TRANSACTION SURVEILLANCE BY THE GOVERNMENT

Christopher Slobogin[*]

Many important aspects of our lives are inscribed in written and digitized records, housed in private businesses, government agencies and other institutions. These records include all sorts of information about us: reports on our medical status and financial condition; data about our purchases, rentals, real estate holdings, licenses, and memberships; logs listing the destination of our emails and our Internet wanderings; and countless other bits of individual descriptors, ranging from salary levels to college grades to driver's license numbers. Whether the information memorializes our own version of personal activities or is created by the record-holder itself, there is often an explicit or implicit understanding that the information will be used or viewed by a limited number of people for circumscribed purposes. In other words, we consider the contents of many of these records private, vis-a-vis most of the world.

Thus, it may be surprising that law enforcement officials can, perfectly legally, gain access to all of this information much more easily than they can search our houses or even our cars. While the latter types of actions require probable cause, government can obtain many of the records just described simply by asking (or paying) for them.[1] And, at most, all the

---

[*] Stephen C. O'Connell Professor of Law, University of Florida Fredric G. Levin College of Law. For their comments on this paper, I would like to thank Jerold Israel, Scott Sundby, Peter Swire, George Thomas, and participants in workshops or symposia at the following schools: Mississippi, DePaul, Florida State, Ohio State, and Hastings.

[1] *See generally* Daniel J. Solove, *Access and Aggregation: Public Records, Privacy and the Constitution*, 86 MINN. L. REV. 1137 (2002).

government needs to show in order get any of these records is that they are "relevant" to a government investigation–a much lower, and much more diffuse, level of justification than probable cause.[2]

This state of affairs might make sense when the records sought are truly public in nature. It might also be justifiable when the records involve an entity such as a corporation, professional service provider, or government department and are sought in an effort to investigate the entity and its members. But today, facilitated by the computerization of information and communication, government routinely obtains *personal* medical, financial and email records, in connection with investigations that have nothing to do with business or governmental corruption.[3] That practice is much more questionable.

This article explores the scope and regulation of what I will call "transaction surveillance" by the government. That term is meant to distinguish the subject of this article from both "physical surveillance" and "communications surveillance." Physical surveillance is real-time observation of physical activities, using either the naked eye or enhancement devices such as binoculars or video cameras. Communications surveillance is real-time interception of the content of communications, relying on wiretapping, bugging, hacking, and various other methods of intercepting oral statements and wire and electronic transmissions. Transaction surveillance, in contrast, involves accessing *already-existing* records, either physically or through computer databanks. It also encompasses accessing, in real-time or otherwise, the *identifying signals* of a transaction (such as the address of an email recipient).[4]

Like physical and communications surveillance, transac-

---

[2] *See infra* text accompanying notes 35-37.

[3] *See* Solove, *supra* note 1.

[4] This tripartite division of surveillance was developed by the American Bar Association's Task Force on Law Enforcement and Technology and is explicated further in Christopher Slobogin, *Technologically-Assisted Physical Surveillance: The American Bar Association's Tentative Draft Standards*, 10 HARV. J. L. & TECH. 383, 387-88 (1997).

tion surveillance is a potent way of discovering and making inferences about a person's activities, character and identity. Yet, despite a bewildering array of statutorily created authorization requirements, transaction surveillance by the government is subject to far less regulation than either physical surveillance of activities inside the home or communications surveillance.[5] My principal argument is that transaction surveillance should be subject to much more legal monitoring than it is.

To get to that conclusion, this article proceeds in four parts. Part I explains why government, and in particular law enforcement, finds transaction surveillance so attractive, and why it is so easy to carry out in this digital age. Part II describes the current law regulating transaction surveillance. Not only is this regulation minimal, it is confusing and contradictory; beyond the traditional subpoena, challengeable by the target of the investigation, current law recognizes a number of subpoena mutations that seem to have little rhyme or reason. If it contributes nothing else, this article should at least clarify the nature of today's regulatory framework.

Part III criticizes this framework and outlines a more promising approach. The proposed reform recognizes, as does the current regime, that different sorts of records merit different levels of protection. But, in contrast to current law, the proposal would significantly increase the degree of protection in a number of situations, to the probable cause level for personal records held by private and public entities and to the reasonable suspicion level for personal records readily available to the public.

Part IV concludes by examining alternatives to the pro-

---

[5] As discussed *infra* text accompanying notes 38-82, transaction surveillance never requires probable cause. In contrast, communications surveillance requires a warrant,, which may be issued only if there is probable cause and other methods of obtaining the information have failed. *See* 18 U.S.C. § 2518(3). Physical surveillance of the home requires a warrant unless it can take place with the naked eye from a lawful vantage point using technology that only replicates such naked eye viewing or it involves technology that is in general public use. Kyllo v. United States, 533 U.S. 27, 34-35 (2001).

posal (and to the current regime). It rejects both an approach that requires probable cause for all records searches and, at the other extreme, an approach that would allow suspicionless records searches on condition that anything discovered is subject to strict limitations on disclosure. It also criticizes an approach that relies on the legislature, rather than the courts and the Fourth Amendment, to establish fundamental regulatory requirements. Not all recorded information warrants the maximum refuge from government intrusion. But much of it deserves much more protection than it receives today.

I. THE CURRENT REACH OF TRANSACTION SURVEILLANCE

Transaction surveillance comes in many forms. This article divides it into two types: target-based and event-based. Using these categorizations, the following discussion relies on hypotheticals to flesh out the various ways transaction surveillance can assist law enforcement in investigating street crime.

A. Target-Based Transaction Surveillance

Assume that I'm a federal agent, and that I'm suspicious of you for some vague reason–perhaps you often pay for your airplane tickets with cash,[6] or you have been observed with accessories you shouldn't be able to afford,[7] or you are a young, Arab male who goes to the local mosque on a daily basis.[8] Under these types of circumstances, I clearly do not have sufficient suspicion for an arrest.[9] On the other hand, I

---

[6] *Cf.* Florida v. Royer, 460 U.S. 491, 493 n.2 (1983) (noting that paying for an airline ticket with cash is often an element of drug courier profiles used by the Drug Enforcement Administration).

[7] *Cf.* State v. Cookson, 361 S.W.2d 683, 684 (Mo. 1962) (informant, who alleged that defendants had robbed a tavern, reported that "they had a large sum of money and were spending freely").

[8] *Cf.* Michael J. Whidden, *Unequal Justice: Arabs in America and United States Antiterrorism Legislation*, 69 FORDHAM L. REV. 2825, 2865 (2001) (recounting FBI surveillance of a Brooklyn mosque).

[9] An arrest or prolonged questioning in the stationhouse requires probable cause. CHARLES H. WHITEBREAD & CHRISTOPHER SLOBOGIN, CRIMINAL PROCEDURE:

feel I would be neglecting my obligation as a law enforcement official if I did not investigate you a bit further. So how do I find out more about you?

I could confront you directly, either on the street or through a grand jury.[10] But neither approach is likely to net much information, and both will tip you off that I'm checking you out. Ditto with respect to going to your acquaintances and neighbors; they will probably not be complely forthcoming and they might let you know I've been nosing around. I could try the undercover agent approach–there might be rich payoffs if I or one of my informants can weasel into your good graces. But success at that endeavor is rare, and spending so much effort on someone about whom I'm merely suspicious would usually be a waste of time. I could also surreptitiously follow you around for awhile, but that tactic is unlikely to produce much, especially if you make most of your contacts through technological means–phones, email–rather than physical travel. Of course, I could tap your phone and intercept your emails, but that requires a warrant based on probable cause, which I do not have.

Thankfully there are other, much more efficient ways I can covertly acquire information about you, many of which I can carry out without leaving my desk and most of which, as the next section describes, require no or little legal authorization. The easiest way to get useful data is to contact one of the many companies, usually called commercial data brokers (CDBs), that use computers and the Internet to dig up "dirt" from public and not-so public records.[11] One such company is LexisNexis, the legal research bohemoth, which operates

---

AN ANALYSIS OF CASES AND CONCEPTS 72-76 (4th ed. 2000).

[10] Note further that even questioning in the field that lasts longer than a few minutes requires reasonable suspicion, which exists only if there are specific and articulable facts that the person is or has been engaging in criminal activity. *Id.*

[11] In fact, the website for one of these companies can be found at "digdirt.com". The services are of uneven quality. *See* Preston Gralia, *Digital Gumshoes*, *available at* http://www.pcmag.com/article2/0,4149,20148,00.asp (Nov. 13, 2001) (recounting efforts to use various services, including digdirt, with mixed results). For present purposes, however, the point is that their potential for transaction surveillance is enormous.

