IS DATA MINING EVER A SEARCH UNDER JUSTICE STEVENS'S FOURTH AMENDMENT?

*Joseph T. Thai**

INTRODUCTION

On a daily basis, we convey to third parties detailed information about the most mundane to the most intimate aspects of our lives. When we place a call, we transmit the number we dialed and the time and length of our call to the phone company.[1] When we carry around a mobile phone, we also broadcast our physical location to the wireless provider.[2] When we get online, we transmit to our Internet service provider ("ISP") the websites we visit, the time and length of our visits, the email addresses we correspond with, and the bandwidth we consume.[3] When we visit a website, we

* Associate Professor of Law, University of Oklahoma. A.B., 1995, Harvard College; J.D., 1998, Harvard Law School. I would like to thank David Berol, Randy Coyne, Stephen Henderson, Huyen Pham, Christopher Slobogin, Paul Thompson, and the participants of the faculty colloquium at the University of Oklahoma College of Law for their helpful comments on this Article, and to Travis Chapman for his able research assistance. I also would like to thank my family for their essential support whenever I set aside time to write. Last but not least, I would like to express my deep gratitude to Justice Stevens for the life-altering privilege and pleasure of serving as his law clerk from 2000-2001, and for his enduring friendship. By his unconscious example of excellence, humility, humor, kindness, courage, and wisdom, he has set high standards for me in law as well as life, and however much I fall short of them, it is not for want of appreciating their worth. A version of this paper was presented on September 30, 2005, at the Conference on the Jurisprudence of Justice Stevens at Fordham Law School, on the occasion of his thirtieth year on the U.S. Supreme Court.

1. *See, e.g.*, Verizon, About Verizon—Privacy and Customer Service Policies—Telephone Company Customer Policy, http://www22.verizon.com/about/privacy/customer/ (last visited Jan. 22, 2006) (stating that "we generally keep our records of the services you buy and the calls you make private").

2. *See, e.g.*, Sprint, Sprint Privacy Policy, http://www.sprint.com/legal/sprint_privacy.html (last visited Jan. 22, 2006) (stating that "[t]o make wireless communications possible, our network knows the general location of your phone or wireless device whenever it is turned on. Your wireless device sends out a periodic signal to the nearest radio tower/cell site so that our network will know where to route an incoming communication and how to properly bill for the service").

3. *See, e.g.*, Cox Communications, About Cox—Policies and Agreements, http://www.cox.com/policy/04privacyrights.asp (last visited Jan. 22, 2006) (stating that "[i]n providing Internet services, we automatically collect personal and usage information, such as the Internet Protocol (IP) addresses assigned (numbers assigned to your computer while online), bandwidth used, system and connection performance, browsers used, dates and times of access, and Internet resource requests, including requests to access web pages"); *see also* Marshall Brain, How E-mail Works, http://computer.howstuffworks.com/email.htm/printable (last visited Jan. 22, 2006).

disclose identifying computer information, browsing history, and other data to the site host.[4] When we use a credit card, we convey to the issuer the price, time, and source of our purchase.[5] When we use a bank, we turn over details about our finances to the institution.[6] When we visit a doctor, we often disclose very personal medical history to the physician and staff. The list goes on and on.[7]

These third parties commonly record the information they receive from us.[8] Furthermore, they may convey this information to others, such as affiliates, partners, advertisers, credit bureaus, insurers, and government entities of various stripes, including law enforcement.[9] In the event these third parties agree to turn over our information to the authorities, the Constitution poses no impediment whatsoever, at least under current

4. *See, e.g.*, Amazon.com, Help: Privacy Notice, http://www.amazon.com/exec/obidos/tg/browse/-/468496/104-8932490-4566300 (last visited Jan. 22, 2006) (stating that "[e]xamples of the information we collect and analyze include the Internet protocol (IP) address used to connect your computer to the Internet; login; e-mail address; password; computer and connection information such as browser type and version, operating system, and platform; purchase history, which we sometimes aggregate with similar information from other customers to create features such as Purchase Circles and Top Sellers; the full Uniform Resource Locator (URL) clickstream to, through, and from our Web site, including date and time; cookie number; products you viewed or searched for; zShops you visited; your Auction history; and the phone number you used to call our 800 number. During some visits we may use software tools such as JavaScript to measure and collect session information, including page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), and methods used to browse away from the page."); The New York Times, Customer Service: Privacy Policy, http://www.nytimes.com/ref/membercenter/help/privacy.html (last visited Jan. 22, 2006) (stating that "[t]he New York Times on the Web employs cookies to . . . track site usage").

5. *See, e.g.*, Citibank, Privacy, http://www.citibank.com/privacy (last visited Jan. 22, 2006) (stating that the information Citigroup collects about its credit card holders includes "[i]nformation about your transactions with us, our affiliates, or non-affiliated third parties, such as your account balances, payment history, and account activity").

6. *See, e.g.*, Bank of America, Bank of America Privacy Policy for Consumers 2005, http://www.bankofamerica.com/privacy/ (follow "Privacy Policy for Consumers" hyperlink) (last visited Jan. 22, 2006) (stating that Bank of America collects and uses "information about your transactions and account experience, as well as information about our communications with you," including "your account balances, payment history, credit card usage, and your inquiries and our responses").

7. For more examples, see Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. Cal. L. Rev. 1083, 1089-95 (2002).

8. *See, e.g.*, Amazon.com, *supra* note 4; Bank of America, *supra* note 6; Citibank, *supra* note 5; Cox Communications, *supra* note 3; The New York Times, *supra* note 4; Sprint, *supra* note 2; Verizon, *supra* note 1; *see also* Dr. D. Johnson, Crystal Park Privacy Rights, http://www.drdonnajohnson.yourmd.com/ (follow "Privacy Rights" hyperlink) (last visited Jan. 22, 2006).

9. *See, e.g.*, Amazon.com, *supra* note 4; Bank of America, *supra* note 6; Citibank, *supra* note 5; Cox Communications, *supra* note 3; Johnson, *supra* note 8; Sprint, *supra* note 2; The New York Times, *supra* note 4; Verizon, *supra* note 1; *see also* Matt Richtel, *Enlisting Cellphone Signals to Fight Road Gridlock*, N.Y. Times, Nov. 11, 2005, at C1 (reporting on states testing traffic monitoring systems based on mobile phone location data provided in real time by cellular carriers).

understanding of U.S. Supreme Court precedent. Specifically, applying the principle from *Katz v. United States* that a "search" regulated by the Fourth Amendment occurs only when the government intrudes into a reasonable expectation of privacy,[10] the Court held decades ago that when we convey information to a third party, we give up all constitutionally protected privacy in that information, for we assume the risk that the third party might relay it to others.[11]

10. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). The Fourth Amendment provides that

> [t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, 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.

11. *See infra* Part I. There is a patchwork of statutory and regulatory protections against government-compelled disclosure of information from third parties, but most do not come close to requiring the government to establish anything as demanding as probable cause or even reasonable suspicion under the Fourth Amendment. *See* U.S. Const. amend. IV; Terry v. Ohio, 392 U.S. 1 (1968). For example, the government generally needs to show only relevance to a legitimate law enforcement inquiry to obtain a subpoena for financial records from a bank under the Right to Financial Privacy Act, 12 U.S.C. § 3405 (2000), or to obtain a subpoena for medical records from a healthcare provider under regulations pursuant to the Health Insurance Portability and Accountability Act, 45 C.F.R. § 164.512(f)(1)(ii)(B) (2004). Furthermore, under the Electronic Communications Privacy Act, the government may obtain a court order for customer and usage information from telephone and Internet service providers ("ISPs") upon a heightened showing of relevance to an ongoing criminal investigation. *See* 18 U.S.C. § 2703(c)-(d) (Supp. II 2002); *see also* Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 Iowa L. Rev. 553, 604-13 (1995) (surveying state data-protection laws); Christopher Slobogin, *Transaction Surveillance by the Government*, 74 Miss. L.J. (forthcoming 2006) (manuscript at 12-30), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=670927 (surveying federal regulations governing surveillance of records held by third parties). However, with respect to the content of electronic communications that may not be third-party data, *see infra* note 18, the Stored Communications Act ordinarily requires a warrant supported by probable cause. *See* 18 U.S.C. § 2703 (2000) (imposing a warrant requirement on compelled disclosure of the content of electronic communications stored by ISPs for less than 180 days). In any event, statutory safeguards may come and go. *See, e.g.*, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272 (2001) (to be codified in scattered sections of 5, 8, 10, 12, 15, 16, 18, 21, 22, 28, 31, 42, 47, 49, and 50 U.S.C.); Electronic Frontier Foundation, EFF Analysis of the Provisions of the USA PATRIOT Act that Relate to Online Activities, http://www.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.php (last visited Jan. 22, 2006) (describing USA PATRIOT Act's expansions of statutory authority for government surveillance in the wake of September 11, 2001). *But see* Orin S. Kerr, *Internet Surveillance after the USA PATRIOT Act: The Big Brother that Isn't*, 97 Nw. U. L. Rev. 607, 608 (2003) (arguing that "[t]he Patriot Act did not expand law enforcement powers dramatically, as its critics have alleged"). By contrast, constitutional guarantees, in theory at least, provide more enduring protections, and therefore make the question of the Fourth Amendment's applicability particularly important. *But see* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801, 802, 806 (2004) (criticizing "the prevailing *zeitgeist* about law,

While the key third-party cases involved less modern forms of data, such as bank records,[12] dialing information,[13] oral conversations,[14] and trash,[15] lower courts and commentators have not hesitated to conclude that the risk-assumption rationale applies to newer kinds of data, such as those conveyed to mobile phone companies and ISPs.[16] Likewise, commentators have concluded that the third-party doctrine applies with equal force to the government's use of powerful search technologies to "data mine" supermassive databases, which aggregate records about us from numerous third-party sources.[17] Even though data mining may compile a matrix of information about us more comprehensive and intimate than any intrusion into our homes, the fact that we have previously conveyed the information to third parties apparently means that we have relinquished Fourth Amendment protections against such government snooping.[18]

technology, and privacy," that "[w]hen technology threatens privacy, the thinking goes, the courts and the Constitution should offer the primary response," and arguing for the primacy of statutory regulation given "[t]he institutional advantages of legislative rule making . . . in areas of technological flux").

