customers reason to presume the records will not typically be publicly accessible. *See* discussion *supra* Part III.D.

180. Burrows v. Superior Court, 529 P.2d 590, 593 (Cal. 1975).

181. *See* People v. Chapman, 679 P.2d 62, 68 (Cal. 1984) (granting protection for bank and telephone records despite no explicit promise of confidentiality).

182. State v. Hempele, 576 A.2d 793, 807 (N.J. 1990) ("It should be reasonable to expect that those who are authorized to remove trash will do so in the manner provided by ordinance or private contract."); People v. Sporleder, 666 P.2d 135, 141 (Colo. 1983) (noting that "telephone companies have not been insensitive to the confidentiality of this information," citing to restrictive provider policies).

183. A circumstance in which such conduct would be reasonable is if the executive branch has inherent and exclusive constitutional authority. See the discussion of warrantless wiretapping for purposes of national security *supra* Part II.

184. *See* California v. Greenwood, 486 U.S. 35, 52 (1988) (Brennan, J., dissenting); People v. Krivda, 486 P.2d 1262, 1268 (Cal. 1971), *vacated*, California v. Krivda, 409 U.S. 33 (1972) (Court was unable to determine whether decision depended on state or federal constitutional law), *reiterated in its entirety by* People v. Krivda, 504 P.2d 457 (Cal. 1973) (as a matter of state constitutional law); *Hempele*, 576 A.2d at 805, 808; State v. Boland, 800 P.2d 1112, 1114-15 (Wash. 1990); *see also* State v. Hunt, 450 A.2d 952, 955 (N.J. 1982) (noting long history of statutory protection for telephonic communications in New Jersey in deciding to restrict government access to telephone dialing information); State v. McAllister, 875 A.2d 866, 875 (N.J. 2005) (noting federal statutory law protecting the confidentiality of bank records in deciding to restrict government access to those records as a matter of state constitutional law).

185. *Hempele*, 576 A.2d at 808; *Boland*, 800 P.2d at 1115. Thus the ordinances affect Factor 4, *supra* Part III.D.

In the words of the Washington Supreme Court, "[s]tate law may be responsive to concerns of its citizens long before they are addressed by analogous constitutional claims. Preexisting law can thus help to define the scope of a constitutional right later established."[186] This seems especially apt when courts are called on to determine whether government conduct is "reasonable."

Just as the absence of statutory protection is not determinative of the constitutional rule,[187] legislatures cannot legislate the Fourth Amendment or a state analog out of existence.[188] But positive law requiring access, either explicitly or implicitly, weighs in favor of permitting requested law enforcement access. Thus the Connecticut Supreme Court refused to restrict police access to garbage in part on account of a law requiring garbage collectors to identify recycling violators,[189] and the Supreme Court of Pennsylvania relied in part on a statute requiring disclosure in refusing to constitutionally restrict law enforcement access to insurance company claim investigation files.[190]

---

186. State v. Gunwall, 720 P.2d 808, 812 (Wash. 1986). Thus in holding that the state constitution restricts government access to telephone numbers dialed, the court relied upon "[t]he long history and tradition of strict legislative protection of telephonic and other electronic communications in this state." *Id.* at 815. Four justices would have similarly granted protection to utility records based in part on existing statutory protection in *In Re Maxfield*, 945 P.2d 196, 200 (Wash. 1997), but other justices disagreed as to the import of the relevant legislation. *See id.* at 206-07 (Guy, J., dissenting).

187. *See* People v. Blair, 602 P.2d 738, 746 (Cal. 1979) ("[T]he rule . . . is based upon constitutional precepts. The mere fact that a statute does not regulate the circumstances under which a credit card company may furnish information regarding a customer to the police cannot be deemed controlling."). Such an absence can of course be relevant. *See* State v. Donato, 20 P.3d 5, 10 (Idaho 2001) (declining to find constitutional protection for garbage left for collection in part based on belief that telephone providers had a duty of confidentiality that was not placed upon garbage collectors).

188. *See Hempele*, 576 A.2d at 807-08 ("[A]lthough government regulation can reduce a privacy expectation, it cannot completely preclude the application of the protections of [our state analog]. Otherwise the government could repeal [the analog] through regulation.") (restricting government access to garbage despite such a law); State v. Butterworth, 737 P.2d 1297, 1300 (Wash. Ct. App. 1987) ("The Legislature may not confer upon the Utilities and Transportation Commission the judicial power to determine the constitutional rights of citizens. If citizens have a constitutionally protected privacy interest in their unpublished telephone listings, then the Commission cannot render warrantless disclosure of those listings lawful by the simple expedient of adopting a rule to that effect.") (restricting access to unlisted address and telephone number held by phone company).

189. State v. DeFusco, 620 A.2d 746, 751 (Conn. 1993).

190. Commonwealth v. Efaw, 774 A.2d 735, 739 (Pa. 2001); *see also* State v. McKinney, 60 P.3d at 49-50 (Wash. 2002) (refusing to restrict access to driver's license records in part because for most of Washington's relevant history statutes had required vehicle ownership information and records of traffic charges and dispositions to be available to the public).

G. *Factor 7. Government Need*

Fourth Amendment reasonableness (and reasonableness under its state analogs) requires a fit between the magnitude of the intrusion into privacy and the government need.[191] As a starting point, completely unfettered law enforcement access is strongly discouraged, because it allows officers to obtain information upon a whim or invidious motive.[192] In the words of the Pennsylvania Supreme Court, "it is our view that a free society will not remain free if police may use [canine sniffs], or any other crime detection device, at random and without reason."[193]

It is not the case that unrestricted access should never be permitted, but absent other determinative factors[194] there should be a strong presumption against such access, with the government bearing the burden of demonstrating that unfettered access is necessary to legitimate government functions.[195] More generally, the government is in the best position to carry the burden, so it should be up to the government to demonstrate that it requires access to information on anything less than a judicial determination of probable cause.[196] Judging from the significant amount of third-party

---

191. United States v. Knights, 534 U.S. 112, 118-19 (2001).

192. Thus the Supreme Court of Vermont refused to declare such an "open season" on garbage:

> [U]nconstrained government inspection of people's trash is not consistent with a free and open society. . . . While at first blush there may be a tendency to accept the notion that a person has no reasonable privacy interest in discarded trash, that attraction vanishes when one contemplates the "prospect of police officers, *without any cause whatever*, opening a securely tied and opaque trash bag, the contents of which are hidden from public view, and then searching the bag to determine the activities, behavior, habits, and lifestyles of persons who deposited the trash in front of their home for disposition by a trash collector."