Accurint, a program that allows "organizations to quickly and easily extract valuable knowledge from . . . tens of billions of data records on individuals and businesses," armed with no more than a name, address, phone number, or social security number.[12] Through this process, I can obtain information about a wide array of your transactions, including: bankruptcies and corporate filings, criminal convictions and criminal and civil court data (including marriage and divorce information), driver's licenses and motor vehicle information, firearms, hunting, fishing and professional licenses and permits, Internet domain names, property deeds and assessments, and voter registration information.[13] For some states, the information held in "public records" by government bureaucracies and available via computer is immensely broader: some types of medical records, Social Security numbers, crime victim's names, credit card and account numbers, psychiatric evaluation reports, tax returns, payroll information, and family profiles.[14] For a time, all of this was made even more easily accessible to state law enforcement officials through MATRIX (Multi-State Anti-Terrorist Information Exchange), a multistate consortium that allowed police to use Accurint for investigative purposes until its federal funding was discontinued in 2005.[15]

The FBI and other federal agencies rely on equally powerful commercial data brokers, with perhaps the most popular being Choicepoint.[16] Under its contract with the federal gov-

---

[12] *See* Accurint Website, *available at* www.accurint.com/aoutus.html (last accessed on Sept. 13, 2005). LexisNexis bought Accurint from SeisInt in 2005.

[13] *Id.*

[14] Robert Ellis Smith, *Here's Why People Are Mad*, 29 PRIVACY J. 7, 7 (Jan. 2003) (citing Stephen Grimes, administrator of the Judicial Records Center in Rhode Island), *available at* http://www.privacyjournal.net/.

[15] *See* Fla. Dep't Law Enforcement, MATRIX Pilot Project Concludes (April 14, 2005), *available at* http://www.fdle.state.fl.us.press_releases/20050415_matrix_project (noting, however, that Florida and several other states may continue funding the program).

[16] *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 & COMM. REG. 595, 617-18 (describing the FBI's "secret, classified contract" with Choicepoint).

ernment, Choicepoint can provide me, as a federal agent, with "credit headers" (information at the top of a credit report which includes name, address, previous address, phone number, social security number and employer); pre-employment screening information (including financial reports, education verification, reference verification, felony check, motor vehicle record and professional credential verification); "asset location services"; information about neighbors and family members; licenses (driver's, pilot's and professional); business information compiled by state bureaucracies; and "derogatory information" such as arrests, liens, judgments and bankruptcies.[17] If you think I wouldn't bother requesting such a check, think again; between 1999 and 2001, Choicepoint and similar services ran between 14,000 and 40,000 searches per month for the United States Marshall's Service *alone*.[18]

The one drawback to the type of information I get from CDBs is that it is pretty general. I may want to know more about what you do on a daily basis. Fortunately, there are a number of services that can help me out. For instance, advances in data warehousing and data exchange technology in the financial sector allow very easy access to a virtual cornucopia of transaction-related information that can reveal, among other things, "what products or services you buy; what charities, political causes, or religious organizations you contribute to; . . . where, with whom, and when you travel; how you spend your leisure time; . . . whether you have unusual or dangerous hobbies; and even whether you participate in certain felonious activities."[19] If I jump through some pro for-

---

[17] *Id.* at 601-02. Note also that once a social security number and other identifying information is obtained, other personal information might become much more easily accessible. *See* Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 TEX. L. REV. 89, 108-14 (2001) (pointing out that schools, financial institutions and other entities make personal information accessible by anyone with the right Social Security number, address, and mother's maiden name).

[18] *Id.* at 4-6. In 2001, the Immigration and Naturalization Service conducted approximately 23,000 such searches a month. *Id.* at 11.

[19] Janet Dean Gertz, *The Purloined Personality: Consumer Profiling in Financial Services*, 39 SAN DIEGO L. REV. 943, 944-45, 951 (2002).

ma legal hoops (detailed in Part II), I can also get records of all the phone numbers you dial and receive calls from,[20] and from your Internet Service Provider (ISP) I can get every website address you have visited (so-called "clickstream data") and every email address you have contacted.[21]

The latter information can be particularly revealing to the extent you transact your business over the Internet. Recently some ISPs, like America OnLine, have stopped maintaining clickstream data, precisely so they won't have to answer such law enforcement requests.[22] No worries. All I have to do is invest in something called "snoopware." Bearing names like BackOrifice, Spyagent, and WinWhatWhere,[23] snoopware is to be distinguished from adware and spyware. The latter software tells the buyer of the program how to contact people who visit the buyer's website. Snoopware, in contrast, allows its buyer to track the target well beyond a single website; it accumulates the addresses of *all* the Internet locations the target visits, as well as the recipients of the target's emails. The FBI has developed a similar program, once dubbed Carnivore, now called DCS-1000, that filters all emails that pass through a particular server.[24] Although some transaction snoopware

---

[20] The Electronic Communications Privacy Act, 18 U.S.C. § 3121 allows prosecutors to obtain this information by certifying to a court that it is "relevant" to an ongoing investigation. *See infra* text accompanying notes 43-47.

[21] The Electronic Communications Privacy Act at most requires a showing of relevance for this information. *See* 18 U.S.C. § 3121; *infra* notes 69-77 and accompanying text; *see also* Gavin Skok, *Establishing a Legitimate Expectation of Privacy in Clickstream Data*, 6 MICH. J. TELECOMM. & TECH. L. REV. 61, 68-69 (2000) (detailing the type of information government can obtain through clickstream data).

[22] Conversation with Peter Swire, Professor, Ohio State School of Law, September 20, 2004. The Electronic Frontier Foundations has recommended that ISPs only keep personally identifiable communications logs for "so long as it is operationally necessary, and in no event for more than a few weeks." Electronic Frontier Foundation, *Best Data Practices for Online Service Providers*, from the Electronic Frontier Foundation *at* http://www.eff.org/osp/20040819_OSPBestPractices.pdf2 (June 29, 2005).

[23] *See* Cade Metz, *Spyware: It's Lurking on Your Machine*, PC MAG., Apr. 22, 2003, at 85, 88.

[24] Jeremy C. Smith, *The USA PATRIOT Act: Violating Reasonable Expectations of Privacy Protected by the Fourth Amendment Without Advancing National Secu-*

requires access to the server or computer to install, other types, called Trojan Horses, can electronically worm their way onto the system disguised as something useful.[25]

In short, even if you stay at home and conduct all your business and social life via phone, email and surfing the 'Net, I can construct what one commentator has called "a complete mosaic" of your characteristics.[26] And I can do all of this without you having a clue I'm doing it. It is also possible that I could surreptitiously obtain an even wider array of transactional information–on matters ranging from medical treatment to financial decisions–with very little effort. But further discussion of that possibility, as well as of the huge amount of transactional information that government can obtain if it is willing to proceed overtly, will have to await Part II's explanation of the current legal regime.

B. Event-Based Transaction Surveillance

Now consider an entirely different type of scenario, one in which government has no suspicion of or even interest in a specific individual, but rather possesses information about a particular crime that has been or will be committed. Government efforts to obtain transactional data in this situation is not target-based, but event-based. Say, for instance, that the police know that a sniper-killer wears a particular type of shoe (thanks to mudprints near a sniper site), that he owns a

---

rity, 82 N.C. L. REV. 412, 448-49 (2003). Recently, the FBI announced that it would no longer use DCS-1000, but instead rely on "unspecified commercial software to eavesdrop on computer traffic." *FBI Cuts Carnivore Internet Probe*, *at* http://www.cnn.com/2005/TECH/internet/01/18/fbi.carnivore.ap/index.html (on file with the *Mississippi Law Journal*).

[25] Metz, *supra* note 23, at 85. Some snoopware, using "key logger" technology, can even tell the user the content of one's computer screen. *Id.* DCS-1000 can also be programmed to access content as well as identifying information. Joseph F. Kampherstein, *Internet Privacy Legislation and the Carnivore System*, 19 TEMP. ENVTL. L. & TECH. J. 155, 167 (2001). Both functions are forms of communications surveillance that are beyond the scope of this article.