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

13. Smith v. Maryland, 442 U.S. 735 (1979).

14. United States v. White, 401 U.S. 745 (1971).

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

16. *See, e.g.*, United States v. Forest, 355 F.3d 942, 950-52 (6th Cir. 2004) (finding no reasonable expectation in location data from a mobile phone used to track movements on public highways), *vacated on other grounds sub nom.*, Garner v. United States, 125 S. Ct. 1050 (2005); Stephen E. Henderson, *Learning from Hoosiers and Razorbacks—How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 Cath. U. L. Rev. (forthcoming 2006) (manuscript at 15-16, on file with author) (same); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) (finding no reasonable expectation of privacy in data conveyed to an ISP); Slobogin, *supra* note 11, at 16 (same).

17. For definitions of "data mining," see *infra* notes 47-49 and accompanying text. For commentary applying the third-party doctrine to data mining, see *infra* note 90 and accompanying text. The author is not aware of any cases having decided specifically whether the use of modern data-mining technologies may be a search within the meaning of the Fourth Amendment. However, under the third-party doctrine, the answer seems clear. *See infra* Part III.

18. However, not all transmissions of data *through* third parties may count as conveyances *to* them for purposes of the third-party doctrine. Most significantly, the Court likely would not regard the content of calls and emails—as opposed to metadata such as time, date, and routing information—as third-party data when obtained from telephone companies and ISPs rather than from their intended recipients. The reason is that the Court has not presumed that we voluntarily convey the content of communications to third parties who act as couriers rather than consumers of those communications. *Compare* Katz v. United States, 389 U.S. 347, 352 (1967) (recognizing a reasonable expectation of privacy in "the words [one] utters into the mouthpiece" of a telephone in an enclosed booth), *and Ex parte* Jackson, 96 U.S. 727, 733 (1877) (declaring that "[l]etters and sealed packages . . . in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles"), *with Smith*, 442 U.S. at 741-46 (deeming unreasonable any expectation of privacy in numbers dialed and conveyed to telephone companies, in contrast to "the *contents* of communications" protected by *Katz*), *and* United States v. White, 401 U.S. 745, 749 (1971) (deeming unreasonable any expectation of privacy that the intended recipient of a

Justice John Paul Stevens has supported this restrictive view of the Fourth Amendment. In every third-party case decided by the Court, he has voted with the majority to deny Fourth Amendment protection. Thus, to the extent that the Court has handed the government a blank check to conduct mass surveillance through data mining third-party records for suspicious persons and activities, the signature line bears Justice Stevens's name alongside those of like-minded colleagues. However, if we look beyond the third-party cases to Justice Stevens's opinions in related Fourth Amendment areas, we may discern critical principles for limiting the reach of the third-party doctrine and its application to data mining.

Accordingly, in answering the question whether data mining is ever a search under Justice Stevens's Fourth Amendment, this article seeks to demonstrate not only the magnitude of the threat that data mining poses to privacy, but moreover the importance of Justice Stevens's contributions to preserving vital Fourth Amendment protections that would dissipate under current doctrine. To those ends, Part I of this Article provides background on the nature of several supermassive databases and their capabilities for data mining. Part II reviews the Court's leading cases on the third-party doctrine and its risk-assumption rationale. Part III then considers the constitutionality of data mining under the third-party doctrine. Finally, Part IV scrutinizes Justice Stevens's Fourth Amendment jurisprudence for principles that impact the third-party doctrine and the constitutionality of data mining.

In particular, Part IV focuses on Justice Stevens's opinions in three cases. First, it considers his majority opinion in *Ferguson v. City of Charleston*,[19] which suggested that a reflexive application of the risk-assumption rationale cannot substitute for a normative assessment of whether a privacy expectation in information conveyed to others deserves protection. Second, it discusses his dissent in *Kyllo v. United States*,[20] which underscored the fundamental role that the Fourth Amendment plays in protecting our private activities from the prying eyes of the government, even when technology renders us helpless to exclude the prying eyes of others. Third, it examines his majority opinion in *Illinois v. Caballes*,[21] which implied a new Fourth

communication will not reveal its content to authorities). Consequently, government data mining of the content of private calls and emails routed through communications couriers typically must comply with the Fourth Amendment, for the third-party doctrine does not preclude the protection of privacy expectations in that context. *Cf.* Josh Meyer & Joseph Menn, *U.S. Spying is Much Wider, Some Suspect*, L.A. Times, Dec. 25, 2005, at A1, *available at* http://www.latimes.com/news/printedition/la-na-spy25dec25,1,4503763.story (reporting that current and former intelligence officials suspect that the National Security Agency has been data mining the content of "large volumes" of calls and emails in the United States without warrants, pursuant to presidential orders). Accordingly, when this Article refers to data mining of third-party information, the reference does not include this class of data.

19. 532 U.S. 67 (2001).

20. 533 U.S. 27, 41 (2001) (Stevens, J., dissenting).

21. 125 S. Ct. 834 (2005).

Amendment paradigm that protects against technology-enabled inferences about lawful activities that may occur in private, even if the technology does not expose actual activities. As will be argued, these opinions suggest principles that resist the third-party doctrine's *Lochnerian* assumption that we consciously and freely cede our privacy in personal data conveyed to others in the necessary course of life in our information society.[22] For related reasons, these opinions of Justice Stevens also suggest important Fourth Amendment restraints on the government's ability to conduct surveillance on its citizens through data mining.[23]

I. SUPERMASSIVE DATABASES AND DATA MINING

As the Introduction indicates, most of us turn over a trove of information about ourselves to third parties on a daily basis, revealing our movements, our purchases, our finances, our health, and our activities in the virtual and physical worlds. Unless we choose to live as a hermit like Ted Kaczynski,[24] or unless we fall within the shrinking minority of Americans who lack such modern necessities as credit cards, mobile phones, and Internet access,[25] we practically "blog"[26] every minute of our lives to various third parties. Additionally, we routinely turn over to government institutions at all levels personal, professional, medical, legal, financial, and biometric information as required by law or as needed to obtain services, benefits, licenses, and the like.[27] Many of these third parties maintain our

22. *See* Solove, *supra* note 7, at 1089 (declaring that "[w]e live in the early stages of the Information Age"). For more on the comparison with *Lochner v. New York*, 198 U.S. 45 (1905), see *infra* note 84 and accompanying text.

23. Needless to say, while Justice Stevens authored some of the opinions discussed in this Article during the year that I clerked for him, the Article's interpretations (or misinterpretations) of them are my own.

24. Ted Kaczynski wrote a manifesto against technological progress entitled *Industrial Society and Its Future*, and lived in a remote cabin in Montana before his capture and conviction as the Unabomber. *See* Wikipedia, Theodore Kaczynski, http://en.wikipedia.org/wiki/Theodore_Kaczynski (last visited Jan. 22, 2006).

25. More than 50% of Americans have mobile phones, *see* CTIA, http://www.ctia.org (last visited Jan. 5, 2006) (stating that there are an estimated 201,415,602 U.S. subscribers), about 80% of American households have at least one credit card, *see* Key Findings Newsletter (July/Aug. 2004), http://www.keyfindings.com/healthcare/julyaug2004.htm, and nearly 75% of American households have Internet access, *see* Netratings, Inc., *Three out of Four Americans Have Access to the Internet, According to Nielsen/Netratings* (Mar. 18, 2004), http://www.netratings.com/pr/pr_040318.pdf.

26. A "blog" is a personal web log, and to "blog" is to write one. *See* Dictionary.com, Blog, http://dictionary.reference.com/search?q=blog (last visited Jan. 22, 2006) (defining "blog" in verb form as "author[ing] an online diary or chronology of thoughts").

27. *See* Daniel J. Solove, The Digital Person 13-16 (2004) (discussing the history and content of public-sector databases); *see also infra* notes 30-40 and accompanying text (containing lists and websites with the kinds of information turned over to the government and available to the public). While the third-party cases have yet to draw a distinction between information provided to a private third party and information provided to the government, by its very terms the third-party doctrine would not appear to apply to material that is not "voluntarily conveyed" to the government, such as tax returns. Smith v. Maryland,

information in databases for internal use or share them with business affiliates and partners,[28] while others, including government institutions, may make our personal data accessible to the public online or offline.[29]

Searching through the information available in the database of any third party may reveal telling details about us. But what emerges from any one database may not paint a complete picture of who we are or what we do. Rather, it may show only a slice of our life from our interactions with that particular party who maintains the database. With a good deal of time, money, and connections, one conceivably could comb through the numerous private and public databases of parties to whom we have conveyed information, and thereby compile a fairly comprehensive personal profile. However, few have the resources to do so. Moreover, if the goal is not to gather information about a particular person, but to find a class of persons fitting a certain profile—say, for marketing or law enforcement reasons—then the detective work would prove even more daunting.

Enter, then, supermassive databases that aggregate scores of individual databases into a searchable whole. Two of the largest private-sector offerings are from data brokers ChoicePoint and LexisNexis.[30] According

442 U.S. 735, 743-44 (1979); *see also* Henderson, *supra* note 16, at 10 n.41 ("Although the Supreme Court has held that one retains no reasonable expectation of privacy in information *retained* by a third party . . . the result should be different if the government is solely responsible for *obtaining* that information.").

28. *See supra* notes 8-9 and accompanying text.

29. *See, e.g.*, ABC Adoptions.com, Adoption Records by State, http://www.abcadoptions.com/adoptionrecords.htm (last visited Jan. 22, 2006); Fairfax County, Virginia, Real Estate Division, http://www.co.fairfax.va.us/dta/re_home.htm (last visited Jan. 22, 2006) (stating that "[o]ur website provides assessed values and physical characteristics extracted from the official assessment records for all property in Fairfax County"); Federal Election Commission, FEC Disclosure Reports, http://www.fec.gov/finance/images.htm (last visited Jan. 22, 2006) (making available federal campaign contributions); New York State Department of Health, Birth, Death, Marriage & Divorce Records, http://www.health.state.ny.us/vital_records/ (last visited Jan. 22, 2006); Texas Department of Public Safety, Crime Records Service, https://records.txdps.state.tx.us/ (last visited Jan. 22, 2006); Yahoo!, People Search, http://people.yahoo.com/ (last visited Jan. 22, 2006) (providing phone, address, and email information).