State v. Morris, 680 A.2d 90, 94 (Vt. 1996) (emphasis added) (quoting People v. Hillman, 834 P.2d 1271, 1278 (Colo. 1992) (Quinn, J., dissenting); *accord* State v. Tanaka, 701 P.2d 1274, 1276 (Haw. 1985); State v. 1993 Chevrolet Pickup, 116 P.3d 800, 805 (Mont. 2005) (forbidding "random and arbitrary fishing expeditions through garbage"). The Supreme Court of Washington decided to restrict technologically-enhanced surveillance because otherwise "there would be no limitation on the State's use of these devices . . . whether criminal activity is suspected or not." State v. Jackson, 76 P.3d 217, 224 (Wash. 2003).

193. Commonwealth v. Johnson, 530 A.2d 74, 79 (Pa. 1987). Even when courts do not expressly condition government access, their language sometimes indicates that they would not permit unfettered access. Thus in refusing to restrain police in the questioning of a third-party locksmith, a California appellate court noted that the officers had not been on a "fishing expedition," but instead were following an investigative lead relating to a safe for which they already had a combination and already suspected a location. People v. Abbott, 208 Cal. Rptr. 738, 742 n.11 (1984). The implication is that if police took to routinely questioning locksmiths, or if on a hunch police obtained information from every person a suspect was known to do business with, the result might be different.

194. For example, if the desired information is routinely available to and lawfully accessed by unrelated private persons, unrestricted government access is appropriate. *See* Factor 4, *supra* Part III.D.

195. The *Burrows* court noted that the government did not even claim a need for unfettered access to bank records. Burrows v. Superior Court, 529 P.2d 590, 593 (Cal. 1974).

196. *See* People v. Oates, 698 P.2d 811, 818 n.7 (Colo. 1985) (noting that government did not

information that some jurisdictions protect via such a standard,[197] courts may find that legitimate law enforcement often does not require a lesser substantive burden. Even so, this would not require that acquisitions must proceed via search warrant. Typically the third party is not a suspect, and law enforcement will often prefer to proceed by the less disruptive subpoena.[198]

When a court finds the government has carried its burden and therefore allows access upon less than probable cause, it might nonetheless require

---

argue that any standard less than probable cause could suffice if the action constituted a search, and therefore requiring a search warrant supported by probable cause for the installation of an electronic beeper in a commercially-purchased item). The Supreme Court of Montana considered government need and Factors 2 and 3 in permitting canine sniffs upon reasonable suspicion:

> The government's interest in discouraging illegal drug trafficking is substantial. Further, this area of law enforcement involves investigation into trafficking activities that are difficult to detect because the activities are inherently transient and appear similar to innocent conduct on the surface. On the other side, as the facts of this case demonstrate, a search by a drug-detecting canine generally involves far less an intrusion than any other type of search technique and is uniquely selective, detecting in most cases only the presence of the particular type of contraband that the dog is trained to recognize. Accordingly, we hold that, given the greater protection afforded individual privacy under Montana's Constitution, the balance between governmental interests and individual interests in this case can best be struck by requiring particularized suspicion as a prerequisite for the use of a drug-detecting canine.

State v. Tackitt, 67 P.3d 295, 302 (Mont. 2003). In discussing whether a customer notice requirement should exist for grand jury subpoenas of bank records, the New Jersey Supreme Court considered investigations that require covert examination of such records, including money laundering, government corruption, identity theft, insurance fraud, and funding of terrorist activity. State v. McAllister, 875 A.2d 866, 879 (N.J. 2005).

197. *E.g.* People v. Krivda, 486 P.2d 1262, 1268 (Cal. 1971), *vacated*, California v. Krivda, 409 U.S. 39 (1972) (requiring judicial determination of probable cause to obtain garbage left for collection); People v. Larkin, 239 Cal. Rptr. 760, 762 (Cal. Ct. App. 1987) (same for pen register); People v. Blair, 602 P.2d 738, 745, 747 (Cal. 1979) (same for telephone and credit card records); People v. Chapman, 679 P.2d 62, 71 (Cal. 1984) (same for unlisted name and address from telephone company); People v. Mason, 989 P.2d 757, 760-62 (Colo. 1999) (requiring advance notice and probable cause for bank or telephone records obtained via trial subpoena but not probable cause for administrative subpoena and neither for grand jury subpoena); People v. Sporleder, 666 P.2d 135, 136 (Colo. 1983) (requiring search warrant supported by probable cause for pen register); *Tanaka*, 701 P.2d at 1277 (requiring warrant supported by probable cause for trash pull); State v. Rothman, 779 P.2d 1, 7-8 (Haw. 1989) (requiring warrant supported by probable cause for pen register); State v. Thompson, 760 P.2d 1162, 1167 (Idaho 1988) (requiring warrant supported by probable cause for pen register); State v. Hempele, 576 A.2d 793, 814 (N.J. 1990) (requiring warrant supported by probable cause for garbage search); Commonwealth v. Melilli, 555 A.2d 1254, 1256 (Pa. 1989) (requiring probable cause for installation of pen register); State v. Boland, 800 P.2d 1112, 1116 (Wash. 1990) (requiring warrant supported by probable cause for trash pull); State v. Morris, 680 A.2d 90, 100 (Vt. 1996) (requiring warrant supported by probable cause for garbage search).

198. Thus in California and Colorado the government can use a subpoena duces tecum to have protected records delivered to the court, but cannot access the records before demonstrating probable cause. *See Chapman*, 679 P.2d at 64 n.1; Carlson v. Superior Court, 129 Cal. Rptr. 650, 655 (Cal. Ct. App. 1976); *Mason*, 989 P.2d at 758.

judicial preclearance.[199] Because so much information can be acquired from third parties today (what courts have termed a "virtual current biography"[200] or a "virtual mosaic of a person's life"[201]), it may often be critical to have a court decide what access is reasonable in each circumstance. Merely because it is reasonable to obtain a suspect's phone records (perhaps including cell phone location information) does not mean that it is reasonable to obtain those records for the past ten years. In the words of the California Supreme Court, the "character, scope, and relevancy" of desired information should not be left solely to the "unbridled discretion of the police."[202] This concern does not apply when the scope of a search is naturally limited, as for canine sniffs that detect only contraband[203] or garbage pulls where police can only search that garbage currently left for collection.[204]

Finally, it is worth noting that the logical path to restricting government conduct on less than probable cause is to find that the challenged action constitutes a "search," but one that is nonetheless reasonable upon the lesser substantive burden. A few states have adopted a less rational path to achieve this same important result, which is to constitutionally restrict police conduct despite declaring that the conduct is *not* considered a "search."[205] Obviously this alternative approach does not commend itself, and should not be adopted in other jurisdictions.