[26] Anthony Paul Miller, *Teleinformatics, Transborder Data Flows and the Emerging Struggle for Information: An Introduction to the Arrival of the New Information Age*, 20 COLUM. J. L. & SOC. PROBS. 89, 111 (1986).

particular type of sweater (because of threads found at another site), and that he reads Elmore Leonard novels (because of allusions to those books made in his communications to the police). Law enforcement understandably might want to peruse the purchase records of local shoe, clothing, and book stores as part of their investigation. Once police obtain the credit card numbers of those who bought, say, the type of sweater found at the murder scene, they can trace other purchases made with the same card, to see if the relevant type of shoe or book was bought by any of the same people. Of course, if there is a match on two or three of the items, the surveillance may then turn into a target-based investigation.

Or say that a CIA informant reports that he believes Al Qaeda is considering blowing up a major shopping mall, using skydivers jumping from rental planes.[27] The FBI might want to requisition the records of all companies near major metropolitan areas that teach ski-diving and that rent airplanes, as well as the "cookie" logs (records of cyberspace visitors) of all websites that provide information about manufacturing explosives, to see if there are any intersections between these three categories of data, in particular involving men with Arab-sounding names. If there are then, again, further target-based surveillance investigation might take place.

Although the first type of event-based surveillance is backward-looking and the second is forward-looking, both law enforcement efforts are a form of what has been called "data mining" or "profiling," that is, an attempt to look through transaction information to find patterns of behavior that permit police to zero in on possible suspects.[28] If the information sought is not digitized, which is likely with respect to records kept by ski-diving companies, for instance, then law enforce-

---

[27] This imaginary scenario is borrowed from the second Markle Report. Markle Foundation, Creating a Trusted Network for Homeland Security: Second Report of the Markle Foundation Task Force, app. D at 121-33 (2003), *available at* http://www.markletaskforce.org/.

[28] For a general description of data mining and its prevalence, see Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 71-88 (2003).

ment may have to rely on good old-fashioned human snooping. In this day and age, however, a significant amount of data mining can be carried out using technology. For example, the Defense Department's Total Information Awareness program, before it was severely limited by Congress, would have used software developed by private companies "to sift through virtual mountains of data of everyday transactions, such as credit card purchases, e-mail and travel itineraries, in an attempt to discover patterns predictive of terrorist activity."[29] Whether it relies on computers or humans, event-based data mining, like transaction surveillance of particular individuals, can easily be conducted unbeknownst to those whose records are surveilled.

C. Summary

Technology has made transaction surveillance a particularly powerful law enforcement tool. Given the potential that transaction surveillance provides the government for creating personality mosaics and linking people to crime, it could well be even more useful than visual tracking of person's activities (physical surveillance) and eavesdropping on or hacking into a person's communications (communications surveillance). But the real beauty of transaction surveillance for the government is that, compared to physical surveillance of activities inside the home and communications surveillance, it is so lightly regulated. As Part II explains, under today's regulatory regime it is much easier for government to obtain information about our most intimate transactions, including medical and financial matters, than it is to intercept our communications about those transactions.

II. CURRENT LEGAL REGULATION OF TRANSACTION SURVEILLANCE

Under the Fourth Amendment, the government usually cannot conduct a search of houses, persons, papers and effects

---

[29] *Id.* at 64; *see also infra* note 122.

without probable cause,[30] a relatively high level of certainty akin to a more-likely-than-not standard (which, in non-exigent situations, must be found by a magistrate pursuant to an application for a warrant).[31] For some less invasive actions (a frisk, for instance), police only need reasonable suspicion, which is a lower level of certainty than probable cause but still requires "specific and articulable facts" that "criminal activity may be afoot," to quote from the famous case of *Terry v. Ohio*.[32] Finally, in some "special needs" situations (searches of school children or employees; drug testing; health and safety inspections; roadblocks), the police need only act "reasonably," but that test still usually requires reasonable suspicion,[33] or at least a showing that those conducting the government action are pursuing some end other than criminal law enforcement.[34]

In contrast, transaction surveillance, whether it is event-based or target-based, *never* requires probable cause or reasonable suspicion, even when conducted by government agents whose primary goal is criminal investigation. At most, government agents seeking transactional information need a subpoe-

---

[30] *See* U.S. CONST. amend. IV.

[31] *See* WHITEBREAD & SLOBOGIN, *supra* note 9, at 137-42.

[32] 392 U.S. 1, 21, 30 (1968).

[33] *See* O'Connor v. Ortega, 480 U.S. 709, 724 (1987) ("The delay in correcting the employee misconduct caused by the need for probable cause rather than reasonable suspicion will be translated into tangible and often irreparable damage to the agency's work, and ultimately to the public interest."); New Jersey v. T.L.O., 469 U.S. 325, 341-42, 344 (1985) (holding that "a search of a student by a teacher or other school official will be 'justified at its inception' when there are reasonable grounds for suspecting that the search will turn up evidence" and finding that this standard was met in this case because there was reasonable suspicion).

[34] *See* Bd. of Educ. v. Earls, 536 U.S. 822, 829 (2002) (upholding warrantless, suspicionless school drug testing, noting that "in the context of safety and administrative regulations, a search unsupported by probable cause may be reasonable when 'special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable'"); City of Indianapolis v. Edmond, 531 U.S. 32, 41 (2000) ("We have never approved a checkpoint program whose primary purpose was to detect evidence of ordinary criminal wrongdoing. Rather, our checkpoint cases have recognized only limited exceptions to the general rule that a seizure must be accompanied by some measure of individualized suspicion.").

na–either a subpoena duces tecum issued by a grand jury, or an "administrative subpoena" issued by a government agency–which is valid as long as the information it seeks is "relevant" to a legitimate (statutorily-authorized) investigation. Relevance, as defined by the Supreme Court, is an extremely low standard. In the grand jury context, a subpoena may be quashed on irrelevancy grounds only when the court "determines that there is no reasonable *possibility* that the *category* of materials the Government seeks will produce information relevant to the *general subject* of the grand jury's investigation."[35] The relevancy standard in the administrative subpoena context is even lower, with the Supreme Court holding that "[e]ven if one were to regard the [subpoena] as caused by nothing more than official curiosity, nevertheless law-enforcing agencies have a legitimate right to satisfy themselves that corporate behavior is consistent with the law and the public interest."[36] In short, the link between the information a subpoena commands and the investigation the government is pursuing can be very tenuous indeed. Although a subpoena may be challenged before it is executed, a successful challenge is exceedingly rare, whether the subpoena is issued by a grand jury or an administrative agency.[37]

Furthermore, as we shall see, the law does not require even a traditional subpoena for most types of transaction surveillance. Instead, the government, in particular Congress,

---

[35] United States v. R. Enters., Inc., 498 U.S. 292, 301 (1991) (emphasis added).

[36] United States v. Morton Salt Co., 338 U.S. 632, 652 (1950); *see also* United States v. Powell, 397 U.S. 48, 57-58 (1964) (holding that administrative subpoenas are valid if the records sought are "relevant" to an investigation conducted for a "legitimate purpose"); United States v. Hunton & Williams, 952 F. Supp. 843, 854 (D.D.C. 1997) (holding that the *Powell* inquiry is more deferential than the "arbitrary and capricious" standard of review for agency action under the Administrative Procedure Act).

[37] *See* WAYNE R. LAFAVE, JEROLD H. ISRAEL & NANCY J. KING, 3 CRIMINAL PROCEDURE 134 (2d ed. 1999) ("Courts generally give grand juries considerable leeway in judging relevancy."); JACOB A. STEIN, GLENN A. MITCHELL & BASIL J. MEZINES, 3 ADMINISTRATIVE LAW 20-59 (2002) ("[S]ubpoenas will be enforced as to any documents that 'are not plainly immaterial or irrelevant to the investigation.'").

has either invented new forms of authorization that are even easier to obtain or has simply permitted unrestrained law enforcement access to transactional information. The following account of this incredibly weak regulatory regime starts with the law regarding transaction surveillance of identifying information, conducted in real-time, then describes regulation of government attempts to obtain public records, and finally describes transaction surveillance of records held by private entities.

A. Interception of Transaction Information

Real-time government interception of the *content* of communications (what I am calling communications surveillance) is prohibited unless authorized by a warrant based on probable cause.[38] In contrast, interception of the identifying features of the communication–the names of the communicators, their phone numbers or email addresses, and the addresses of websites visited–can take place on a much lesser showing. The Fourth Amendment does not apply at all to this type of transaction surveillance, and statutory law places virtually no restrictions on it.

The Fourth Amendment's justification requirements–probable cause and the like–only apply if government engages in a "search or seizure." Although one might reasonably label government efforts to track down a person's phone and email correspondents a search, the Supreme Court has held that a *Fourth Amendment* search occurs only when a government action infringes a reasonable expectation of privacy.[39] More importantly for present purposes, the Court has determined, in *Smith v. Maryland*,[40] that we do not have a

---

[38] 18 U.S.C. § 2518(3). The court must also find that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous." *Id.* § 2518(3)(c).