30. Another massive database is maintained by ACXIOM. *See* ACXIOM, InfoBase, http://www.acxiom.com/default.aspx?ID=1756&DisplayID=18 (last visited Jan. 22, 2006); ACXIOM, InfoBase Enhancement, http://www.acxiom.com/default.aspx?ID=1757&DisplayID=18 (last visited Jan. 22, 2006) (marketing a database that purportedly contains the "most accurate and comprehensive, multi-sourced data coverage available in today's marketplace," from "thousands of public and private sources"); *see also* MyPublicInfo, Public Information Profile, http://www.mypublicinfo.com/products.aspx (last visited Jan. 22, 2006) (offering consumers "[a] Public Information Profile (PIP)," which "is a detailed summary of the vast quantity of information available to others about *you*" from "more than 10 billion records"); SearchSystems.net, Largest Free Public Records Directory, http://www.searchsystems.net/ (last visited Jan. 22, 2006) (boasting the ability to search more than 35,000 state, federal, and foreign databases of public records). For more on these and other supermassive databases and data-mining services, see Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. Int'l L. & Com. Reg. 595, 600-07 (2004); Andrew J. McClurg, *A*

to ChoicePoint's website, its online database allows private and public clients access to "more than 17 billion current and historical records on individuals and businesses."[31] Searching those records apparently can return "[c]omprehensive" and "[e]asy-to-read" reports about us, from more cut-and-dry data such as addresses, assets, licenses, and employers, to potentially more revealing data such as credit headers, criminal records, relatives, and a category that ChoicePoint suggestively refers to as "derogatory information."[32] Similarly, through a service called Accurint, LexisNexis makes available a searchable database of "tens of billions of data records on individuals and businesses"[33] from "public records" as well as "non-public information" from companies to whom we have conveyed information.[34] Touting its breadth and ease of use, LexisNexis markets Accurint to law enforcement as a way to "shorten investigation time, free up valuable staff, minimize costs associated with lengthy investigations, and even in some cases save lives," all at "the click of a button."[35]

Not surprisingly, the investigative value of searchable supermassive databases has not escaped the notice of Uncle Sam or the states. On the federal level, the Pentagon worked to develop an ambitious program called

Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling, 98 Nw. U. L. Rev. 63, 75-87 (2003).

31. ChoicePoint, AutoTrackXP and ChoicePoint Online, http://www.choicepoint.com/industry/government/public_le_1.html (last visited Jan. 22, 2006).

32. *Id*. (claiming the ability to "[c]ompile[] a comprehensive report on an individual including current and previous addresses, relatives, assets, corporate involvement and derogatory information"); *see also* ChoicePoint, SQL Direct, http://www.choicepoint.com/industry/government/public_le_5.html (last visited Jan. 22, 2006) (listing available databases on credit headers, real property, corporations, limited partnerships, Uniform Commercial Code filings, bankruptcies, liens and judgments, telephone and business listings, Securities and Exchange Commission significant shareholders, Federal Aviation Administration aircraft and pilots, U.S. Coast Guard watercraft registrations, physician reports, address inspector, Federal Employer Identification Number ("FEIN") listings, Occupational Safety and Health Act filings, professional licenses, and fictitious business name registrations).

33. Accurint, Accurint Overview, http://www.accurint.com/aboutus.html (last visited Jan. 22, 2006).

34. Accurint, Manage Risk with More Intelligence, http://www.accurint.com/index.html (last visited Jan. 22, 2006). Although Accurint's website does not further identify the kinds or sources of its data, a presentation by former owner Seisint on a related program it operated, the Multistate Anti-TeRrorism Information eXchange program ("MATRIX"), reveals information likely contained in its Accurint incarnation. *See infra* note 42 and accompanying text; *see also* Tom Zeller, Jr., *How Billions of Pieces of Information Are Bought and Sold*, N.Y. Times, Mar. 17, 2005, at C8 (noting that data brokers amass public records that "run[] the gamut from birth certificates and voter registrations to bankruptcy filings and tax lien records" from government agencies, and purchase "a wealth of private consumer information—including magazine subscriptions, recent purchases, travel records and the four crucial ingredients for identity theft: name, address, date of birth and Social Security number—from credit reporting agencies, publishers, retailers and other companies").

35. Accurint, Accurint for Law Enforcement, http://accurint.com/lawenforcement.html (last visited Jan. 22, 2006).

Total Information Awareness ("TIA") in the aftermath of the September 11, 2001, terrorist attacks.[36] The program sought to amass "[a] wide range of intelligence data, both classified and open source," about as many individuals as possible, and to develop search tools "to find relevant information for understanding the terrorist intent."[37] Congress shut down TIA after it provoked a firestorm of criticism from privacy advocates, both inside and outside the Beltway, for its potential surveillance of, among other things, "every banking transaction, every credit card use, every visit to a doctor and prescription, and every phone call made by American citizens."[38] However, the development of the project continues with respect to foreign surveillance,[39] and the federal government actively pursues other data surveillance projects, such as the Transportation Security Administration's Computer Assisted Passenger Prescreening System ("CAPPS II").[40]

36. *See* Dep't of Def., Report to Congress Regarding the Terrorist Information Awareness Program 1 (2003), *available at* http://www.eff.org/Privacy/TIA/TIA-report.pdf. For marketing reasons, the program was renamed "Terrorist Information Awareness." *Id*. at 1 & n.1.

37. *Id.* at 3.

38. Letter from Sen. Tom Harkin to Sen. Daniel K. Inouye, Chairman, Subcomm. on Def., U.S. Sen. Comm. on Appropriations (Jan. 13, 2003), *available at* http://www.eff.org/Privacy/TIA/harkin-letter.php; *see also* Letter from ACLU, Am. Conservative Union, Am. for Tax Reform, Ctr. for Democracy and Tech., Ctr. for Nat'l Sec. Studies, Eagle Forum, Elec. Frontier Found., Elec. Privacy Info. Ctr., & Free Cong. Found. to Rep. Duncan Hunter, Chairman, U.S. House of Representatives Comm. on Armed Services & Rep. Ike Skelton (Jan. 14, 2003), *available at* http://www.eff.org/Privacy/TIA/duncan-hunter-letter.php (arguing that "Congress should not allow the Defense Department to develop unilaterally a surveillance tool that would invade the privacy of innocent people inside the United States").

39. *See* H.R. Rep. No. 108-283, at 327 (2003) (Conf. Rep.), Department of Defense Appropriations Act, 2004, 149 Cong. Rec. H8771 (Sept. 24, 2003), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getpage.cgi?position=all&page=H8771&dbname=2003_record. Furthermore, according to recent reports, the National Security Agency may have pursued and operated a domestic surveillance program similar to TIA over the past several years, pursuant to presidential orders. *See* Charles Babington & Dafna Linzer, *Senator Sounded Alarm in '03*, Wash. Post, Dec. 20, 2005, at A10; James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times, Dec. 16, 2005, at A1; *see also supra* note 18.

40. *See* Press Release, Dep't of Homeland Sec., Fact Sheet: CAPPS II at a Glance (Feb. 12, 2004), *available at* http://www.dhs.gov/dhspublic/display?content=3162 (stating that with passenger information from airlines such as name, date of birth, home address, and home telephone number, "the system will quickly verify the identity of the passenger and conduct a risk assessment utilizing commercially available data and current intelligence information"); Letter from ACLU, Am. Conservative Union, Am. Def. Council, Am. for Tax Reform, Ctr. for Democracy and Tech., Christian Coal., Eagle Forum, Elec. Frontier Found., Elec. Privacy Info. Ctr, Free Cong. Found. & People for the Am. Way to Rep. Christopher Cox, Chairman & Rep. Jim Turner, Ranking Member, U.S. House of Representatives Select Comm. on Homeland Sec. (Mar. 25, 2003), *available at* http://www.eff.org/Privacy/TIA/20030324_capps_letter.php (arguing that "Congress should not allow the TSA to develop unilaterally a tool that could invade individual privacy and brand innocent airline passengers a security risk without meaningful review").

On the state level, Florida led a coalition of states in developing the Multistate Anti-TeRrorism Information eXchange ("MATRIX"), with millions in funding from the federal government.[41] MATRIX allowed law enforcement to search through "billions of records from disparate datasets" from participating states as well as "commercially available data sources."[42] The database itself actually was developed and maintained by Seisint, Inc., based on its Accurint service that LexisNexis later acquired.[43] Like TIA, MATRIX provoked criticism for its privacy intrusions,[44] and it shut down last year for lack of continued federal funding.[45] Some states such as Florida, however, have expressed a willingness to continue using the program as it exists.[46]

All of these supermassive databases would enable the government to engage in two distinct forms of what is called "data mining." First, as more commonly used, "data mining" refers to the process of extracting useful, *existing* information from particularly large data sets.[47] The ability to search the supermassive databases of ChoicePoint, LexisNexis, TIA, and MATRIX for relevant existing information on a specific individual or on individuals matching a certain profile[48] fits within this definition of "data mining." Second, as more technically used, "data mining" refers to the

41. *See* Official MATRIX FAQ 2 (2003), *available at* http://www.aclu.org/Privacy/spying/15020res20031202.html; Robert O'Harrow, Jr., *U.S. Backs Florida's New Counterterrorism Database*, Wash. Post, Aug. 6, 2003, at A1.

42. Seisint, Seisint's FACTS for the MATRIX Project 6 (2003), *available at* http://www.aclu.org/privacy/spying/15270res20030929.html. Although the MATRIX itself never disclosed a full list of its database holdings, news reports indicate that they include, among other things, past and present addresses and telephone numbers; names, addresses, and telephone numbers of family members, neighbors, and business associates; social security numbers; birth dates; fingerprints; credit information; property holdings; registered car information; driver's license photos; speeding tickets; criminal histories; court and business filings; marriages and divorces; and Internet domains. *See* Jill Barton, *Controversial Database Shuts Down*, Tallahassee Democrat, Apr. 16, 2005, at A8; Duane Stanford & Joey Ledford, *Matrix Links Private Data*, Atlanta J.-Const., Oct. 10, 2003, at A1.