---

199. For example, Florida seems to require a judicial determination of reasonable suspicion in order to install a pen register. Shaktman v. State, 553 So. 2d 148, 152 (Fla. 1989).

200. *Burrows*, 529 P.2d at 596.

201. *Oates*, 698 P.2d at 817.

202. *Chapman*, 679 P.2d at 71 (quoting *Burrows*, 529 P.2d at 590).

203. For example, Colorado requires reasonable suspicion for a dog sniff, even of vehicles, luggage, and other inanimate objects, but judicial preclearance is not required. *See* People v. Haley, 41 P.3d 666, 672 (Colo. 2001) (requiring reasonable suspicion for canine sniff of vehicle exterior when it prolongs a traffic stop); People v. May, 886 P.2d 280, 282 (Colo. 1994) (requiring reasonable suspicion for canine sniff of mail); People v. Boylan, 854 P.2d 807, 810 (Colo. 1993) (same for private courier); People v. Unruh, 713 P.2d 370, 377-79 (Colo. 1986) (requiring reasonable suspicion for canine sniff of safe stolen from home); People v. Wieser, 796 P.2d 982, 985-86 (Colo. 1990) (fractured decision regarding canine sniff of storage locker from public walkway).

204. For example, Indiana requires reasonable suspicion for garbage searches but no judicial preclearance. *See* Litchfield v. State, 824 N.E.2d 356, 363-64 (Ind. 2005).

205. *See* State v. Snitkin, 681 P.2d 980, 983-84 (Haw. 1984) (canine sniff); State v. Groves, 649 P.2d 366, 371-73 (Haw. 1982) (same); State v. 1993 Chevrolet Pickup, 116 P.3d 800, 805 (Mont. 2005) (trash pull). The Supreme Court of Idaho has insinuated the same, finding no constitutional protection for garbage left for collection but nonetheless going on to assert that a reliable informant tip in conjunction with knowledge of the defendant's prior drug involvement "gave the officers the right to make the trash pull." State v. McCall, 26 P.3d 1222, 1224 (Idaho 2001).

H. Factor 8. Personal Recollections

When the information sought is the personal recollection of a witness rather than a retained record, Professor Slobogin has persuasively argued that there is an autonomy interest that favors permitting unfettered access:

> Human information sources . . . should have a right to decide what to do with the information they possess; in such cases, the subject's privacy interest is outweighed by the source's autonomy interest. When the third party is an impersonal record-holder, on the other hand, concerns about denigrating "personhood" through limitations on when information may be revealed are non-existent. It is the absence of a legitimate third party interest in surrendering the target's private information . . . that distinguishes the records request scenario from the interview setting.[206]

I am not aware of courts explicitly making this distinction,[207] which builds on the work of Professor Mary Coombs,[208] but I think it absolutely right. Third parties should be permitted to share personal recollections and presumably also personal documents, such as private letters.

This is not to say, however, that an autonomy interest is without limit. Janet Randolph clearly had an autonomy interest in relating her experience with her husband's drug use.[209] Nonetheless, according to the Supreme Court, that interest was not sufficient to permit the further invasion of her inviting police into the couple's home over his objection.[210] In these circumstances I agree with the Court; Janet's autonomy interest was

206. Slobogin, *supra* note 9, at 185-86.

207. It is probably what an appellate court in California was trying to articulate when it declined to restrict police from interviewing a locksmith who had changed the combination on the defendant's safe: "The information is of an entirely different character emanating from a different *type* of source than that involved in [obtaining bank records, credit card records, and telephone records]. The locksmith was a *witness* in a criminal investigation." People v. Abbott, 208 Cal. Rptr. 738, 741 (Ct. App. 1984) (emphasis in original) (internal citation omitted). Although the opinion is not explicit, the court's language is consistent with the locksmith having remembered the information without consulting any documentation. *See id.* at 637. Even if that were the case, however, one could question whether a purely business association—even one requiring personal interaction—would suffice to create an autonomy interest sufficient to outweigh the disclosing party's privacy interest.

208. *See* Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 833-35 (2005); Mary I. Coombs, *Shared Privacy and the Fourth Amendment, or the Rights of Relationships*, 75 CAL. L. REV. 1593, 1643 (1987).

209. *See* Georgia v. Randolph, 126 S. Ct. 1515, 1519 (2006); *supra* notes 44-56 and accompanying text.

210. *See id.* at 1520.

sufficient for police to request her story, but not for them to enter the home without a warrant or exception to the warrant requirement.

But what if the third party is not the helpful sort, meaning he or she does not wish to disclose either record or recollection? Although the focus of this paper is the search and seizure rights of the disclosing party, for a moment it is instructive to consider those of the third party. Current law typically makes it easy to compel both record and recollection from a recalcitrant third party on pain of contempt. For example, law enforcement can often subpoena a witness to testify before, or produce documents to, a grand jury upon at most a very lenient standard of relevance and overbreadth.[211] Only if an answer would incriminate a witness can the witness decline to answer based upon the Fifth Amendment privilege against self-incrimination.[212] If police investigating a deviant rape want to question a suspect's former lover, answers to their questions might be extremely personal, but typically would not be incriminating.[213]

This article argues that law enforcement should be restricted in obtaining certain information from third parties, such as bank records. But could such a restriction be limited to the acquisition of records? What of the acquisition of mental recollections? Should law enforcement be permitted to compel a former lover to disclose the most intimate of recollections when it could not force a bank to disclose checks drawn on an account? Should agents be permitted to compel the contents of a personal letter via the recipient's recollection when they are unable to obtain the same information via the letter itself? I contend that neither would be acceptable, and therefore that the Fourth Amendment and its state analogs should restrict access to compelled third-party recollections.

This makes the adoption of a rational third-party doctrine more far-reaching than one might have imagined. And there is one more layer to unpeel. Only a bizarre jurisprudence would better protect information disclosed to a third party than information never disclosed. So if the law is to forbid unrestrained law enforcement access to certain third-party recollections, it must also forbid unfettered access to such "first-party recollections." Protecting third-party information should therefore lead to another significant shift in Fourth Amendment jurisprudence, namely adopting the proposal of Timothy O'Neill that government questioning

211. *See generally* WAYNE R. LAFAVE ET AL., 3 CRIMINAL PROCEDURE §§ 8.1, 8.7, 15.1(d)-(g) (2006); Slobogin, *supra* note 208, at 806.