[39] Kyllo v. United States, 533 U.S. 27, 33 (2001) ("[A] Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.") (citing Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

[40] 442 U.S. 735 (1979).

reasonable expectation in the phone numbers we dial because we know or should know that phone companies keep a record of these numbers, and thus "assume the risk" that the phone company will decide to disclose this information to the government.[41] Because it is generally known that Internet service providers monitor, if only temporarily, our emails and Internet surfing, the Court would probably also say that we assume the risk these providers will become government informants. Although Universal Resource Locators (URLs) can be more informative than a mere phone number, both because they are addresses (e.g., www.amazon.com/kidneydisease) and because they allow access to the website and thus permit government to ascertain what the user has viewed, the lower courts applying *Smith* appear to see no difference between the two types of routing information.[42] Accordingly, the government can probably ignore the Fourth Amendment when intercepting phone numbers *and* Internet addresses.

---

[41] *Id.* at 744 ("[P]etitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business . . . [thereby] assum[ing] the risk that the company would reveal to police the numbers he dialed.")

[42] *Cf.* Thygeson v. U.S. Bancroft, No. CU-03-467-ST 2004 WL 2066746 (D. Or. Sept. 15, 2004) ("[W]hen the information defendants collected was only the website addresses, rather than the actual content of the websites Thygeson visited, [the surveillance] is analogous to a pen registry search, where in the Fourth Amendment context, courts have held that defendants have no reasonable expectation of privacy in the telephone numbers they dial because the numbers are conveyed to the telephone company."); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) ("When defendant entered into an agreement with Road Runner for Internet service, he knowingly revealed all information connected to the IP address . . . ."); *see also infra* note 46. Billing records of ISPs may also be unprotected by the Fourth Amendment. United States v. Hambrick, 225 F.3d 656 (4th Cir. 2000) (unpublished opinion) (holding that person does not have a reasonable expectation of privacy "in the account information given to the ISP in order to establish the e-mail account, [because it] is non-content information" disclosure of which "to a third party destroys the privacy expectation that might have existed previously"), *available at* 2000 U.S. App. LEXIS 18665, at *12. Indeed, some courts have held that the *content* of email messages, once they are opened, deserve no Fourth Amendment protection because one assumes the risk the recipient will reveal it to others. United States v. Charbonneau, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997); Smyth v. Pillsbury, 914 F. Supp. 97, 101 (E.D. Pa. 1996); United States v. Maxwell, 45 M.J. 406, 417-18 (C.A.A.F. 1996).

Congress has imposed some statutory restraints on this type of surveillance, but nothing approaching the usual Fourth Amendment protections. In the Electronic Communications Privacy Act of 1986 (ECPA), it created a new, streamlined type of authorization process for use of pen registers (technology which intercepts outgoing phone numbers) and trap and trace devices (technology which intercepts incoming numbers), a process that can be initiated by either a federal government attorney or a state law enforcement officer. All the government agent must do is certify to a court facts that show the information is "relevant to an ongoing investigation" and is "likely to be obtained by [the surveillance]."[43] If that certification is made, the court *must* issue the order.[44]

The USA Patriot Act of 2001 expanded the definition of pen registers and trap and trace devices to include all devices that obtain "dialing, routing, addressing, or signaling information utilized in the processing and transmitting of wire or electronic communications . . . "[45] Thus, to use snoopware, DCS-1000, and other means of ascertaining a person's email correspondents and favorite websites, the government need only certify the relevance of this information to a current investigation.[46] Again, if this certification is made, the court must issue an order.

Those of us who teach Fourth Amendment law sometimes

---

[43] 18 U.S.C. § 3123(a)(1) (2000).

[44] United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995) (the "judicial role in approving use of trap and trace devices is ministerial in nature").

[45] 18 U.S.C. § 3121(c) (2000).

[46] Most courts have held that companies that acquire "clickstream data" about where an Internet user goes on the Internet do not violate ECPA because the websites visited by the user have authorized the companies to access this information. *See In re* DoubleClick, Inc., Privacy Litig., 154 F. Supp. 2d 497, 526 (S.D.N.Y. 2001); Chance v. Ave. A, Inc., 165 F. Supp. 2d 1153, 1163 (W.D. Wash. 2001); *In re* Toys R Us, Inc., Privacy Litig., No. C00-2746 2001 U.S. Dist. LEXIS 16947, at *28 (N.D. Cal. Oct. 9, 2001). Thus, government could also obtain routing information from these private companies, without using snoopware. However, some courts might consider that approach to be accessing "stored" information. *See, e.g.*, United States v. Steiger, 318 F.3d 1039, 1050 (11th Cir. 2003). If so, government may have to obtain a subpoena. *See infra* text accompanying notes 65-68.

joke about supposedly "neutral and detached" magistrates rubberstamping warrant applications, but we also assume that judicial independence is theoretically possible.[47] Here, in contrast, Congress has legislatively invented *mandatory* rubberstamping. It is tempting to call this type of authorization a "rubberstamp order," but I will instead use the more measured term *certification order*. Whatever one calls the authorization process, it amounts to minimal limitation on interception of transaction information.

B. Access to Publicly-held Records

Most transaction surveillance does not involve real-time interception of information, but rather contemplates accessing already-existing records, held either by public or private institutions. Information in public records is particularly easy to secure. Under current law, law enforcement officials do not need even a certification order to use MATRIX, Choicepoint and similar vehicles for perusing public records. In fact, law enforcement officials need consult *no* other entity (certainly not a court, and not even a prosecutor) before obtaining such information.

Again, the Fourth Amendment's ban on unreasonable searches and seizures might appear to apply here, because looking for and through records is a search in the usual meaning of the word. But, as already noted, the Supreme Court has made clear that one cannot reasonably expect privacy in connection with information voluntarily given to third parties. Even more important than *Smith* in this regard is *United States v. Miller*,[48] decided three year earlier. There the Court held that once a person surrenders information to an agency or institution, he or she assumes the risk the third party will

---

[47] See RICHARD VAN DUIZEND, L. PAUL SUTTON & CHARLOTTE A. CARTER, THE SEARCH WARRANT PROCESS: PRECONCEPTIONS, PERCEPTIONS AND PRACTICES 47-48 (1985) (describing study of warrant process indicating varying degrees of judicial rubberstamping across jurisdictions).

[48] 425 U.S. 435 (1976).

hand it over to the government.[49] The key declaration in *Miller* is worth quoting in full: "[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, *even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.*"[50]

The Privacy Act, enacted by Congress in 1974, does bar or limit access to public records when they are sought by private individuals, and even when most government officials want them.[51] But when *law enforcement* officials are after the records, the Act merely requires a letter from the head of the agency that is seeking the information, detailing the law enforcement reasons a particular person's records are needed.[52] No court is involved, and neither individualized suspicion or even a relevance showing is required, just the sayso of the law enforcement department. I will call this kind of authorization an *extrajudicial certification.*

Not even this level of authorization is necessary for government access to most public records, however. The Privacy Act only applies to federal documents. Unless there is similar legislation at the state level, law enforcement access to state public records is unrestricted.[53] Furthermore, the federal gov-

---

[49] *Miller*, 425 U.S. at 443.

[50] *Id.* at 443 (emphasis added).

[51] *See* 5 U.S.C. § 552a(b) (2000) ("No agency shall disclose any record which is contained in a system of records . . . unless [listing 12 exceptions].").

[52] *Id.* § 552a(b)(7) (permitting disclosure "to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought").