43. *See* Seisint, *supra* note 42, at 9-11; LexisNexis, LexisNexis Acquires Seisint, Inc., http://www1.seisint.com/ (last visited Jan. 22, 2006).

44. *See, e.g.*, ACLU, Feature on MATRIX (Mar. 8, 2005), http://www.aclu.org/Privacy/Privacy.cfm?ID=14240&c=130.

45. *See* Press Release, Fla. Dep't of Law Enforcement, MATRIX Pilot Project Concludes (Apr. 15, 2005), *available at* http://www.fdle.state.fl.us/press_releases/20050415_matrix_project.html.

46. *See id.*

47. *See* Wikipedia, Data Mining, http://en.wikipedia.org/wiki/Data_mining (last visited Jan. 22, 2006) (defining "data mining" as "'[t]he science of extracting useful information from large data sets or databases") (quoting D. Hand et al., Principles of Data Mining (2001)); *cf.* Henderson, *supra* note 16, at 18 n.66 (observing that "data mining" is "often used to refer to products that merely present existing data in usable form"); Webopedia, Data Mining, http://webopedia.com/TERM/d/data_mining.html (last visited Jan. 22, 2006) (stating that "data mining" is "commonly misused to describe software that presents data in new ways").

48. For example, a company may want to data mine for possible consumers of its products, and law enforcement may want to data mine for possible drug couriers or terrorists.

discovery of useful, *previously unknown* patterns and correlations in such data sets.[49] Each of the programs noted boasts the ability to perform highly useful data mining of this sort as well. For example, ChoicePoint purports that its "i2" software provides investigators with "visual investigative analysis" that enables them "to quickly understand complex scenarios and volumes of seemingly unrelated data."[50] LexisNexis claims that its "Relavint" tool produces "intelligent, visual associations" that "identify links between people, businesses, and other items of interest."[51] MATRIX made a similar claim with respect to its use of the Accurint service.[52] And finally, TIA set out to develop algorithms that would "automatically extract evidence about relationships among people, organizations, places, and things" from immense quantities of "unstructured textual data," based on patterns predictive of terrorist planning and execution.[53] The program would visually represent the evidence to enable "rapid discovery of previously unknown relationships of operational significance."[54]

Assuming these data mining programs live up to their hype, they would enable the government to scour supermassive sets of records about its citizens, obtain information about their lives, and discover insights into their activities on a scale not humanly possible or previously conceivable. For instance, shortly after the September 11th attacks, Seisint used Accurint to create a list of 120,000 individuals in the U.S. with "High Terrorist Factor" scores, which it turned over to the FBI and other federal authorities.[55] It is understandable, then, why the government would want to employ data mining for investigative purposes.[56] The question examined

49. *See* Dictionary.com, Data Mining, http://dictionary.reference.com/search?q=data+mining (last visited Jan. 22, 2006) (defining "data mining" as "data processing using sophisticated data search capabilities and statistical algorithms to discover patterns and correlations in large preexisting databases; a way to discover new meaning in data"); Webopedia, *supra* note 47 (defining "data mining" primarily as "[a] class of database applications that look for hidden patterns in a group of data that can be used to predict future behavior"); Wikipedia, *supra* note 47 (defining "data mining" alternatively as "the practice of automatically searching large stores of data for patterns" or "'[t]he nontrivial extraction of implicit, previously unknown, and potentially useful information from data'" (quoting W. Frawley et al., *Knowledge Discovery in Databases: An Overview*, AI Magazine, Fall 1992, at 213-28)).

50. ChoicePoint, Investigative Solutions, http://www.choicepoint.com/industry/government/i2inc.html (last visited Jan. 22, 2006).

51. Accurint, Newsroom, Seisint Adds Dynamic Visual Link Analysis Tool to Accurint Product Suite (July 27, 2004), http://www.accurint.com/news/news_7_27_2004.html.

52. *See* Seisint, *supra* note 42, at 10 (stating that, through Accurint, MATRIX "employs special fuzzy matching technology that can provide accurate links between records in disparate data sources").

53. Dep't of Def., *supra* note 36, at 7, app. at A-3.

54. *Id.* at 16.

55. Seisint, Matrix First Responder Support 5 (2003), *available at* http://www.aclu.org/Privacy/Privacy.cfm?ID=15814&c=130.

56. Although TIA and MATRIX both have shut down, the government has availed itself liberally of commercially available data mining services. *See, e.g.*, Slobogin, *supra* note 11, at 7 (noting that, from 1999 to 2001, the U.S. Marshal's service ran between 14,000 and

next is whether the government may use them free from any Fourth Amendment fetters.

II. THIRD-PARTY PRECEDENT

As with any other discussion of the Court's modern search jurisprudence, an examination of the third-party doctrine must begin with *Katz v. United States*.[57] In that landmark decision, the Court overruled the holding of *Olmstead v. United States*[58] that a "search" occurs within the meaning of the Fourth Amendment only when the government physically trespasses into a constitutionally protected area.[59] Instead, responding to the threat of electronic surveillance, the Court underscored in *Katz* that "the Fourth Amendment protects people, not places."[60] Accordingly, the Court construed the applicability of the amendment to turn on whether the government "violate[s] the privacy upon which [a person] justifiably relie[s]."[61] Under this view, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[62] However, "what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[63]

The Court did not expand on these conclusory statements to define further the privacy protected by the Fourth Amendment. In his concurrence, however, Justice John Marshall Harlan offered a two-step test that has supplied the analytic framework for subsequent cases.[64] Under this test, first, a person must have "exhibited an actual (subjective) expectation of privacy," and second, the expectation must be "one that society is prepared to recognize as 'reasonable.'"[65] Justice Harlan favored this

40,000 searches per month on data services such as ChoicePoint); Solove, *supra* note 7, at 1095 (describing multimillion dollar contracts between the FBI, the Internal Revenue Service, and other federal agencies with ChoicePoint); ChoicePoint, Public Records Group, http://www.choicepoint.com/industry/government/public.html (last visited Jan. 22, 2006) (listing as clients federal, state, and local government agencies, including the FBI, Drug Enforcement Administration, and U.S. Immigration & Naturalization Service). Additionally, as noted, the government also may be engaging in large-scale data mining through the National Security Agency. *See supra* notes 18, 39.

57. 389 U.S. 347 (1967).

58. 277 U.S. 438 (1928).

59. *See Katz*, 389 U.S. at 352-53 (overruling *Olmstead*).

60. *Id.* at 351.

61. *Id.* at 353.

62. *Id.* at 351.

63. *Id.* at 352. For a discussion of the Court's doctrinal shift from *Olmstead* to *Katz*, see Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 Minn. L. Rev. 349, 357 (1974).

64. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 33 (2001); Smith v. Maryland, 442 U.S. 735, 740 (1979).

65. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

normative inquiry[66] over a trespass-based trigger for Fourth Amendment protection, which he characterized as "bad physics as well as bad law, for reasonable expectations of privacy may be defeated by electronic as well as physical invasion."[67]

Although the Court decided third-party cases prior to *Katz*,[68] it was not until after the *Katz* decision that the Court developed a consistent rationale for addressing and ultimately denying Fourth Amendment claims against government use of information from third parties. The leading cases in that regard were *United States v. Miller*[69] and *Smith v. Maryland*.[70]

In *Miller*, the defendant sought to suppress checks, deposit slips, statements, and other items related to accounts that his banks had turned over to the government pursuant to subpoenas.[71] He argued that he gave those documents to the banks for the "limited purpose" of using their services, and therefore that he otherwise retained "a reasonable expectation of privacy" in those items under *Katz*.[72] The Court, however, turned *Katz* against him. It stressed *Katz's* comment that "'[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.'"[73] It reasoned that, by "voluntarily convey[ing]" his documents to the banks, the defendant "exposed [them] to their employees in the ordinary course of business," and thereby took "the risk . . . that the information will be conveyed" to the government.[74] Furthermore, referring to its pre-*Katz* cases, the Court noted that it had "held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities."[75] This had been so, added the Court, "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[76]

66. For a discussion of the normative nature of the inquiry, see 1 Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment § 2.1(d), at 443-44 (4th ed. 2004).

67. *Katz*, 389 U.S. at 362 (Harlan, J., concurring).

68. *See, e.g.*, Hoffa v. United States, 385 U.S. 293, 302 (1966) (finding no Fourth Amendment violation in the government's use of an informant to listen to the defendant's hotel-room conversations, as he was "not relying on the security of the hotel room" but "upon his misplaced confidence that [the informant] would not reveal his wrongdoing"); Lopez v. United States, 373 U.S. 427, 439 (1963) (finding no Fourth Amendment violation in an Internal Revenue Service agent's entry into the defendant's office and recording conversations with him, as there was no "physical invasion of [his] premises" and the agent was there "with [his] assent").

69. 425 U.S. 435 (1976).

70. 442 U.S. 735 (1979).

71. *See Miller*, 425 U.S. at 438-39.

72. *Id.* at 442.

73. *Id.* (quoting Katz v. United States, 389 U.S. 347, 351 (1967)).

74. *Id.* at 442-43.

75. *Id.* at 443.

76. *Id.* (citing United States v. White, 401 U.S. 745, 752 (1971); Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States, 373 U.S. 427 (1963)).

Thereafter, in *Smith*, the Court rejected the claim that the use of a pen register at a telephone company to record the numbers dialed from the defendant's home constituted a "search."[77] Following Justice Harlan's framework more closely, the Court first expressed doubt as to whether the defendant subjectively expected privacy in the numbers he dialed. Even though the defendant argued that he did expect privacy because he called from his home, the Court observed that "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company" to complete their calls, and that such companies record those numbers, as evidenced by the monthly bills in which they appear.[78] In any event, as in *Miller*, the Court concluded that any such privacy expectation cannot be reasonable, because the defendant "voluntarily conveyed" the numbers to the telephone company, and by doing so "assumed the risk" that the company would reveal them to the police.[79]

Miller and *Smith* exemplify the rationale the Court has invoked in other post-*Katz* cases to reject Fourth Amendment claims involving other matters conveyed to third parties, such as private conversations recorded by an informant in *United States v. White*,[80] or garbage placed curbside for collection in *California v. Greenwood*.[81] In short, regardless of whether we may expect privacy in information "voluntarily conveyed" to a third party, that kind of expectation is categorically unreasonable, given the "risk" we "assumed" that the party would disclose those matters to the government. This is so, apparently, regardless of how unlikely or unknown the risk, or how necessary the risk-taking to life in our society. Like the bakers in *Lochner v. New York*[82] or the railroad worker in *Farwell v. Boston & Worcester R.R. Corp.*,[83] we presumptively exercise a knowing and willing choice over the risks we assume.[84] Consequently, it is easy to predict how

77. Smith v. Maryland, 442 U.S. 735, 745-46 (1979).

78. *Id.* at 742.