212. The Fifth Amendment provides that "[n]o person shall be . . . compelled in any criminal case to be a witness against himself . . . ." U.S. CONST. amend. V.

213. LaFave does note that in some circumstances it is not uncommon for associates to make bogus, but not demonstrably bogus, assertions of their Fifth Amendment privilege, in which case the government might grant immunity to obtain the testimony. LAFAVE ET AL., *supra* note 211, at § 8.3(e).

constitutes a Fourth Amendment search.[214] In the context of police questioning of a suspect this would often be straightforward to implement, because stationhouse questioning requires either consent or probable cause, either of which would typically be sufficient.[215] But in the context of grand juries and other inquiries it could work a significant departure, although as in the case of records requests care must be taken not to unduly impede those inquiries to the extent they are necessary for the effective administration of the laws.[216]

Although courts are sensibly more willing to consider minor modifications to existing law, a complex jurisprudence is preferable to an irrational one, and the same concerns that motivate me to change the third-party doctrine are implicated when police on a whim (or minimal threshold) question innocent persons about the most intimate details of life.

I. Factor 9. Changing Social Norms and Technologies

The law should account for changing social norms and technologies, including those that require the provision of additional information to third parties and those that allow third parties (including law enforcement) to acquire information they would not previously have acquired.[217] I have written elsewhere concerning the effects of changing social norms and advancing technology, and it will suffice to direct the reader to those discussions rather than repeat them here.[218] This factor is essentially a reminder that the Fourth Amendment requirement of "reasonableness" should not be diminished by advancing technology, and it is probably adequately incorporated into other factors as I have discussed them above. For example, if information not intended to be disclosed to anyone is obtained by way of new technology, or if the information of interest is now necessarily disclosed by any reasonable participant in society, these are both

214. Timothy P. O'Neill, *Rethinking* Miranda*: Custodial Interrogation as a Fourth Amendment Search and Seizure*, 37 U.C. DAVIS L. REV. 1109 (2004).

215. Moving a suspect to the stationhouse (or almost any other location) for questioning constitutes a seizure for Fourth Amendment purposes and requires probable cause whether or not it is deemed a formal arrest. *See* Florida v. Royer, 460 U.S. 491, 499 (1983).

216. *See* LAFAVE ET AL., *supra* note 211, at § 8.6(a) (discussing the reluctance of courts to unduly hamper grand jury investigations); Slobogin, *supra* note 208, at 837-41 (arguing that restricting subpoenas of personal documents would not unduly hamper effective administration of the laws).

217. *See* State v. McAllister, 875 A.2d 866, 875 (N.J. 2005) ("[T]he advent of modern technology, coupled with the ubiquity of commercial banking, underscores both the ability of prying government eyes to obtain bank records and the need to protect ordinary citizens' financial privacy.").

218. *See* Henderson, *supra* note 85, at 509-11, 521-44; Henderson, *supra* note 7, at 373-93, 412-14.

considerations discussed in my first factor. I risk the redundancy of including it as a separate factor only because I deem it so important. One should not need to become an information curmudgeon in order to enjoy a reasonable degree of privacy from government intrusion. The Fourth Amendment and its state analogs were designed to conform to our world, rather than to require our world to conform to them. Unfortunately, with the exception of its decision in *Kyllo*, I agree with Jeffrey Rosen that "the Supreme Court's response to the growth of new technologies of monitoring and surveillance . . . has proved to be distressingly passive at every turn."[219]

J. Irrelevant Consideration 1. The Form of the Information

The government has no more right to access a record generated by the third party but containing only disclosed information than it has to obtain the disclosed information in its pristine form.[220] What is important is not who owns the information in a property law sense, but rather whether government access would unreasonably invade the disclosing party's privacy.[221] Thus I agree with the Supreme Court of Pennsylvania that the *Miller* Court's contrary view[222] represents a "simplistic proprietary analysis."[223] Manipulation of disclosed information does not diminish an expectation of privacy.

---

219. JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 58 (2001).

220. *See* Slobogin, *supra* note 208, at 831-33.

221. *See* Katz v. United States, 389 U.S. 347, 353 (1967) ("The premise that property interests control the right of the Government to search and seize has been discredited."); State v. Domicz, 873 A.2d 630, 645-46 (N.J. Super. Ct. App. Div. 2005) (noting rejection of this criterion by those courts that have departed from federal doctrine), *rev'd on other grounds*, 907 A.2d 395 (N.J. 2006). Thus in its consent jurisprudence the Supreme Court permitted searches supported by "the consent of one who possesses common authority over premises or effects," United States v. Matlock, 415 U.S. 164, 170 (1974), but took pains to clarify that such "authority" is not governed by property law:

> The authority which justifies the third-party consent does not rest upon the law of property, with its attendant historical and legal refinements, but rests rather on mutual use of the property by persons generally having joint access or control for most purposes, so that it is reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched.

Id. at 171 n.1 (internal citations omitted).

222. *See* United States v. Miller, 425 U.S. 435, 440 (1976) (stating that a bank customer can "assert neither ownership nor possession" of the records); *accord* State v. Klattenhoff, 801 P.2d 548, 552 (Haw. 1990) ("The records are owned by the banks because they are business records, they are not the private papers of the account holder."); Samson v. State, 919 P.2d 171, 174 (Alaska Ct. App. 1996) (holding that a utility customer lacks standing to challenge government acquisition of utility company records because the records belong to the utility and are in its possession).

223. Commonwealth v. DeJohn, 403 A.2d 1283, 1290 (Pa. 1979).

K. Irrelevant Consideration 2. The "Good Citizen" Motivation of a Third Party

A third party's "good citizen" motivation to assist law enforcement is not relevant to the constitutional analysis.[224] Thus, Janet Randolph's desire to assist law enforcement in locating evidence of her husband's drug use was not sufficient to overcome his Fourth Amendment rights.[225] Only when the third party is a victim of the alleged crime, or when the third party is acting upon its own initiative, does the desire of the third party become relevant. In the case of a third-party victim, the victim's independent interest in transferring the relevant information to law enforcement outweighs the disclosing party's privacy interest.[226] Where the third party itself initiates the transfer, the "private search" doctrine is controlling, in that the Fourth Amendment and its state analogs only restrict government conduct.[227] To the extent this allows verbose and careless third parties to create a rather gaping hole in privacy protection, it is simply one that only legislation can stem. As discussed with respect to Factor 6, however, such legislation can influence constitutional rights.