[53] *See* Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 605 (1995) (most states lack "omnibus data protection laws," but rather have "scattered laws [that] provide only limited protections for personal information in the public sector."). One reason Florida is an attractive place to base an operation like MATRIX is that its public records law is quite extensive. *See* FLA. STAT. § 119.01 *et seq.* ("It is the policy of this state that all state, county and municipal records

ernment takes the position that when it obtains information from a commercial data broker like Choicepoint, the Privacy Act does not apply at all, because the Act literally only refers to law enforcement efforts to get records from other government agencies and from private companies that are administering a system of records for the government.[54] Under this interpretation, the only obstacle to complete government access to all the data maintained by commercial brokers is the price of the information.[55]

C. Access to Privately-held Records

Compared to the meager limitations on intercepting transactional information and accessing public records, the restrictions on government access to the contents of records held by nominally private entities, such as hospitals and banks, phone companies and Internet providers, have more teeth, but the teeth are blunt. Again, the Fourth Amendment is pretty much irrelevant here. The notion that one assumes the risk that third parties will be, or turn into, government informants applies to private entities as well as public agencies. The Supreme Court has specifically so held with respect to phone companies (in *Smith*)[56] and banks (in *Miller*).[57] It has wavered in its willingness to declare private entities untrustworthy confidants only in the medical context, where it has stated, in dictum, that the Fourth Amendment or the due process clause *might* place constitutional limitations on law enforcement access.[58] Although there are also statutory constraints

---

shall be open for personal inspection by any person."). Recognizing this problem, the Florida Supreme Court recently ordered a moratorium on the digitization of Florida's public records. Jason Krause, *Too Much Information? County Clerks Tussle with Nervous State Officials Over Posting Court Records Online*, A.B.A. J., April 2004, at 24.

[54] 5 U.S.C. § 552a(m).

[55] *See* Hoofnagle, *supra* note 16, at 623 ("[A] database of information that originates at a CDB would not trigger the requirements of the Privacy Act [, thus allowing CDBs] to amass huge databases that the government is legally prohibited from creating.").

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

[57] *Miller*, 425 U.S. at 443.

[58] *Cf.* Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001) ("The reasonable

on government accessing of privately-held records, they are extremely weak.

Medical records receive the most protection. Even here, however, neither probable cause or reasonable suspicion is required. Rather, pursuant to rules promulgated under the Health Insurance Portability and Accountability Act (HIPAA), the government can obtain medical records from HMOs and hospitals with a simple subpoena. A subpoena, it will be recalled, merely requires a finding that the information sought is relevant to a law enforcement investigation (although the target is entitled to notice and thus has the opportunity to challenge the subpoena on relevance or privilege grounds).[59] Given the limited scope of the Privacy Act described above, even that obstacle is removed if, as is true in some states, medical and similar information is maintained as a "public record" and the government receives it through a commercial data broker.

Financial records receive similarly minimal protection. To get detailed information from credit agencies, a regular subpoena is required under the Fair Credit Reporting Act.[60]

---

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."); Jaffee v. Redmond, 518 U.S. 1, 15 (1996) ("Because we agree with the judgment of the state legislatures and the Advisory Committee that a psychotherapist-patient privilege will serve a public good transcending the normally predominant principle of utilizing all rational means for ascertaining truth, . . . we hold that confidential communications between a licensed psychotherapist and her patients in the course of diagnosis or treatment are protected from compelled disclosure under Rule 501 of the Federal Rules of Evidence."); Whalen v. Roe, 429 U.S. 589, 605 (1977) (recognizing, in the context of a case involving disclosure of medical information, that a "statutory or regulatory duty to avoid unwarranted disclosures . . . in some circumstances . . . arguably has its roots in the Constitution").

[59] 45 C.F.R. § 164.512(f)(1)(ii)(B) (2005) (disclosure of medical records under HIPAA is permissible without permission of their subject if information is sought for law enforcement purposes through a grand jury subpoena). Some courts have required a greater showing to obtain medical records. *See, e.g.*, Doe v. Broderick, 225 F.3d 440, 450-51 (4th Cir. 2000) (finding *Miller* inapplicable to medical records); Haw. Psychiatric Soc., Dist. Branch of American Psychiatric Ass'n v. Ariyoshi, 481 F. Supp. 1028 (D. Haw. 1979); King v. State, 535 S.E.2d 432, 495 (Ga. 2000); Thurman v. State, 861 S.W.2d 96, 98 (Tex. Ct. App. 1993).

[60] 15 U.S.C. § 1681b(a)(1). Name, addresses, and places of employment can be

However, analogous to the situation with medical records, no law governs government requests for similar information from database companies and other companies that have obtained it from credit agencies.[61] As a result, the government routinely gets the financial information it wants directly from a commercial data broker, without bothering with a subpoena.[62] Bank records are also easily accessible. The Right to Financial Privacy Act generally requires only a traditional subpoena to obtain financial records from a bank. It also recognizes a significant variation to the traditional subpoena process: notification of the seizure may be delayed for up to 90 days if there is concern that service of the subpoena will tip off a suspect, result in loss of evidence, endanger witnesses or in some other way compromise the government's investigation.[63] In these circumstances, in contrast to the typical subpoena process, the target of a financial investigation will not find out that the government has the information until well *after* it is obtained. I will call this type of authorization a *delayed-notice subpoena.*

Outside of situations covered by the Right to Financial Privacy Act and the Internal Revenue Code, a government agency that is authorized to use administrative subpoenas to obtain financial and business information from third party entities need not give *any* notice to the customer whose records are sought.[64] This practice recognizes still another sub-

---

obtained simply upon a request. *Id.* § 1681f.

[61] Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1146 (2002).

[62] Chris Hoofnagle has made the argument that this ability to obtain information through a private agency circumvents the Privacy Act, which prohibits government from collecting such information unless there is a specific need for it. Hoofnagle, *supra* note 16, at 18.

[63] 12 U.S.C. § 3409. Furthermore, when subpoena power is not available to the government, it need only submit a formal written request for the information, a process this article calls extrajudicial certification. § 3408. Indeed, apparently banks sometimes still simply hand over information upon request. *See* DAVID F. LINOWES, PRIVACY IN AMERICA: IS YOUR PRIVATE LIFE IN THE PUBLIC EYE? 106-108 (1989) (describing a number of cases in which banks surrendered account information to law enforcement officers simply upon request and describing a survey finding that seventy-four percent of banks did not inform their customers of their routine disclosures to law enforcement).

[64] ELLEN S. PODGOR & JERRY H. ISRAEL, WHITE COLLAR CRIME IN A NUT-

poena mutation, which I will call an *ex parte subpoena*. This label is meant to distinguish between third party subpoenas that allow the target to contest the demand for production and those that don't. The term "ex parte subpoena" emphasizes that the customer is outside the process entirely, thus removing, in most cases, the only meaningful inhibition on fishing expedition-by-subpoena.

Transaction surveillance of communications-related information is regulated in a similarly weak fashion. Under ECPA, real-time interception of the content of phone and email communications requires a warrant based on probable cause.[65] But if email has sat on a server for longer than 180 days without being opened, or the recipient of email or voicemail accesses it and stores it on an outside server for any length of time, then a subpoena–delayed if necessary–is all that is needed to obtain the content of the communication.[66] Apparently, the rationale behind permitting easy access to unopened mail that is stored for 180 days is that it is, in effect, abandoned.[67] The rationale for permitting access on less than probable cause to opened email and other communications stored by a third party is that it becomes akin to a business record.[68]

SHELL 269 (2004).

[65] 18 U.S.C. § 2518(3) (2000).

[66] 18 U.S.C. § 2703(a) (2000); 2703(b)(1)(B). Further, a subpoena is only required when the information is sought from a "remote computer service" (e.g., a service available to the general public, like AOL). If the information is stored with a service not available to the general public (e.g., one run by an employer), then ECPA does not apply *at all* and government may obtain the stored information (content or identifying) simply upon a request. *See* 18 U.S.C. § 2703(a)(1-3); *see also* 18 U.S.C. § 2711(2) (2000) (defining remote computing service); U.S. Dep't of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations 89 (July 2002), *available at* http://www.cybercrime.gov/s&s manual2002.htm.

[67] *See* Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1421 (2004). This article is an extremely helpful roadmap and analysis of ECPA which, unfortunately, I discovered only after wading through the statute myself. *Id.*

[68] *See* CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING AND EAVESDROPPING § 26:9 (2d ed. 1995) (explaining that Congress felt that when an e-mail stays on a server longer than 180 days the service provider is less like a Post Office and more like a storage facility).

ECPA also gives the government easy access to business records held by phone companies and Internet service providers. Under Title II of ECPA, as amended by the Patriot Act of 2001, basic subscriber information–name, address, session times and durations, length and type of service, means and source of payment (including credit card numbers), and the identity of Internet users who use a pseudonym–can be obtained pursuant to an ex parte subpoena, the type of authorization that requires no customer notice.[69] If the government seeks additional transactional information–such as account logs and email addresses of other individuals with whom the account holder has corresponded–it still need not alert the subscriber, but must allege "specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation."[70]

Apparently, this latter standard, found in § 2703(d) of ECPA, is meant to be more demanding than the relevance standard normally required for a subpoena. Yet it is not clear that it is much different. Although the "specific and articulable" language sounds like it requires reasonable suspicion, note that the specific and articulable facts need only support a finding that the information is *relevant* and *material* to an ongoing investigation. Even if the latter highlighted word is meant to augment the former, it does not add much; materiality, in evidence law, merely means that the evidence be logically related to a proposition in the case.[71] Further-

---

[69] 18 U.S.C. § 2703(c)(1)(E) (2001) (describing information that can be obtained); § 2703(c)(3) ("A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.").