79. *Id.* at 743-44.

80. 401 U.S. 745, 749 (1971) (holding that "'a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it'" is not an expectation of privacy protected by the Fourth Amendment (quoting *Hoffa*, 385 U.S. at 302)).

81. 486 U.S. 35, 40 (1988) (holding that no reasonable expectation of privacy can exist in trash so "exposed" to "animals, children, scavengers, snoops, and other members of the public," and moreover left curbside "for the express purpose of conveying it to a third party, the trash collector, who might himself have sorted through respondents' trash or permitted others, such as the police, to do so").

82. 198 U.S. 45 (1905).

83. 45 Mass. (4 Met.) 49 (1842).

84. *Cf. Lochner*, 198 U.S. at 53, 56 (holding that the liberty component of the Fourteenth Amendment's Due Process Clause guarantees "[t]he right to purchase or to sell labor," including apparently the right of workers to voluntarily assume the health risks of working long hours in unsanitary conditions under contracts that "may seem . . . appropriate or necessary"); *Farwell*, 45 Mass. (4 Met.) at 57 (stating "[t]he general rule, resulting from considerations . . . of justice as of policy . . . that he who engages in the employment of another for the performance of specified duties and services, for compensation, takes upon

the Court will decide any third-party case. As Justice William J. Brennan described the Court's recurrent reasoning in another context, "while the sets sometimes change, the actors always have the same lines."[85]

III. IS DATA MINING A SEARCH UNDER THE THIRD-PARTY DOCTRINE?

Without Justice Stevens to complicate matters, analyzing whether data mining may constitute a "search" regulated by the Fourth Amendment is a fairly straightforward exercise. Reading the "lines" from the Court's third-party cases, we must first ask whether any of us subjectively expects privacy in our records in third-party databases. The answer, of course, depends on the individual. Do we personally care whether records of our phone calls, banking transactions, credit card purchases, web surfing, physical location, and the like remain private? Judging from the reaction to the recent spate of breaches of commercial databases, including those of ChoicePoint and LexisNexis,[86] it appears that many of us do.[87]

himself the natural and ordinary risks and perils incident to the performance of such services, and in legal presumption, the compensation is adjusted accordingly").

85. United States v. Leon, 468 U.S. 897, 949 (1984) (Brennan, J., dissenting). Justices and commentators have roundly criticized the Court's third-party doctrine. *See, e.g.*, *Greenwood*, 486 U.S. at 56 (Brennan, J., dissenting) (stating that "[t]he American society with which I am familiar . . . is more dedicated to individual liberty and more sensitive to intrusions" into privacy "than the Court is willing to acknowledge" in its application of the doctrine); 1 LaFave, *supra* note 66, § 2.7(b), at 736 (criticizing the *Smith* Court for a "crabbed interpretation of the *Katz* test" that "makes a mockery of the Fourth Amendment").

86. *See, e.g.*, Eric Dash & Tom Zeller, Jr., *MasterCard Says 40 Million Files Are Put at Risk*, N.Y. Times, June 18, 2005, at A1 (reporting on the MasterCard International disclosure that more than forty million credit card accounts might have been exposed to data thieves); Bill Husted & David Markiewicz, *Info. Theft Slams Chain 1.4 Million Card Numbers Stolen*, Atlanta J.-Const., Apr. 20, 2005, at A1 (noting that, in addition to Ameritrade losing a backup tape with files on over 200,000 clients, DSW Shoe Warehouse had disclosed unauthorized access by data thieves to a database with credit card records on about 1.4 million customers, and ChoicePoint had disclosed unauthorized access by data thieves to information on 145,000 individuals); Bruce Mohl, *Concerns Over ID Theft Mount*, Boston Globe, Apr. 13, 2005, at D1 (reporting LexisNexis's disclosure that information on about 310,000 individuals may have been stolen); Tom Zeller, Jr., *Personal Data on Millions of Citigroup Clients Lost in Transit*, Int'l Herald Trib., June 8, 2005, at 14 (reporting that United Parcel Service lost Citibank Citifinancial computer tapes with account information on 3.9 million customers). For consumer reactions, see *infra* note 87.

87. *See, e.g.*, Tom Zeller, Jr., *The Scramble to Protect Personal Data*, N.Y. Times, June 9, 2005, at C1 (reporting that at least twenty-two bills to combat identity theft have been proposed in Congress since January 2005); Frank Davies, *Congress to Take Up Growing Problem of Identity Theft*, Yahoo! News, Mar. 9, 2005, http://story.news.yahoo.com/news?tmpl=story&u=/krwashbureau/20050309/ts_krwashbureau/_bc_cpt_idtheft_wa_1 (reporting on congressional hearings into how data brokers acquire and sell information, on the need for new laws "to improve security and privacy," on consumer groups pushing for such legislation, and on Senator Nelson stating that "[i]f we don't do something in the law, no American will have any privacy left").

Regardless, any expectation of privacy that we may have would be unreasonable under *Miller* and *Smith*'s risk-assumption rationale.[88] As noted, the risk we assume in conveying information to a third party is that the party would disclose that information to the authorities, and it is the possibility of that disclosure that makes any privacy expectation unreasonable.[89] Under this rationale, there is no distinction between a direct conveyance of information to the authorities and the conveyance of information to a database that the government might mine. The risk of exposure of either sort is present when we convey the information, and therefore any expectation of privacy loses Fourth Amendment protection at that point as well.[90]

IV. IS DATA MINING A SEARCH UNDER JUSTICE STEVENS'S JURISPRUDENCE?

Justice Stevens has joined the majority in all of the Court's third-party cases, with the exception of *White*, which preceded his tenure on the Court. Consequently, he has proven a reliable vote for curtailing Fourth Amendment protections in the third-party context, at least in cases that have directly addressed the doctrine. However, Justice Stevens is not a judge who applies rules and rationales mechanically. Rather, under his jurisprudence, they often yield to compelling facts or fundamental principles overlooked by others.[91] This too may be the case with respect to the third-party doctrine, for close consideration of Justice Stevens's statements in *Ferguson*, *Kyllo*, and *Caballes* suggests Fourth Amendment

88. However, it bears repeating that the third-party doctrine may not apply to data mining of the content of telephone calls and emails acquired from communications couriers rather than their intended recipients—a practice that the National Security Agency reportedly has engaged in over the past several years. *See supra* note 39. As explained *supra* note 18, such content acquired from such sources may not be considered third-party data.

89. *See* Smith v. Maryland, 442 U.S. 735, 744 (1979); United States v. Miller, 425 U.S. 435, 443 (1976).

90. Not surprisingly, other commentators applying the third-party doctrine to government data mining also have concluded that the Fourth Amendment provides no protection. *See, e.g.*, Henderson, *supra* note 16, at 20 (concluding that the third-party doctrine "provides no leash at all" on government data mining); Hoofnagle, *supra* note 30, at 622 (concluding that "[t]he current conception of protections under the Fourth Amendment," and in particular under *Miller*, "provides individuals with little protection" against government use of commercial data brokers); Slobogin, *supra* note 11, at 18-21 (observing that, with respect to government use of MATRIX, Choicepoint, or other government data mining, "the Fourth Amendment is pretty much irrelevant" in light of *Smith* and *Miller*, but also noting a possible Fourth Amendment limitation in the medical context under *Ferguson v. City of Charleston*, 532 U.S. 67 (2001)); Solove, *supra* note 7, at 1137-38 (discussing the "inapplicability of the Fourth Amendment" under *Smith* and *Miller* to "[g]overnment information gathering from the extensive dossiers being assembled with modern computer technology").

91. *See generally* Frederick Schauer, *Justice Stevens and the Size of Constitutional Decisions*, 27 Rutgers L.J. 543 (1996); Joseph T. Thai, *John Paul Stevens*, *in* Encyclopedia of Am. Civil Liberties (forthcoming 2006), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=872855.

principles that may limit the doctrine as well as its application to government surveillance through data mining.[92]

A. Ferguson v. City of Charleston

In *Ferguson*, pregnant women at a state hospital underwent drug testing, the results of which were turned over to law enforcement for criminal prosecution.[93] The state contended that such testing accorded with the Fourth Amendment under the Court's "special needs" doctrine, which determines the constitutionality of a search by weighing the government's intrusion into privacy against its non-law-enforcement interests.[94] In that doctrinal context, considering the privacy interest at stake, Justice Stevens's majority opinion observed that "[t]he reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent."[95] The privacy expectation is reasonable even though, as Justice Stevens acknowledged, reporting laws "might lead a patient to expect" his medical providers to turn over incriminating evidence to the police.[96]

This assessment of the typical patient's privacy interest is the only majority statement contrary to the third-party doctrine in result and reasoning. It flatly contradicts the previously impervious notion that the risk of disclosure assumed in conveying information to a third party, even in the strictest confidence, makes any expectation of privacy in that information unreasonable.[97] Accordingly, later in his opinion, Justice Stevens attempted to distinguish *Ferguson* from traditional third-party cases on the ground that the Court here assumed that the patients did not consent

92. While Justice Stevens has stated that "[i]t would be far wiser to give legislators an unimpeded opportunity to grapple with these emerging issues [of technological surveillance] rather than to shackle them with prematurely devised constitutional constraints," Kyllo v. United States, 533 U.S. 27, 51 (2001) (Stevens, J., dissenting), he has not hesitated to "say what the law is" under the Fourth Amendment and elsewhere when necessary to decide a case, Marbury v. Madison, 5 U.S. (1 Cranch) 137, 177 (1803). *See* Thai, *supra* note 91 (manuscript at 5).