---

224. *See* Burrows v. Superior Court, 529 P.2d 590, 593 (Cal. 1974). The third party's motivation may also be personal or institutional laziness, taking the path of least resistance: "[A]s a practical matter, the bank simply does not have the same incentive to vigorously assert even its limited defenses against [a state] request." State v. McAllister, 875 A.2d 866, 879 (N.J. 2005). Such indifference is of course no more availing than a beneficent desire to assist police.

If the information is a personal recollection there may be an autonomy interest in relating that information. *See* discussion of Factor 8, *supra* Part III.H.

225. *See supra* notes 44-56 and accompanying text (discussing Georgia v. Randolph, 126 S. Ct. 1515 (2006)). Justice Thomas' dissent relies on the contrary principle. *See Randolph*, 126 S. Ct. at 1541-43.

226. *See Burrows*, 529 P.2d at 594 ("However, if the bank is not neutral, as for example where it is itself a victim of the defendant's suspected wrongdoing, the depositor's right of privacy will not prevail."); People v. Lopez, 776 P.2d 390, 391 (Colo. 1989).

227. *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984) ("This Court has . . . consistently construed this protection as proscribing only governmental action; it is wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official.") (internal quotation marks omitted). Other than a short-lived jurisprudence in Montana that excluded evidence obtained via invasive private searches, *see* State v. Hyem, 630 P.2d 202 (Mont. 1981), *overruled by* State v. Long, 700 P.2d 153 (Mont. 1985), the author is not aware of any state that has ever deviated from the Fourth Amendment in this regard. A favorable response to a government request is of course not private action. *See Burrows*, 529 P.2d at 594 (noting that voluntary relinquishment is irrelevant where it is in response to police request).

L. Irrelevant Consideration 3. The Government's Method of Acquisition

Unless it affects one of the nine factors, the government's manner of acquiring information is irrelevant. Thus, acquiring information on electricity consumption via a thermal scan is equivalent to obtaining that information from utility company records,[228] and the acquisition of telephone numbers dialed in real time via a pen register is equivalent to the acquisition of those numbers from a telephone company record.[229] Therefore the constitutional restraint on government access should be identical. Both processes acquire the same information,[230] and it is no more invasive to have information captured in real time. Though presumably humiliating, it is no worse to have the government watch you dance in your underwear as you break a move than for agents to watch it later on tape. Or, to give a third-party example, it is no more intrusive to have the government read your e-mail as it travels to its intended destination than to have it obtained from an Internet service provider an hour later and read then.[231]

To the extent people have a bias toward greater restriction on real-time acquisition, it probably arose because obtaining the content of a telephone

---

228. *See* State v. Domicz, 873 A.2d 630, 649 (N.J. Super. Ct. App. Div. 2005) ("[W]e find no philosophical distinction to be drawn between the purpose behind excluding evidence obtained from a warrantless thermal scan of a residence and excluding evidence derived from a warrantless search of a utility's records as to electrical usage in an accused's home. Both searches seek information as to the amount of electricity used within a home."), *rev'd*, 907 A.2d 395 (N.J. 2006). Although the New Jersey Supreme Court did not ultimately decide whether utility records are constitutionally protected, it did reject this asserted equivalence. *See Domicz*, 907 A.2d at 403. Obviously I find that rejection unpersuasive.

229. The Supreme Court's decision in *Smith v. Maryland*, 442 U.S. 735 (1977) concerned real-time acquisition. *See id.* at 736 n.1. But the Court's logic applies equally to acquisition of historic information. *See* People v. Larkin, 239 Cal. Rptr. 760, 762 (Ct. App. 1987) ("A pen register, providing information about outgoing and incoming calls, involves the same privacy rights as toll information in phone company records."); People v. Blair, 602 P.2d 738, 747 (Cal. 1979); People v. Sporleder, 666 P.2d 135, 142 (Colo. 1983); State v. Hunt, 450 A.2d 952, 954; *cf.* State v. Gunwall, 720 P.2d 808, 813, 816 (Wash. 1986) (requiring significantly more for real-time acquisition).

230. Of course, if different information were obtained because it was easier to accurately sort (without reading) historically, the two acquisitions would not be identical.

231. The current statutory regime does differentiate between real-time and historic surveillance. To acquire e-mail in real time the government must obtain a Title III "super warrant." *See* 18 U.S.C.A. § 2510(12) (West 2004) (defining "electronic communication"); §§ 2511, 2516, 2518 (providing requirements). To obtain e-mail from an Internet service provider, the government must obtain, at most, a search warrant. *See* 18 U.S.C.A. § 2703(a). If the government is willing to wait until that e-mail is no longer in "electronic storage," which the government argues ceases to be the case once it is read by the recipient, a subpoena with delayed notice will suffice. *See* 18 U.S.C.A. § 2703(b). The government's interpretation of "electronic storage," however, has proved controversial. *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1075-77 (9th Cir. 2004) (rejecting government interpretation). There is some risk in waiting and using a subpoena, because the target may choose not to store a copy of the e-mail on the Internet service provider's server. But this concern can be alleviated by requesting that the Internet service provider preserve all such data. *See* 18 U.S.C.A. § 2703(f) (West 2004).

conversation, a very invasive procedure, has historically only been possible in real time.[232] A more modern application demonstrates the absurdity of a contrary rule. When a federal magistrate rejected the government's application requesting real-time location information from a suspect's cell phone company, the government modified its approach.[233] Instead of requesting that the location information travel directly from the suspect's phone, the government requested that it instead first be "stored" by the provider.[234] Constitutional rights should not so easily be evaded, and the magistrate so held.[235]

Similarly, unless it will affect dignitary interests typically not relevant in the third-party context,[236] it is no less invasive of privacy to obtain information by third-party subpoena than by warrant.[237] It is also no more invasive to passively intercept an on-going disclosure (e.g., grab trash awaiting collection or eavesdrop on a bank cable) than to obtain the information from the third party following disclosure (e.g., obtain trash from a garbage collector or records from a bank).[238] Therefore these too should be irrelevant.

---

232. To the extent it remains so as providers migrate to digital technology is merely a matter of expense and inertia. *See* Henderson, *supra* note 85, at 528-29. Obtaining the contents of a telephone conversation in real time requires a Title III "super warrant." *See* 18 U.S.C.A. §§ 2511, 2516, 2518. Ironically, however, it seems that federal statutes currently make it easier to obtain non-content information in real time, *see* 18 U.S.C.A. § 3121(b)(2), than historically. *See* 18 U.S.C.A. § 2703(c)(1).