[70] § 2703(c) (describing requirements for a court order to obtain "[r]ecords concerning electronic communication service or remote computing service").

[71] MCCORMICK ON EVIDENCE § 185 at 276-78 (John W. Strong ed., 5th ed. 1999) ("Materiality . . . looks to the relation between the propositions that the evidence is offered . . . and the issues in the case. . . . A fact that is 'of consequence' is material . . . . It is enough if the item could reasonably show that a fact is slightly more probable than it would appear without that evidence.").

more, whereas *Terry* contemplated that reasonable suspicion exist with respect to the targeted individual, a § 2703(d) order, like a subpoena, allows accessing *any* records that might be relevant to an investigation, not just the target's. Finally, it is not clear that the "relevant and material" language can be meaningfully enforced. The statute seems to say that the only ground on which an order issued pursuant to § 2703(d) may be challenged is burdensomeness, which eliminates a challenge on relevance grounds.[72]

Post-9/11, government access to some sorts of privately-held records is even easier when a significant purpose of the investigation is to nab terrorists or spies. In such cases, Section 215 of the Patriot Act authorizes the FBI to demand the production of "any tangible things (including books, records, papers, documents and other items)" if it follows a simple two-step process.[73] First, the Director or his or her designee must certify to a court that the items sought are "for an investigation to protect against international terrorism or clandestine intelligence activities," and that the investigation does not focus "solely" on activities protected by the First Amendment.[74] Second, the court must find that the investigation meets these conditions; if so, it "shall" issue a Section 215 order authorizing the seizure.[75] In other words, a variant of the certification order discussed in connection with use of pen

---

[72] § 2703(d) (providing court may quash or modify order if the request is "unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider").

[73] 50 U.S.C. § 1861 (2001).

[74] § 1861(a) & (b).

[75] § 1861(c). This provision also indicates that the judge may modify the government's order. Apparently, the modification power is meant to protect against First Amendment and overbreadth concerns. But, assuming no such concerns, the judge must issue the order when the tangible items sought are "for an authorized investigation . . . to obtain foreign intelligence information." § 1861(b). *Cf.* Paul Rosenzweig, *Civil Liberty and the Response to Terrorism*, 42 DUQ. L. REV. 663, 694-95 (2004) (arguing that the provision for judicial modification, together with the requirements that the government swear the certification is correct and that the Attorney General report to Congress on the use of Section 215, provide more safeguards than those associated with a subpoena reviewable only after challenge).

registers and trap and trace devices will suffice in this situation. In an additional twist, however, not only is the target unable to challenge such orders, but the third party record-holder is *prohibited* from telling the target the order has been issued.[76] In counter-terrorist investigations, this procedure is all that is required to obtain customer records of Internet service providers, libraries, video stores, schools and other private entities (including, possibly, medical providers). Further, the records that may be obtained in this way are not just those of suspected terrorists, but those of anyone who might be "relevant" to the investigation.[77]

Finally, even a Section 215 order is not needed when the FBI is seeking a particular subset of "tangible items" (electronic or communication records, financial records or credit records) in connection with a national security investigation. Rather, all it must do is issue a form of administrative subpoena, known as a "National Security Letter," in which a Special Agent (in other words, a field agent) certifies that the information sought is relevant to a national security investigation to protect against international terrorism or clandestine intelligence activities.[78] This type of authorization is akin to the extrajudicial certification discussed in connection with law enforcement efforts to seek public documents under the Privacy Act, but with the same gag order proviso that exists with Section 215 orders.[79]

The Patriot Act allowed this extrajudicial process with respect to financial information only when it was held by banks. However, in December, 2003, that power was expanded by the Intelligence Authorization Act of 2003, which was en-

---

[76] 18 U.S.C. § 2709(c) (2001); 50 U.S.C. § 1861(d).

[77] Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1331-33 (2004); *see also* 18 U.S.C. § 2709(b) (wire or electronic service providers); 20 U.S.C. § 1232g(j)(A) (school records); Kathryn Martin, *The USA Patriot Act's Application to Library Patrons Records*, 29 J. LEGIS. 283 (2003) (discussing library records).

[78] 12 U.S.C. § 3414(a)(5)(A) (2003). Again, the record-holder is prohibited from informing the target of the request. § 3414(a)(5)(D).

[79] Swire, *supra* 77, at 1332-33.

acted by Congress as part of an appropriations bill, with no vetting by the Judiciary Committee and no debate on the floor or in the media.[80] The 2003 Act allows the FBI to use extra-judicial certification to obtain statements and records from *any* financial institution "whose cash transactions have a high degree of usefulness in criminal, tax or regulatory matters," including banks, stockbrokers, car dealers, casinos, credit card companies, insurance agencies, jewelers, pawn brokers, travel agents and airlines.[81] All of this information is the government's simply on its sayso.[82]

D. Summary of Transaction Surveillance Law

Transaction surveillance has spawned a wide array of new regulatory schemes, which are usefully summarized by locating them within the standard Fourth Amendment hierarchy. As noted earlier, the most protective type of authorization is the warrant, based on probable cause. Although intercepting the content of communications and physical surveillance of the home both require a warrant,[83] no type of transaction surveillance requires this most demanding form of authorization. The next type of authorization in the hierarchy, at least in theory, is an order based on reasonable suspicion, or what could be

---

[80] Kyle O'Dowd, *Congress Hands FBI "Patriot II" Snooping Power*, 28 Feb. CHAMP. 18 (2004)

[81] 31 U.S.C. § 5312 (1996).

[82] The Patriot Act's National Security Letter (NSL) provision was declared unconstitutional in *Doe v. Ashcroft*, 334 F. Supp. 2d 471 (2004), because of the lack of judicial review and the gag provision. However, the decision did not find fault with either the relevance standard or the fact that letters can be issued by a special agent. Indeed, the court stated "the standard of review for administrative subpoenas similar to NSLs is so minimal that most such NSLs would likely be upheld in court." *Id.* at 502. Recent proposed amendments at most are likely to codify *Doe*. Eric Lichtblau, *Congress Nears Deal to Renew Antiterror Law*, N.Y. TIMES, Nov. 17, 2005, at A1, A21. In the meantime, the FBI issues roughly 30,000 NSLs a year, maintains all the records thereby obtained (even when not linked to terrorism), and as of this writing had still not responded to a year-old congressional request for information about their use. Barton Gellman, *The FBI's Secret Scrutiny*, WASH. POST (Nov. 6, 2005), at A1.

[83] *See supra* note 5.

called a *Terry* order, after *Terry v. Ohio*,[84] which required this degree of justification for a stop and frisk. Again, none of the statutory provisions I have described (or any other regulatory regime for that matter) mandates this type of order; I include it both for the sake of comprehensiveness and because it is important to the regulatory scheme I propose below. After a *Terry* order comes the traditional subpoena, issued upon a judicial finding of relevance and challengeable by the target. This is the first type of authorization that plays a role in transaction surveillance; subpoenas are required to access most medical, financial and stored email records.

Below the traditional subpoena is the delayed-notice subpoena, which authorizes, temporarily, unobstructed access to financial records and stored email when a traditional subpoena might frustrate the investigation. Next is the ex parte subpoena (unchallengeable by the target), which allows access to many types of customer records held by third party entities, including phone and ISP account records.[85] The certification (judicial rubberstamp) order follows in the hierarchy; it authorizes the use of pen registers, trap and trace devices and other forms of transaction-oriented snoopware, as well as tangible items other than financial records thought to be relevant to national security investigations.[86] At the bottom of the authorization totem pole there is the extrajudicial certification, which permits access to public records, and to financial and other records relevant to national security investigations. However, even this type of authorization is not needed to

---

[84] 392 U.S. 1 (1968).

[85] Arguably, the "specific and articulable facts" ex parte subpoena required by 18 U.S.C. § 2703(d) is more difficult to obtain than an ordinary subpoena (and apparently Congress so believed), but for the reasons suggested above, *see supra* notes 69-72 and accompanying text, it is classified here as less protective than a regular subpoena, at least one that notifies the target.