93. *Ferguson*, 532 U.S. at 73, 77. The policy under which the drug testing occurred was developed by medical staff in conjunction with law enforcement, with the "ultimate goal" of treating substance abuse but also "the immediate objective" of generating evidence for the police. *Id*. at 82-83.

94. *Id.* at 76-78.

95. *Id.* at 78.

96. *Id.* at 78 n.13.

97. For example, in *United States v. Miller*, 425 U.S. 435 (1976), *United States v. White*, 401 U.S. 745 (1971), and *Hoffa v. United States*, 385 U.S. 293, 302 (1966), the Court rejected the argument that conveyance of information to a third party for a presumably limited and private purpose preserves Fourth Amendment protection against police acquisition of that information from the third party for law enforcement purposes. *See supra* notes 71-85 and accompanying text. By contrast, the Court in *Ferguson* suggested that the typical patient may succeed on a claim that the relinquishment of privacy to a third party in a confidential context does not necessarily amount to a relinquishment for other purposes.

to testing, and therefore did not voluntarily turn over their information.[98] However, this factual distinction did not undermine the assessment, which referred broadly to "the reasonable expectation of privacy" of "the typical patient," who presumably consents to medical testing at least for the limited purpose of treatment.[99] Consequently, in dissent, Justice Antonin Scalia complained that the majority had "open[ed] a hole" in the third-party doctrine, "the size and shape of which is entirely indeterminate."[100] Likewise, commentary on *Ferguson* has noted the inconsistency between Justice Stevens's statement and prior third-party decisions.[101]

Given that statement, *Ferguson* suggests that the Court may not apply the third-party doctrine as relentlessly as its rationale and prior cases dictate. Notably, the conclusory language hearkens back to *Katz*'s ultimately normative approach for determining what the Fourth Amendment protects.[102] Consistent with *Katz*'s qualification that "what [we] seek[] to preserve as private, even in an area accessible to the public, may be constitutionally protected,"[103] the opinion did not categorically deny the reasonableness of a typical patient's expectation of privacy based on a theoretical risk of third-party disclosure. Rather, it evinced a value judgment that such an expectation nonetheless may be worthy of constitutional protection. The opinion thus implies that normative considerations may override application of the third-party doctrine.

Justice Scalia's criticism notwithstanding, it may be possible to glean the "size and shape" of this normative "hole" from *Ferguson* itself. At the very least, Justice Stevens's opinion indicates that a patient's conveyance of relevant information for medical care does not necessarily make a privacy expectation in that information unreasonable.[104] More broadly, the opinion suggests that, rather than focusing solely on risk assumption in the third-

98. *Ferguson*, 532 U.S. at 85 n.24.

99. *Id.* at 78.

100. *Id.* at 95 (Scalia, J., dissenting).

101. *See, e.g.*, Slobogin, *supra* note 11, at 20-21 & nn.54-55 (noting that the Court "has wavered in its willingness to declare private entities untrustworthy confidants only in the medical context," and citing *Ferguson* as a Fourth Amendment example).

102. *See supra* notes 65-66 and accompanying text.

103. Katz v. United States, 389 U.S. 347, 351-52 (1967).

104. Even prior to *Ferguson*, this argument was not that far-fetched. *See, e.g.*, Doe v. Broderick, 225 F.3d 440, 451 (4th Cir. 2000) (holding that the Fourth Amendment protects medical records, notwithstanding *Miller*, because they "contain intimate and private details that people do not wish to have disclosed, expect will remain private, and, as a result, believe are entitled to some measure of protection from unfettered access by government officials"). For a discussion of "existing norms and the norm-shaping power of the law" with respect to information disclosed by patients to physicians, see Solove, *supra* note 7, at 1155-56. Additionally, some commentators have suggested that medical records also might be protected under the Court's due process jurisprudence. *See* Henderson, *supra* note 16, at 6 & n.29 (observing that "[m]edical records might be protected by a *Griswold/Whalen/Roe* right to privacy"); Slobogin, *supra* note 11, at 21 & n.54 (observing that, in addition to "the dictum" in *Ferguson* suggesting Fourth Amendment protection, "the due process clause *might* place constitutional limitations on law enforcement access" to medical records).

party context, the reasonableness inquiry under *Katz* also should focus on the nature of the privacy interest, considering the type of information and the circumstances of disclosure. Thus, in different situations, one might ask whether other information from third parties is as private in character as the results of medical testing, and whether it was disclosed in as confidential a setting.[105] If so, then the privacy expectation may be one that is reasonable.

More subtly, Justice Stevens's opinion may be read to reinterpret functionally and practically the requirement of the third-party doctrine that the conveyance of information be voluntary. Generally speaking, patient disclosures in the context of medical care may be elective in a metaphysical sense,[106] and hence voluntary under third-party precedent.[107] However, they may be necessary to obtain essential medical services and may be made only for that limited purpose. Consequently, considering the function of such disclosures and their practical necessity, they may not meaningfully amount to a general relinquishment of privacy in the information disclosed. *Ferguson*'s positive assessment of the reasonableness of a typical patient's privacy expectation may reflect this view. If so, then applying *Ferguson*, one might ask whether other disclosures to third parties fairly constitute general relinquishments of privacy or serve the more limited function of obtaining services that have become essential to life in our society.[108]

105. *But cf.* United States v. White, 401 U.S. 745, 749 (1971) (stating that Fourth Amendment "affords no protection to 'a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it'" (quoting Hoffa v. United States, 385 U.S. 293, 302 (1966))).

106. *Cf.* Dickerson v. United States, 530 U.S. 428, 434 (2000) (holding the Due Process Clause to require exclusion of confessions where "'a defendant's will was overborne'" (quoting Schneckloth v. Bustamonte, 412 U.S. 218, 226 (1973))).

107. *Cf.* United States v. Miller, 425 U.S. 435, 443 (1976) (treating banking transactions as voluntary disclosures "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed").

108. *Cf.* Smith v. Maryland, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting) (arguing that "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"). *But cf.* Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 Mercer L. Rev. 507, 526 (2005) (arguing that the third-party doctrine should be limited to information "voluntarily provided to a third party *for that party's use*"). Measured against the privacy interest and context of disclosure in *Ferguson*, certain expectations of privacy in more modern forms of information conveyed to third parties may be entitled to Fourth Amendment protection. For example, consider the information collected by ISPs regarding our online activities, including all the web pages we visit, the people we email, and the times we access the Internet from our own homes. *See supra* note 3 and accompanying text. It does not take much imagination to realize that the nature of the information may be as intimate, if not more, than the results of medical testing. Furthermore, while conveyances of this data may not occur in the context of a confidential relationship, the activities that generate them occur in a setting—the home—whose protection constitutes "the very core" of the Fourth Amendment. Kyllo v. United States, 533 U.S. 27, 31 (2001) (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)). Finally, like medical records, privacy in this kind of information is protected to some degree by

If other third-party records compare favorably with information conveyed for medical care, then *Ferguson* suggests that the Fourth Amendment may protect privacy expectations in them as a normative matter, notwithstanding the third-party doctrine. Logically, this protection should apply whether the government obtains those records directly from third parties or indirectly through mining data sets amassed by the likes of TIA, MATRIX, LexisNexis, or ChoicePoint.[109] The more difficult question is whether *Ferguson* would protect against information aggregation, from records not separately protected, if the aggregation would be impossible without data mining.

To answer this question, consider the amount of aggregation that data mining may achieve. As noted, the data mining programs examined tout their ability to comb through "tens of billions"[110] of public and private records to assemble a "comprehensive" dossier[111] on us with "the click of a button."[112] That dossier would "far exceed[] the capacity of unaided humans" to create,[113] and could provide a window into our lives more revealing than any snooping in our doctors' offices or intrusions into our homes.[114] Furthermore, that dossier would only grow increasingly detailed over time, as more and more aspects of our lives become digitized in the databases of third parties with whom we interact—sometimes by genuine choice, but often out of practical necessity. Finally, that dossier may not appear as an unorganized mass of information. Tools for data mining in the technical sense[115] may draw "intelligent, visual associations"[116] that enable the "rapid discovery of previously unknown relationships" within our lives as well as between them.[117] As a result, at some point in time, if not now

legislation requiring the government to obtain a subpoena in order to compel its disclosure from third parties. *See supra* note 11; *see also* Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 Colum. L. Rev. 279, 309-10 (2005) (discussing requirements for subpoenaing records from ISPs under the Electronic Communications Privacy Act); *cf.* Christopher Slobogin, *Subpoenas and Privacy*, 54 DePaul L. Rev. 805, 836-37 (2005) (arguing that, given the private nature of personal information held by third-party recordholders such as ISPs, hospitals, and banks, the government should be required to make a heightened showing to subpoena such information). Of course, such an application of *Ferguson* may call into question cases involving arguably analogous information, such as telephone dialing or bank records. *See supra* notes 71-79 and accompanying text (discussing *Smith* and *Miller*).

109. As noted, the government does, apparently frequently, engage in such data mining. *See supra* note 56.

110. Accurint, *supra* note 35.

111. ChoicePoint, *supra* note 31.

112. Accurint, *supra* note 35; *see also* Solove, *supra* note 7, at 1084 (coining the phrase "digital dossier"); *supra* notes 31-42 and accompanying text.

113. Dep't of Def., *supra* note 36, at 2.

114. *See supra* notes 32, 34, 38, 42 and accompanying text.

115. *See supra* note 49 and accompanying text.