233. *In re* Application of the United States for Orders Authorizing the Installation and Use of Pen Registers and Caller Identification Devices, 416 F. Supp. 2d 390, 391-92 (D. Md. 2006).

234. *Id.* at 392.

235. *Id.* at 395.

236. Typically, it is less disruptive and humiliating to produce relevant documents than to have the government search for them. But in the third party context, even when agents obtain a warrant, they often allow the third party to proceed as if it were a subpoena. For example, when agents obtain a warrant for a suspect's e-mails, they typically request that the Internet service provider gather the relevant information. *See* United States v. Bach, 310 F.3d 1063, 1065 (8th Cir. 2002) (accepting that procedure). In other contexts dignitary interests can certainly be relevant. For example, it is arguably much more invasive to have a canine sniff one's person than to have either (1) that same dog sniff an inanimate object belonging to that person or (2) have a "mechanical sniffer" conduct the same sniff of one's person. *See* United States v. Garcia-Garcia, 319 F.3d 726, 730-31 (5th Cir. 2003) (assuming canine sniff of a person was a search despite doctrine that sniff of inanimate object is not a search); Commonwealth v. Rogers, 849 A.2d 1185, 1190-91 (Pa. 2004) (requiring probable cause for canine sniff of a person despite requiring only reasonable suspicion for sniff of inanimate objects).

237. *See* Carlson v. Superior Court, 129 Cal. Rptr. 650, 655 (Ct. App. 1976) (permitting subpoena of bank records only if they are returned to court that will determine probable cause before releasing them to prosecution). "Surely an accused's constitutional right to privacy in his papers and records is not diminished because law enforcement officials seek to obtain them by subpoena rather than by warrant." *Id.*

238. *See* State v. Hempele, 576 A.2d 793, 798 (N.J. 1990) ("The facts in *Greenwood* are almost

M. Irrelevant Consideration 4. Expectations Created by Police Conduct

Whereas expectations created by private conduct are relevant, those created by government conduct are not. The Supreme Court has recognized the latter limitation in the context of its "subjective expectation of privacy" criterion:

> Situations can be imagined, of course, in which *Katz'* two-pronged inquiry would provide an inadequate index of Fourth Amendment protection. For example, if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation or privacy regarding their homes, papers, and effects. Similarly, if a refugee from a totalitarian country, unaware of this Nation's traditions, erroneously assumed that police were continuously monitoring his telephone conversations, a subjective expectation of privacy regarding the contents of his calls might be lacking as well . . . . In determining whether a "legitimate expectation of privacy" existed in such cases, a normative inquiry would be proper.[239]

In the more pithy language of the California Supreme Court, "[s]ince respondents' privacy claim is a reasonable one, it cannot be wiped out by the simple and expedient device of its universal violation."[240] The relevant "societal expectation" discussed in Factor 4 cannot be manipulated by the government.

---

identical to those here. The primary difference is that . . . the police themselves removed the garbage from the curb, whereas in *Greenwood* a trash collector gave the garbage to the police. That distinction has no fourth-amendment significance."). Obviously, if the interception were typically to disrupt the intended disclosure this would be more invasive than obtaining the information ex post, but such disruption is irrelevant in the case of garbage intended for a landfill.

239. Smith v. Maryland, 442 U.S. 735, 740 n.5 (1979); *see also id.* at 750 (Marshall, J., dissenting) ("[T]o make risk analysis dispositive in assessing the reasonableness of privacy expectations would allow the government to define the scope of Fourth Amendment protections. For example, law enforcement officials, simply by announcing their intent to monitor the content of random samples of first-class mail or private phone conversations, could put the public on notice of the risks they would thereafter assume in such communications."); State v. Butterworth, 737 P.2d 1297, 1298-99 (Wash. App. 1987) ("The privacy protections of our state constitution encompass more than the defendant's merely subjective expectations, which may depend on such things as advances in surveillance technology, and may, moreover, be subject to manipulation by police and other agents of the state. Instead, the appropriate analysis . . . focuses on those privacy interests which citizens of this state have held, and should be entitled to hold, safe from governmental trespass absent a warrant.") (internal citation and quotation marks omitted).

240. People v. Chapman, 679 P.2d 62, 71 (Cal. 1984) (internal quotation marks omitted).

IV. TWO PROPOSALS

Professors Daniel Solove and Christopher Slobogin have each drafted thoughtful proposals that would better protect privacy than the current federal third-party doctrine.[241] The more straightforward is that of Professor Solove, who would require probable cause before police could obtain any third-party information contained in a "system of records."[242] That Solove would propose a content-neutral solution is not surprising when one considers the excellent work he has done in analyzing and contrasting the many differing conceptions of privacy.[243] But although such a regime would be wonderfully administrable, especially as law enforcement more commonly turns to data brokers from which it seeks an amalgam of information, I agree with Professor Slobogin that Solove's solution is overinclusive.[244] It would require probable cause before the police could obtain everything from basic subscriber information to the most personal of records. Although states like California require probable cause for significant third-party information, even these most restrictive states have never implied they would apply that standard across-the-board. Unless no other alternative is possible to administer, I cannot accept a regime that deems it "reasonable" to acquire name and address information on the same showing that accesses medical records, location information, telephone dialing information, and bookstore receipts.

Professor Slobogin has been arguing for the application of a "proportionality principle" in Fourth Amendment jurisprudence for many years,[245] so it is not surprising that he would distinguish among third-party content. But he limits himself to three distinctions, namely organizational v. personal records, private v. public records, and content v. catalogic

241. SOLOVE, DIGITAL PERSON, *supra* note 9; Slobogin, *supra* note 9. Solove presented an earlier version of his proposal in Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2002).

242. SOLOVE, DIGITAL PERSON, *supra* note 9, at 217, 220-21. Solove takes the term "system of records" from the Privacy Act, which defines the term as "a group of any records . . . from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." *Id.* at 214. To obtain such information Professor Solove would require that law enforcement obtain a statutory "regulated subpoena" that fuses traditional warrants and subpoenas in an attempt to capture the benefits of both. *See id.* at 220.

243. *See generally* Solove, *supra* note 105.

244. *See* Slobogin, *supra* note 9, at 185.

245. See Christopher Slobogin, *Let's Not Bury Terry: A Call For Rejuvination of the Proportionality Principle*, 72 ST. JOHN'S L. REV. 1053, 1081-82 (1998), which builds upon his earlier work, Christopher Slobogin, *The World Without a Fourth Amendment*, 39 UCLA L. REV. 1, 68-75 (1991).

information.[246] These distinctions are insightful, and add a nuance missing from Solove. Unfortunately, I do not find the final category to be administrable.