[86] People who have worked at the Department of Justice state that, in practice, a certification order may be harder to obtain than a subpoena. Personal conversations with Orin Kerr (Feb. 17, 2005) and Paul Ohm (Jan. 20, 2005). But I rank the certification order lower in the hierarchy of protection because the judge plays such a minimal role; at least with a subpoena the judge is permitted to find a seizure invalid on relevance grounds, although he may rarely do so.

access public records that come from a state with no privacy statute or that are accumulated by a commercial data broker. All of the authorization mechanisms described in this paragraph are statutory inventions, and are particularly punchless given the lack of a remedy in the unlikely event government is found to have abused them.[87]

The chart below depicts the foregoing summary, consisting of eight levels of authorization:

CURRENT LAW OF TRANSACTION SURVEILLANCE

Transaction	Auth'zation Req'd	Certainty Level
———	Warrant	Probable cause
———	*Terry* Order	Reasonable suspicion
Medical, financial & tax records; stored email	Subpoena	Relevance, challengeable by target
Financial records and stored email if notification poses risks	Delayed-notice Subpoena	Relevance, challengeable by target only after records obtained
Billing records and logs of phone companies & ISPs; most customer records	Ex Parte Subpoena	Relevance, challengeable only by third party record-holder
Interception of catalogic information re calls & email; tangible items re terrorism	Certification Order	Relevance (determined by government), issued by court, challengeable only by third party record-holder

[87] For instance, there is no exclusionary sanction under ECPA, or under the Right to Financial Privacy Act. WHITEBREAD & SLOBOGIN, *supra* note 9, at 344-45; United States v. Kington, 801 F.2d 733, 734 (5th Cir. 1986). Nor are damages actions a significant deterrent, given the intangible nature of the harm involved. *Cf.* Doe v. Chao, 306 F.3d 170, 177 (4th Cir. 2002) (holding that, under ECPA, "a person must sustain actual damages to be entitled to the statutory minimum damages award" of $1,000).

Federal public records; financial records re terrorism	Extrajudicial Certification	Relevance (determined by government), not challengeable by any party(?)[88]
State public records not protected by law or that are acquired by a CDB	None	None

III. A PROPOSAL FOR REGULATION OF TRANSACTION SURVEILLANCE

The differences between the various types of authorization outlined above are sometimes subtle, but one thing is certain: their number goes well beyond (and below) the traditional three-tiered approach of probable cause, reasonable suspicion, and special needs/reasonableness determinations, all challengeable by the target of the investigation. As a conceptual matter, a system that recognizes more than three authorization levels may make sense. In previous work, for instance, I have argued for application of a proportionality principle, which specifically requires that the certainty required for a search be roughly proportionate to its intrusiveness, and which suggests that the traditional probable cause/reasonable suspicion dichotomy is insufficient as a means of implementing that idea.[89] My disagreement with current law is not with the general approach, but with the order and substance of the hierarchy.

The degree to which transaction surveillance is regulated should not depend on whether the information sought is intercepted in real-time or is stored, or on whether it may be related to terrorist actions or some other crime. Rather, the key variables should be the type of information sought and the

[88] *See supra* note 82 and accompanying text.

[89] Christopher Slobogin, *Let's Not Bury* Terry*: A Call for Rejuvenation of the Proportionality Principle*, 72 ST. JOHN'S L. REV. 1053, 1081-82 (1998); Christopher Slobogin, *The World Without A Fourth Amendment*, 39 UCLA L. REV. 1, 68-75 (1991).

type of transaction surveillance (target-based or event-based) that is at issue. I propose recognizing three types of distinctions based on the type of records sought: (1) the content of personal records would be entitled to more protection than the content of organizational records; (2) the content of personal records held by private entities would be entitled to more protection than the content of personal records held by public entities for public consumption; and (3) the content of records, regardless of their subject or who holds them, would presumptively be entitled to more protection than records memorializing what I call "catalogic data" (information that simply identifies the nature of a communication or links a person to an activity). With catalogic data, however, the second variable mentioned above–the government's motivation in carrying out the surveillance–is also important. If the information is sought in connection with target-based, as opposed to event-based, surveillance it should receive heightened protection.

More specifically, I propose that government should have to obtain: (1) a warrant based on probable cause when it seeks the content of personal records, or seeks catalogic data in connection with target-based surveillance; (2) a *Terry* order based on reasonable suspicion when it seeks the content of records that are "public" in nature; (3) a traditional subpoena based on relevance–or when there is concern about tipping off a suspect, a delayed-notice subpoena based on relevance[90]–to access the content of organizational records and to access catalogic data in connection with event-based transaction surveillance. Ex parte subpoenas, certification orders and extrajudicial certifications should *never* be sufficient authority to carry out nonconsensual searches and seizures for personal

[90] Orin Kerr notes that, given the ease with which subpoena-service delays can be obtained, the government can use subpoenas "without meaningful notice." Orin S. Kerr, Symposium, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1234 (2004). He also argues that the ninety-day delay period "serves no legitimate purpose," and instead proposes a thirty-day delay, permitted only upon judicial authorization, with (rare) further extensions only after further judicial review. *Id.* at 1235. This regime seems sensible.

transaction information, except in emergencies, and then only if quickly subject to judicial review. The following chart represents my proposal:

PROPOSED LAW OF TRANSACTION SURVEILLANCE

Transaction	Auth'zation Req'd	Certainty Level
Content of privately-held personal records	Warrant	Probable Cause
Content of publicly-held personal records	*Terry* Order	Reasonable Suspicion
Content of organizational records	Subpoena	Relevance
Catalogic Data		
Target-based surveillance	Warrant	Probable Cause
Event-based surveillance	Subpoena	Relevance

Under this scheme, again, the contents of "personal" records are distinguished from the contents of "impersonal," organizational records, with acquisition of the former requiring something more than mere relevance. Within the "personal" record category, "privately-held" records are distinguished from "publicly-held" records, with acquisition of the former requiring probable cause and of the latter reasonable suspicion. Finally, "content" is distinguished from "catalogic data" that simply describes the nature of a transaction, with the authorization level for the latter dependent on whether it is sought in connection with event-based surveillance of the type involved in data mining and profiling, where only relevance is required, or target-based surveillance which requires probable cause. The reasoning behind these proposals, and definitions of the key terms, follow, beginning with the all-important distinction between organizational and personal transactions.

A. Organizational v. Personal Content

In a previous article, *Subpoenas and Privacy*, I canvassed several possible justifications for the current relaxed state of transaction surveillance regulation.[91] Although I discussed six such justifications, they all fit within one of two categories: they either minimize privacy concerns associated with transactional information or rest on an assertion that law enforcement could not function if transaction surveillance were subject to significant regulation. I also concluded that these rationales are not unpersuasive in the context in which subpoenas first flourished–government efforts to obtain documentary evidence of crimes committed by or within a business or other regulated organization. As the Supreme Court has recognized on numerous occasions, records of businesses and similar entities are associated with a minimal degree of privacy, given their impersonal nature and the high degree of state regulation to which organizations are subject.[92] The Court has also pointed out in several cases that investigation of economic crimes and regulatory violations would be extremely difficult without ready access to documents detailing business activity.[93] But my previous analysis also concluded that neither the diminished-privacy rationale or the heightened-need justification applies when the records sought are personal.

The diminished-privacy rationale, as applied to personal

---

[91] Christopher Slobogin, *Subpoenas and Privacy*, 34 DEPAUL L. REV. 805 (2005).

[92] In *Hale v. Henkel*, 201 U.S. 43 (1906), the leading Supreme Court case on grand jury document subpoenas, the Court stated that while a corporation "is a creature of the state . . . [it] is presumed to be incorporated for the benefit of the public [and] "receives certain special privileges and franchises, and holds them subject to the laws of the state and the limitations of its charter," while an individual "owes no such duty to the state, since he receives nothing therefrom, beyond the protection of his life and property." *Id.* at 74. In *United States v. Morton Salt Co.*, 338 U.S. 632 (1950), one of the Court' leading administrative subpoena cases, it was even more forthright: "[C]orporations can claim no equality with individuals in the enjoyment of a right to privacy." *Id.* at 652.