116. Accurint, *supra* note 51.

117. Dep't of Def., *supra* note 36, at 16; *see supra* notes 49-53 and accompanying text.

already, the word "diary" rather than "dossier" may more appropriately describe what data mining may expose about each of us.[118]

At that point, surely *Ferguson* should short circuit the application of the third-party doctrine. Even if none of the data individually would implicate privacy interests as justifiable as those interests in the medical treatment context, it is hard to imagine a more valued expectation of privacy in our free society than this: No one, especially the government, will monitor virtually every aspect of our lives.[119] If this expectation is unreasonable, then no privacy protected by the Fourth Amendment may amount to much, for by data mining, the government may learn vastly more about us than by more traditional methods of invading our privacy.[120]

B. Kyllo v. United States *and* Illinois v. Caballes

Reading Justice Stevens's opinion in *Ferguson* to override the third-party doctrine normatively is not without its problems. In the data-mining context, two objections readily come to mind. First, because private parties

118. *Cf.* Solove, *supra* note 27, at 1 (observing that "[i]t is ever more possible to create an electronic collage that covers much of a person's life—a life captured in records, a digital person composed in the collective computer networks of the world"). Professor Daniel Solove has also evocatively described this "aggregation problem" caused by "the accumulation of details" as "[s]imilar to a Seurat painting, where a multitude of dots juxtaposed together form a picture." Solove, *supra* note 7, at 1154.

119. *See* United States v. Jacobsen, 466 U.S. 109, 138 (1984) (Brennan, J., dissenting) (stating that "this Court ultimately stands ready to prevent [an] Orwellian world from coming to pass"); George Orwell, 1984 (1949); *see also* Solove, *supra* note 27, at 175 (observing that "[h]istorically, totalitarian governments have developed elaborate systems for collecting data about people's private lives").

120. At least one commentator has suggested that *Ferguson*'s "undermining of *Miller's* premise" provides "a glimmer of hope" for protection from information surveillance such as data mining that creates "personality mosaics" through information aggregation. Slobogin, *supra* note 11, at 46, 55-56 (internal quotations omitted). While beyond the scope of this Article, it is worth noting that other commentators, who have recognized that the third-party doctrine in its current form offers no protection against data mining, *see supra* note 90, have suggested non-Stevens-specific routes to regulate data mining under the Fourth Amendment, in whole or part. For example, Professor Stephen Henderson has argued that construing the third-party doctrine to apply only to information given to a third party for its use would call into question data mining such information from "a database of entirely unforeseeable scope and intent" to the original giver. Henderson, *supra* note 108, at 548. Alternatively, Professor Solove has argued that the "aggregation problem" should be tackled by regulating (by "a fusion of Fourth Amendment architecture and the architecture of subpoenas and court orders") government access to third-party "systems of records," because the root of the problem lies in growing data collection by the private sector. Solove, *supra* note 7, at 1089, 1152-59. Professor Christopher Slobogin has provided a thoughtful critique of the latter approach, in which he concludes that "the [degree] of that protection should depend on the degree of privacy associated with the information, not simply on whether it exists in record form." Slobogin, *supra* note 11, at 47-51. For his part, in proposing such a regime of proportional protection, Professor Slobogin has concluded that, while the Fourth Amendment might supply some of that protection after *Ferguson*, the source "is not so important" as "[t]he goal [of] meaningful protection of personal information." *Id.* at 30-46, 56. However, as I have argued, constitutional protections may be more desirable than statutory ones. *See supra* note 11.

may avail themselves of the most invasive sorts of data-mining services, little if any privacy appears to remain for the Fourth Amendment to protect. Second, because data mining does not expose new information but only facilitates new inferences, it does not create any cognizable incursions into privacy. To these objections, statements by Justice Stevens in *Kyllo* and *Caballes* suggest responses that preserve the historical role of the Fourth Amendment in guarding against arbitrary government intrusions, and that imply an important principle, independent of *Ferguson*, for limiting application of the third-party doctrine to advancing forms of technological surveillance.

Of relevance to the first objection, companies such as ChoicePoint and LexisNexis offer their supermassive databases and data-mining programs commercially. Credit card companies, banks, insurers, employers, landlords, attorneys, detectives, angry spouses, and other private parties may avail themselves of the services these data brokers offer.[121] What additional privacy interest, then, would be served by hindering law enforcement access? Indeed, suggesting that the answer would be none, the Court has often stated the general rule that the police may view what may be available "from a public vantage point."[122]

In response, one might start with the basic observation that, while the Constitution does not restrain surveillance by private parties, no matter how intrusive,[123] it does restrict government snooping. After all, it was colonial experience with arbitrary government searches and seizures that "was one of the major catalysts of the struggle for independence," as well as the adoption of the Fourth Amendment.[124] Thus, in the famous words of

121. *See* Accurint Home Page, http://www.accurint.com/ (last visited Jan. 22, 2006) (linking to services for "banking," "collections," "government," "insurance," "law enforcement," and "legal profession"); ChoicePoint Home Page, http://www.choicepoint.com (last visited Jan. 22, 2006) (displaying a drop-down menu of various "industry," "business," and "consumer" solutions); *see also supra* note 30 (listing other publicly available, searchable supermassive databases).

122. California v. Ciraolo, 476 U.S. 207, 213 (1986); *see also* Florida v. Riley, 488 U.S. 445, 449 (1989); *cf.* Horton v. California, 496 U.S. 128, 133 (1990) (stating that "[i]f an article is already in plain view, neither its observation nor its seizure would involve any invasion of privacy" protected by the Fourth Amendment); Katz v. United States, 389 U.S. 347, 351 (1967) (stating that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection").

123. *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984) (observing that the Fourth Amendment "proscrib[es] only government 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'" (quoting Walter v. United States, 447 U.S. 649, 662 (1980) (Blackmun, J., dissenting))).

124. United States v. N.Y. Tel. Co., 434 U.S. 159, 180 & n.3 (1977) (Stevens, J., dissenting in part); *see* Nelson B. Lasson, The History and Development of the Fourth Amendment to the United States Constitution 51-78 (1937); Orin S. Kerr, *Search and Seizure: Past, Present, and Future*, *in* Oxford Encyclopedia of Legal History (forthcoming 2006), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=757846. *See generally* Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 Mich. L. Rev. 547 (1999).

Justice Louis D. Brandeis's *Olmstead* dissent, the Fourth Amendment originally "conferred, *as against the Government*, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."[125] Consequently, the fact that private parties may invade our privacy should not necessarily preclude Fourth Amendment protections.[126]

Justice Stevens appeared to endorse this fundamental point in his *Kyllo* dissent. There, the Court held that the use of a thermal imager to detect heat radiating from a home constituted a "search."[127] However, the majority implied that Fourth Amendment protections would dissipate once the technology was "in general public use."[128] In dissent, Justice Stevens criticized this criterion as "somewhat perverse because it seems likely that the threat to privacy will grow, rather than recede, as the use of intrusive equipment becomes more readily available."[129] By doing so, Justice Stevens implied that the privacy protected by the Fourth Amendment is not simply a general expectation of secrecy that may be defeated by private intrusions.[130] Rather, as a safeguard from arbitrary state intrusions, the provision entitles us to expect a certain degree of privacy from our government, even if it is invaded by our neighbors.[131]

125. Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting). In *California v. Hodari D.*, Justice Stevens quoted with approval Justice Louis D. Brandeis's "eloquent[]" statement regarding "the overarching purpose of the Fourth Amendment." 499 U.S. 621, 646 n.18 (1991) (Stevens, J., dissenting); *cf.* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 195 (1890) (discussing "the right to be let alone" (internal quotation omitted)).

126. *See* Joshua Dressler, Understanding Criminal Procedure 124 (3d ed. 2002) (observing, in criticizing *Ciraolo*, 476 U.S. at 213, for holding that aerial surveillance from an airplane is not a search because flights in public airways are routine, that "[t]his fact of modern life . . . does not answer the question of whether a person should have a *right* to expect privacy in this regard, *at least from government surveillance*"); *cf. Katz*, 389 U.S. at 351-52 (stating that "what [someone] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected").

127. Kyllo v. United States, 533 U.S. 27, 34-35 (2001).

128. *Id.* at 34.

129. *Id.* at 47 (Stevens, J., dissenting). On the perversity of this criterion, see Christopher Slobogin, *Peeping Techno-Toms and the Fourth Amendment: Seeing Through* Kyllo*'s Rules Governing Technological Surveillance*, 86 Minn. L. Rev. 1393, 1393-95 (2002) (arguing that *Kyllo* may be "a pyrrhic victory," because the "general public use" exception may eventually "swallow the Court's newly minted prohibition of technologically enhanced investigation of homes").

130. *Cf.* Solove, *supra* note 7, at 1136 (arguing that the third-party doctrine "stems from a particular conception of privacy that views Fourth Amendment privacy as constituting a form of total secrecy. . . . If information is not secret in this way, if it is in any way exposed to others, then it loses its status as private."). In earlier cases, however, Justice Stevens implied a contrary view. *See* United States v. Jacobsen, 466 U.S. 109, 117 (1984) (Stevens, J.) (holding that "[t]he Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated" by an antecedent private search); Walter v. United States, 447 U.S. 649, 657 (1980) (Stevens, J., plurality opinion) (same).

131. *Ferguson* of course provides an example and perhaps a measure of when Justice Stevens may find that the Fourth Amendment protects privacy against government intrusion, even when that privacy may have been compromised previously by exposure to other parties.

The second objection to extending the Fourth Amendment to data mining is that doing so essentially would treat inferences as searches. As the argument goes, data mining under its common definition[132] simply makes information retrieval more efficient by finding needles of data in a haystack of records, and data mining in the technical sense[133] simply organizes the needles to make patterns and connections more apparent. Because data mining merely reveals and rearranges information already compromised by third-party conveyances, data mining's only arguably new incursions into privacy are the additional inferences it enables. Thus, if the Fourth Amendment applies to data mining at all, then its application must target those inferences.