Slobogin first distinguishes between "organizational" and "personal" records, organizational records being those that "pertain to a collective entity or . . . fit the [Supreme Court's Fifth Amendment] required-records criteria."[247] Because he agrees with the Supreme Court that significantly restricting access to organizational records would unduly hamper legitimate law enforcement, he permits government access to organizational records via a subpoena supported by relevance.[248] Any record that is not "organizational" is "personal," and receives greater Fourth Amendment protection.

By this definition, however, significant "personal" information is publicly available. Thus Slobogin next distinguishes between "publicly-held" personal records and "privately-held" personal records, publicly-held personal records being those held by a public entity that would be subject to release under the federal Freedom of Information Act and similar state statutes.[249] Although such records are available to the public for the asking, because the "government's resources and power are so much more significant, and its hunger for information so much more voracious,"[250] Slobogin would permit government access to publicly-held personal records via court order supported by reasonable suspicion.[251]

If the government wishes to access the content of privately-held personal records, it must obtain a warrant supported by probable cause.[252] But Slobogin proposes that not all privately-held personal records constitute "content," and it is this distinction that I ultimately find unsatisfactory. Slobogin more generally distinguishes between what he terms "content" and "catalogic" data.[253] Content represents a transaction itself, while catalogic data "classifies and describes a transaction."[254]

---

246. Slobogin, *supra* note 9, at 169.

247. *Id.* at 173.

248. *Id.* at 169-70, 173.

249. *Id.* at 175-76.

250. *Id.* at 176.

251. *Id.* at 169, 176.

252. *Id.* at 169.

253. *Id.* at 177-80.

254. *Id.* at 177. According to Slobogin,

> [c]atalogic data includes descriptors of communications and transmissions, such as phone numbers dialed, the addresses that route emails, and the duration of phone calls and Internet session times. This category of transactional information also includes membership lists; plane, train and ship passenger manifests; business records listing who purchased what and when; and other archives that describe the identities of those who have participated in a particular activity or communication.

Id.

In the case of telephone conversations, this distinction has long been both constitutionally and statutorily recognized. There is both Fourth Amendment and significant statutory protection for the content of a telephone conversation,[255] but no Fourth Amendment and very minimal statutory protection for all other information regarding a call, such as the dialing information identifying the communicants.[256] The Supreme Court's justification for this distinction, namely that the non-content dialing information was voluntarily provided to the telephone provider, has never held any weight because the content is likewise voluntarily transferred to that provider.[257] So to the extent there is a distinction, and I think there is, it must be based either on some "content"/"non-content" (i.e. "catalogic") criterion that is universally applicable, or else just on the happenstance that the technology of telephonic communication operates in such a manner wherein both types of information are implicated, and telephonic content is deemed more private by society. Unfortunately for Slobogin's proposal, I think it is the latter.

For example, consider the location of a cell phone customer, information which is "transferred" to a provider any time a customer's phone is "turned on" within the service provider's network.[258] My initial impression is that a customer's location is not the "content of the transaction,"[259] as the content would instead consist of any conversations held via the phone. Hence the customer's location would be "information that classifies and describes [that] transaction,"[260] or "catalogic" data, in this case information describing the location from which calls are sent and received. But what of such data when no call is in progress? Would it then be content information, as there is no underlying transaction to classify or describe? It would be odd if the government restraint vacillated or depended upon a technological fortuity, but if we make distinctions based upon the particular technology of a traditional phone call, it seems we might reach just that result.

---

255. *See* Berger v. New York, 388 U.S. 41, 51 (1967) (recognizing Fourth Amendment protection); 18 U.S.C.A. §§ 2510-2522 (West 2004).

256. *See* Smith v. Maryland, 442 U.S. 735, 745-46 (1979) (holding there is no Fourth Amendment protection); 18 U.S.C. §§ 3121-3127 (2000).

257. *See Smith*, 442 U.S. at 746 (Stewart, J., dissenting) ("The telephone conversation itself must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment.").

258. *See* Henderson, *supra* note 7, at 380.

259. Slobogin, *supra* note 9, at 177.

260. *Id.*

Consider a stand-alone Global Positioning System device (meaning one not connected to a telephone) that relies upon a third party.[261] Now it would seem location information would always be content, because there is no other transmission it could be said to classify or describe. If so, the government might be more restricted in obtaining the same location information from a standalone service than from a cell phone provider. More generally, it does not seem that the distinction between content and catalogic is operating as a suitable substitute for how private society deems location information.

Similar difficulties arise in categorizing other types of information. Are utility records content, because there is no underlying data they describe? Or do such records merely catalogue a transaction, namely that a given customer purchased 'x' kilowatts of power today? Slobogin typically considers commercial transaction records to be catalogic.[262] But he also makes an exception for one type of transaction record, uniform resource locators ("URLs") used to navigate the World Wide Web (e.g., http://www.law.ufl.edu/faculty/slobogin).[263] His justification is that knowledge of a URL allows the recipient to view the very website, but of course so does a "business record[] listing who purchased what and when."[264] Indeed, it is more likely the content of a website will have since changed than that police will be unable to inspect an identical product for themselves. I am sympathetic to protecting freedom of thought and expression by restricting access to URLs, but it seems another content distinction has wormed its way into his system.[265]

What about the information that started it all in *Burrows*, bank records? At first blush they seem to be content, because they represent the entirety of my transaction with the bank,[266] and I believe this is how Slobogin would characterize them. But just like catalogic telephone dialing records, which record who I call, who calls me, and when, my bank merely records to whom I pay money, from whom I receive money, and when. Would it only be the *amount* of one's transactions that would be deemed content? Presumably not to Slobogin, because the same distinction could be made for all merchant transactions. That I shopped at a certain Victoria's Secret location on a certain day and time would be catalogic. But if the amount of

261. Although in its current manifestation it is possible to take advantage of the Global Positioning System satellites without a third party, this would not have to be the case. Moreover, there are third-party providers that offer more accurate location information. *See, e.g.*, OmniSTAR, http://www.omnistar.com.

262. Slobogin, *supra* note 9, at 177.

263. *Id.*

264. *Id.* (defining catalogic data).

265. Professor Slobogin later explicitly recognizes a separate category of "catalogic data that implicates First Amendment interests." *Id.* at 182.

266. To the extent it is confusing to conceptualize "bank records" because banks handle many different types of transactions, consider a credit card company instead.

my bank transaction was content, so too would be the fact that I purchased a red thong at Victoria's Secret. By defining catalogic information to include "who purchased what and when," Slobogin renders that interpretation impossible.[267]

In many circumstances the distinction would have no practical effect, because Slobogin would require a warrant supported by probable cause both for acquisition of the content of privately-held personal records and for what he terms "target-based" catalogic surveillance.[268] "Target-based" surveillance is the gathering of information about a specific person, as opposed to a specific event.[269] An example of "event-based" surveillance would be the acquisition of the name of every person who purchased a shoe that left a print at a murder scene.[270] When the acquisition of catalogic data is "event-based" Slobogin permits a low threshold, judicial determination of relevance.[271]

I understand his desire to grant significant protection to target-based catalogic surveillance. Given the vast amount of "transactional" information available today, the government can quickly amass a "virtual complete biography" or "virtual mosaic of a person's life." Thus Slobogin justifies this restriction by citing to the databases that today aggregate catalogic data.[272] But what if the government genuinely only wants access to the telephone numbers a suspect has dialed (as might be the case, for example, in the investigation of telephone harassment)? If that information is not otherwise worthy of the protection, it seems no justification for requiring probable cause to say that "we know you *could* acquire so much third-party information from existing records that we are going to require a warrant even for this minimal request."

I am also concerned by the low threshold for event-based catalogic surveillance given the extensive information this can parse. As discussed with respect to my Factor 3 (the amount of information), it should not only be relevant what information police ultimately desire, but also what they are seeking to search through to obtain it. Unless restrained by law, police are less and less likely to head to Frank's Yarns to inquire about who purchased 'x' in the last month, and are instead more likely to pay a private company to run an inquiry on billions of records that contain a "complete mosaic" of the

267. *Id.* at 177.
268. *Id.* at 169.
269. *Id.* at 142-43.
270. *Id.* at 147-48.
271. *Id.* at 169, 179-80.
272. *Id.* at 178.

very characteristics that Slobogin agrees we need to protect. In fact, they are likely not to run a profile of merely that one clue, but will instead include everything they know about the crime and its perpetrator. I cannot see why the government should be able to search *through* all of this information upon mere relevance when they would have to demonstrate probable cause to obtain that information. If a sophisticated data mining operation resulted in a few names, presumably that itself would give the probable cause Slobogin deems necessary to directly access (rather than merely search through) the information on those persons.[273] This would be a circular manner of acquisition.

Slobogin might reach the same result because he questions whether current data mining algorithms can even satisfy a relevance standard.[274] I suspect, however, that given typical increases in computing power and storage and ever-expanding databanks, the technology will develop to where it might. To the extent Slobogin is otherwise willing to restrict event-based transaction surveillance based on the type or quantity of information it searches through,[275] his proposal once again seems to depend upon additional implicit criteria.

Ultimately, despite Slobogin's characteristically impressive article, I am left both with the concern that I cannot adequately distinguish between content and catalogic information, and that even if I could, the distinction would not always reflect societal expectations of privacy.

V. CONCLUSION

While it has been instructive to analyze and categorize the doctrines of those courts that have rejected the federal third-party doctrine, I have to admit I am disappointed that they do not offer more. When I began working on the third-party doctrine a few years back, I was convinced the Supreme Court's jurisprudence was wrongheaded and that I could offer a far better solution. After critiquing that doctrine in light of modern technology and social norms, looking to the states to see which had diverged and with respect to what information, and now looking more closely at the rationales for those departures, I remain convinced that the Supreme Court is wrong. I believe I have a better solution, but it too seems less than ideal.

---

273. If the solution were to forbid searches of aggregate databases upon mere relevance, we would have to determine when a given source acquires "too much" information such that it shifts to the "target-based" protections even for event-based surveillance.

274. *See id.* at 181.

275. *See id.* Slobogin asserts that "[i]f one accepts the concern about creation of 'personality mosaics' . . . data mining would need a high hit rate to the extent it accumulates a significant amount of identifiable data about individuals, even if . . . all of the information is catalogic in nature." *Id.* I share this concern, but with respect to event-based surveillance this seems to be a distinction that is not articulated in his table of restrictions. *See id.* at 169.

Professor Solove is right in saying that it would be best if we did not have to distinguish among different types of information, and Professor Slobogin is right in saying it would be better if we could only make a few distinctions. But I cannot find such a solution that adequately accommodates the diversity of third-party situations, and therefore I see no alternative to requiring courts to distinguish among types of information and a number of other factors.

But then perhaps such a case-by-case, item-by-item jurisprudence should not be so depressing. Many jurisdictions have operated under it for a number of years. Although the questions they will (or at least should) soon face are perhaps more difficult—as more and more information is created, shared, aggregated, and deemed critical to law enforcement—they seem to operate at least as well as the federal system. And if they adopt principled factors, their jurisprudence need not resemble "one immense Rorschach blot."[276]

If nothing else, it is critical that courts and commentators understand where we have been as we seek to move forward. Merely because a readily administrable doctrine has persisted does not render it acceptable, and things are already on the move. In my last paper I listed ten states that I believe might reject the federal doctrine.[277] I would add one more to that list.

On June 9, 2006, a New Mexico appellate court held that the state constitution requires a warrant supported by probable cause to search garbage left for collection.[278] Although New Mexico had previously diverged from the Fourth Amendment on a number of issues, it had not given reason to believe it would depart from the federal third-party doctrine.[279] While this appellate holding is only a limited divergence,[280] the court's strong language gives reason to believe that New Mexico may join the rank of states rejecting the doctrines of *Smith* and *Miller*.

This is an active and important area of law, and for now I reaffirm my commitment to a flexible reasonableness criterion that considers the totality of the circumstances. In the words of the New Mexico court: "In all cases that invoke [our Fourth Amendment analog], the ultimate question is

276. *See* Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 393 (1974) (warning that a graduated Fourth Amendment would become "one immense Rorschach blot").

277. Henderson, *supra* note 7, at 395 tbl.1.

278. State v. Granville, 142 P.3d 933, 943-44 (N.M. Ct. App. 2006), *cert. granted*, 2006 N.M. Lexis 379 (Aug. 22, 2006) (No. 29,890).

279. Henderson, *supra* note 9, at 407 n.145.

280. Garbage would receive protection under a "limited third-party doctrine" which ignores disclosures to mere conduits. *See* Factor 1, *supra* Part III.A.

reasonableness. We avoid bright-line, per se rules in determining reasonableness; instead, we consider the facts of each case."[281]

281. *Granville*, 142 P.3d at 939 (internal citations omitted).