To this objection, Justice Stevens suggested an answer in his majority opinion in *Caballes*. Responding to the argument that the drug-sniffing canine in that case and the thermal imager in *Kyllo* belong in the same unconstitutional kennel, Justice Stevens separated them into two distinct breeds based on the kinds of inferences they enable. On the one hand, dog sniffs detect evidence of illegal drugs only, and therefore enable inferences only about the occurrence of unlawful activities. On the other hand, thermal imagers detect evidence of heat, and therefore enable inferences about the occurrence of both lawful behavior, such as the taking of a sauna and bath, and unlawful behavior, such as the growing of marijuana indoors.[134]

This additional capability was "[c]ritical" to the *Kyllo* decision, according to Justice Stevens.[135] As he noted, the Court established in *United States v. Place*,[136] which involved another dog sniff, and *United States v. Jacobsen*,[137] which involved a chemical test for illegal drugs, that technology detecting only evidence of illegality "does not compromise any legitimate interest in privacy" protected by the Fourth Amendment.[138] In

It is worth noting here that the reading of Justice Stevens's *Kyllo* dissent proffered in the text—protective of privacy in one critical respect—is not inconsistent with his vote to dissent in that case. His dissent was not based on any general hostility to protecting privacy, but on his belief that the limited capabilities of the thermal imager in that case—merely to detect heat emissions "in the public domain"—did not compromise any reasonable expectation of privacy. *Kyllo*, 533 U.S. at 42, 45 (Stevens, J., dissenting). Instead, Justice Stevens suggested that the Fourth Amendment should extend to the use of technology that provides the government with "the functional equivalent of actual presence" in an otherwise private area. *Kyllo*, 533 U.S. at 47; *cf. id.* at 49 (characterizing *Katz* as a case in which an electronic listening device made officers "the functional equivalent of intruders because they gathered information that was otherwise available only to someone inside the private area"). Furthermore, as discussed *infra* note 142, Justice Stevens also critiqued another aspect of *Kyllo*'s holding that he did not think sufficiently protective of privacy in other situations.

132. *See supra* note 47 and accompanying text.

133. *See supra* notes 49-54 and accompanying text.

134. *See Kyllo*, 533 U.S. at 44 (Stevens, J., dissenting).

135. Illinois v. Caballes, 125 S. Ct. 834, 838 (2005).

136. 462 U.S. 696 (1983).

137. 466 U.S. 109 (1984). Justice Stevens authored the majority opinion in this case.

138. *Id.* at 123; *see also Place*, 462 U.S. at 707.

contrast, Justice Stevens explained, devices such as the thermal imager in *Kyllo* do implicate the Fourth Amendment, because a "legitimate expectation" exists that "information about perfectly lawful activity will remain private."[139]

By thus differentiating thermal imagers and dog sniffs, Justice Stevens's *Caballes* opinion suggested a new Fourth Amendment principle, which is the converse of the *Place-Jacobsen* principle. To wit, if the use of technology to detect only evidence of illegal activity is not a search, because any compromised privacy expectation in such activity is not legitimate, then the use of technology to detect evidence of more than that may constitute a search, because it may compromise legitimate privacy expectations in lawful activity. Indeed, the suggested principle may be stated more broadly. Given that the thermal imager in *Kyllo* detected heat that could be attributed correctly to unlawful activity (marijuana growing),[140] or incorrectly to lawful activity (sauna bathing),[141] *Caballes* implies that the Fourth Amendment governs technologically enabled inferences concerning the occurrence of lawful activities where one reasonably may expect privacy, regardless of whether those inferences are correct. Enabling those inferences may compromise privacy expectations worthy of Fourth Amendment protection.

Of course, this no-enabling-inferences-about-the-occurrence-of-lawful-and-private-activities principle (or *Kyllo-Caballes* principle for short) emerges merely by implication rather than by adoption.[142] Consequently, it is unclear whether the principle, expressly stated, would garner majority support on the Court. For the same reason, the parameters of the principle remain largely unexplored. For example, if adopted, would the Court construe the principle narrowly, to apply only when technology enables inferences to a degree that provides the government with the "functional

139. *Caballes*, 125 S. Ct. at 838.

140. *See* Kyllo v. United States, 533 U.S. 27, 30 (2001).

141. *Id.* at 38.

142. Nevertheless, this principle seems to follow from Justice Stevens's prior reading of *Kyllo*. In dissent there, he criticized the majority for equating the detection of relative amounts of heat outside of a home, in a public area, with a search of its interior. *See id.* at 45 (Stevens, J., dissenting). Reasoning that any information obtained regarding interior activities only came about as a result of inferences from exterior data, Justice Stevens concluded that the majority had "assume[d] that an inference can amount to a Fourth Amendment violation." *Id.* at 44. Writing for the majority in *Caballes*, Justice Stevens of course had to accept *Kyllo* as governing law. In explaining the decision, however, he appeared to have adopted his inferences-may-be-searches understanding of *Kyllo*. Additionally, by describing *Kyllo* essentially as the converse of *Place* and *Jacobsen*, neither of which was set near a home, Stevens implied that *Kyllo*'s inference principle could extend beyond the confines of the home to other private areas deserving of Fourth Amendment protection. This implication would be consistent as well with his dissenting view in *Kyllo*. *See id.* at 48-49 (arguing that "a rule that is designed to protect individuals from the overly intrusive use of sense-enhancing equipment should not be limited to a home," but should extend to other "private place[s]").

equivalent of actual presence" in a private area?[143] So limited, the principle would find support in prior precedent, as well as in Justice Stevens's views in *Kyllo*.[144] However, it would run counter to the crude capability of the thermal imager in that case.[145] Alternatively, more consistent with that fact, would the Court construe the principle broadly, to apply to the technological enabling of any inference (correct or incorrect) regarding the occurrence of lawful activity in a private area? So construed, the principle could dramatically expand the scope of the Fourth Amendment. While information "knowingly expose[d] to the public" would remain beyond the provision's protection,[146] the technological use of that information to enable inferences about underlying activities could fall within the amendment's reach.

Interpreted either way, the *Kyllo*-*Caballes* principle would represent a significant paradigmatic shift. *Jacobsen* and *Place* have served as a sword for slashing claims of privacy in situations where technology detects only evidence about the presence or absence of illegality.[147] The *Kyllo*-*Caballes* principle would transform that sword into a shield in situations where technology detects evidence of potentially more than mere illegality. If taken broadly, the principle may protect against the use of other devices, mentioned by Justice Stevens in *Kyllo*, that "detect[] emissions in the public domain such as . . . traces of smoke, . . . odorless gases, airborne particulates, or radioactive emissions."[148] Furthermore, as relevant here, the principle may guard against data mining to the extent that its needle-finding or, especially, its rearranging function enables inferences about activities in which a legitimate expectation of privacy exists.[149] The enabling of such inferences is not far-fetched. Considering the size and scope of supermassive databases and their touted data-mining capabilities,[150] data mining may make possible an immense range of conclusions about who we are and what we do. Finally, even narrowly

143. *See id.* at 47.

144. In *Kyllo*, Justice Stevens stated that he would "not erect a constitutional impediment to the use of sense-enhancing technology unless it provides its user with the functional equivalent of actual presence in the area being searched." *Id.*; *cf.* United States v. Karo, 468 U.S. 705, 715 (1984) (holding that the use of an electronic beeper attached to a container to infer the latter's presence in a home constituted a search, because the government "could not have otherwise" verified that fact without physically entering the premises).

145. *See Kyllo*, 533 U.S. at 50-52 (Stevens, J., dissenting) (noting that the device only produced "vague thermal images of petitioner's home," and displaying those images in an appendix).

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

147. *See Conduct Constituting a Search or Seizure*, 33 Geo. L.J. Ann. Rev. Crim. Proc. 10 & n.19 (2004) (citing cases).

148. *Kyllo*, 533 U.S. at 45; *see also id.* at 48 (arguing that *Kyllo* would make Fourth Amendment searches out of inferences enabled by "new devices that might detect the odor of deadly bacteria or chemicals for making a new type of high explosive").

149. As such, the principle would operate independently of Ferguson's normative limitations on the third-party doctrine and data mining. *See supra* Part IV.A.

150. *See supra* Part I.

construed, the *Kyllo*-*Caballes* principle still may provide some Fourth Amendment protection against data mining. When data mining can construct digital diaries from third-party records,[151] if not earlier, then it certainly will provide more than the "functional equivalent of actual presence" in a private area.[152] It will supply the virtual equivalent of our lives.

In the end, whatever the scope of the *Kyllo*-*Caballes* principle if adopted, it would critically enlarge current Fourth Amendment protections. While *Katz* may protect against government snooping in areas where we reasonably expect privacy, the third-party doctrine leaves constitutionally exposed data from which the government can infer what activities may occur there. The *Kyllo*-*Caballes* principle would provide some constitutional cover against surveillance of such information, based on the insight that enabling inferences about our activities at some point may compromise our privacy as much as actual exposure. That cover may preserve the Fourth Amendment for the future. If, as one commentator has observed, the third-party doctrine is "the new *Olmstead*,"[153] whose trespass regime rendered the provision obsolete in the face of electronic surveillance, then perhaps the *Kyllo*-*Caballes* principle will serve as the new *Katz*, updating the Fourth Amendment for an age of information surveillance.[154]

CONCLUSION

Under Justice Stevens's jurisprudence, data mining of information we previously conveyed to third parties may constitute a "search" governed by the Fourth Amendment. While this result contradicts the third-party doctrine, Justice Stevens has suggested that normative considerations rather than risk assumption ultimately must determine the extent of our freedom from unreasonable searches; that this freedom from government intrusion deserves greater rather than lesser protection when our privacy is threatened by technological forces beyond our control; and that technology-enabled inferences about our personal lives may violate this freedom as much as actual exposure of our private activities. Admittedly, gleaned as they are from opinions dealing neither with the third-party doctrine nor data mining, these suggestions may seem too vague or broad to follow in future cases

151. *See supra* notes 112-18118 and accompanying text.

152. *See Kyllo*, 533 U.S. at 47 (Stevens, J., dissenting).

153. *See* Solove, *supra* note 7, at 1137.

154. *See* Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) (stating that to protect the Fourth Amendment's right "to be let alone," "every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation"); Lawrence Lessig, Code 115, 116 (1999) (interpreting Brandeis to mean that "[t]he aim must be to *translate* the original protections of the Fourth Amendment into a context in which the technology for invading privacy ha[s] changed," in order to "neutralize[] those changes and preserve[] an original meaning").

without additional fleshing. Moreover, it is not at all certain that the Court, or even Justice Stevens, will embrace these suggestions when confronted with third-party cases involving data mining, or will continue to assume that information transfers, even in this day and age, involve voluntary risk assumptions that dissipate our privacy. Still, these are wise suggestions. They point the way to a future in which the Fourth Amendment may staunch the loss of privacy from surveillance technologies that approach total information awareness about us. When that day comes, we can thank Justice Stevens's jurisprudence at least for supplying us with the constitutional coagulants.