[93] *See, e.g.*, United States v. White, 322 U.S. 694, 700 (1944) ("The scope and nature of the economic activities of incorporated and unincorporated organizations and their representatives demand that the constitutional power of the federal and state governments to regulate those activities be correspondingly effective.").

records, is both descriptively and normatively flawed. When such records are retained by the individual, they are thought to be, and ought to be, as private as anything else in one's home. Even when maintained by a third party, records about an individual are, and should be, considered similarly private if, as is usually the case, the transfer or collection of the information occurred because the third party *requires* it in order to carry out an important societal service. Hospitals, banks, Internet service providers and public agencies usually only have personal data because we must provide it (or allow it to be accumulated) in order to receive the services these entities provide. Stated another way, most third party record-holders possess information about us because we cannot otherwise realistically function in the modern world. Thus, contrary to the Supreme Court's assertion in *Miller*, the surrender of personal information to these third parties is hardly "voluntary." Nor does it, or should it, lead us to "assume" that the third party will function as an institutional undercover agent, a conduit for any information the government wants.[94]

The argument that more rigorous regulation of transaction surveillance would unduly hinder the government's law enforcement efforts is also weak when applied to personal records. There is no doubt that requiring probable cause to obtain records will make investigation of crime more difficult. But to convert that fact into a rationale for removing restrictions on government evidence-gathering makes a mockery of constitutional protections, for the warrant and probable cause requirements always have that effect. In this context as well,

---

[94] Empirical research confirms that most people view a search of records containing their personal information to be at least as intrusive as a search of a car or luggage. *See* Christopher Slobogin & Joseph Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society"*, 42 DUKE L.J. 727, 738-39 (1993) (Table 1) (finding that a sample of 217 individuals, on average, ranked "perusing bank records" as more "intrusive" than searches of the trunk of a car and a footlocker in a car); *see also* Lior Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919 (2005) (arguing that, under social networks theory, information revealed to small social groups should generally be considered private unless the target's actions or status removes it from obscurity).

a viable distinction exists between investigations of organizational activity and investigation of street crime and the like. Evidence of organizational crime, particularly of the economic variety, is largely if not entirely documentary; indeed, without such evidence even the victims of such crime may not realize it has occurred. But the same is seldom true of other types of crime. Whereas "it is a fact of life that agencies charged with regulating economic activity often cannot articulate probable cause or even reasonable suspicion that a violation has transpired without first examining documents reflecting a party's economic activity,"[95] police engaged in investigating other types of criminal activity usually can develop some non-documentary lead, whether it is from the victim, a third party eyewitness, or physical surveillance of public movements.[96]

If one accepts these arguments, then it is important to separate personal from organizational documents. Fortunately, as I explained in *Subpoenas and Privacy*,[97] the Supreme Court has already done much work in this regard, in the course of defining the concept of a "collective" entity and the notion of "required records" for purposes of determining when there is a Fifth Amendment right to resist documentary subpoenas. Although the Court's reconceptualization of the Fifth Amendment in the mid-1970s has rendered these cases largely irrelevant for Fifth Amendment purposes,[98] they are directly

---

[95] Parks v. FDIC, 65 F.3d 207, *11 (1st Cir. 1995), *withdrawn* 64 USLW 2166 (Selya, J., dissenting).

[96] SARA SUN BEALE ET AL., 1 GRAND JURY LAW & PRACTICE 6-3 (2d ed. 2002) ("Ordinarily, investigations of so-called 'street crimes' such as murder, rape, robbery, and assault, can be conducted effectively without resort to the subpoena power."); KENNETH MANN, DEFENDING WHITE COLLAR CRIME: A PORTRAIT OF ATTORNEYS AT WORK 233-34 (1985) (noting that the easiest crimes to hide are those where the victim does not realize he or she has been victimized, those where the location of the crime is "not apparent"–making witnesses hard to identify–and those where the "inculpatory information is embedded in normal social life," all factors much more likely to be associated with organizational rather than individual crime).

[97] Slobogin, *supra* note 91.

[98] The crucial decision was *Fisher v. United States*, 425 U.S. 391 (1976), which decisively moved the Court's Fifth Amendment jurisprudence from a focus on privacy to a focus on coercion. There the Court held that because a document

pertinent to the current task of identifying which types of records are associated with minimal privacy. That is because these cases explicitly tried to demarcate when records are entitled to what the Court eventually called "a zone of privacy."[99] In essence, in its collective entity cases the Court concluded that the records of any organization that has an identity separate from its individual members lie outside that zone.[100] In its required records cases, the Court similarly held that the government may force individuals to keep and disclose documents that are crucial for regulating their activities and "have assumed 'public aspects' which render [the records] at least analogous to public documents."[101] Consistent with these two lines of cases, records that pertain to a collective entity or that fit the required-records criteria ought to be accessible on mere issuance of a subpoena.

Other records, however, should receive more protection. The Fourth Amendment specifically speaks of searches of papers, as well as searches of persons, houses, and effects, and it usually requires probable cause for these searches. Accordingly, subpoenas demanding the contents of personal records should generally be invalid under the Fourth Amendment unless they are based on such a showing. The rest of this section discusses whether there should be any other exceptions to this rule outside of the organizational investigation setting.

---

subpoena does not compel the creation of documents, it only implicates the Fifth Amendment when the act of production it compels provides the prosecution with useful incriminating information. *See also* Andresen v. Maryland, 427 U.S. 463 (1976) (holding that a search warrant compels neither the creation *or* production of documents).

[99] Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

[100] *See* Bellis v. United States, 417 U.S. 85, 92, 94-95 (1974) (holding that even though a small law firm "embodies little more than the personal legal practice of the individual partners," it is a "formal institutional arrangement organized for the continuing conduct of the firm's legal practice," and thus was "an independent entity apart from its individual members").

[101] *See* Grosso v. United States, 390 U.S. 62, 67-68 (1968) (describing the components of the required records doctrine established in *Shapiro v. United States*, 335 U.S. 1 (1948)).

B. Private v. Public Records

One distinction regarding personal records that could be made is between those records that are "private" and those that are in the public domain. As the required-records line of cases suggests, when the records fit in the latter category, the privacy associated with their content is considerably diminished. With truly public records, the information can no longer be said to be "owned" solely by the individual and the record-holder. In that instance, reasonable suspicion–the justification level that falls between probable cause and relevance–ought to be sufficient justification for permitting government access.

Public records and records held by a public entity are not synonymous however. The word "public" can apply to functionally "private" institutions such as hospitals, schools and libraries, as well as to courthouses and government agencies. And even government agencies can house records that are more personal than public.[102]

How can we determine when public records are not really public and therefore deserving of full Fourth Amendment protection? Once again, statutory law and litigation in other contexts have already ploughed this ground. In particular, provisions in the federal Freedom of Information Act and similar state statutes are directly on point. While these laws establish a presumption in favor of disclosure of records held by government agencies, primarily as a means of increasing government transparency and facilitating social transactions such as business deals,[103] they usually exempt from disclosure a wide array of "personal" records. Thus, under the federal statute, government agencies must resist a FOIA request for "commercial or financial information obtained from a person and privileged or confidential,"[104] "personnel and medical

---

[102] *See* DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 127 (2002) (describing "a system where the government extracts personal information from the populace and places it in the public domain").

[103] *Id.* at 140.

[104] 5 U.S.C. 552(b)(4). Many circuits have held that voluntarily submitted infor-

files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy,"[105] and law enforcement records to the extent they include information that "could reasonably be expected to constitute an unwarranted invasion of personal privacy."[106] State FOIA statutes or interpretive caselaw protect various other types of records. For instance, Florida, which is known as the Sunshine State not only because of its weather but also because of the breadth of its public records disclosure law, nonetheless exempts from unrestricted disclosure some types of motor vehicle registration information,[107] identifying information relating to health care provided by the state,[108] credit information held by state agencies,[109] and educational records.[110] In many states, some types of licensing information are also exempt from disclosure.[111]

---

mation will be deemed "confidential" for the purpose of this exemption if it is of a kind that would customarily not be released to the public by the person from whom it has obtained records. *See, e.g.,* Critical Mass Energy Project v. Nuclear Regulatory Comm'n, 975 F2d 871, 872 (D.C. Cir. 1992), *cert. denied*, 507 U.S. 984 (1992). *See generally What Constitutes "Trade Secrets and Commercial or Financial Information Obtained from Person and Privileged or Confidential," Exempt from Disclosure under Freedom of Information Act (5 U.S.C.A. § 552(b)(4)) (FOIA)*, 139 A.L.R. FED. 225 (2004).

[105] *Id.* § 552(b)(6). The Supreme Court has defined "similar files" broadly, to include "detailed Government records on an individual which can be identified as applying to that individual," U.S. Dep't of State v. Washington Post Co., 456 U.S. 595, 602 (1982), although it has also made clear that such files cannot be withheld simply because such identification cannot be guaranteed, and that redaction of identifying names may be sufficient. Department of Air Force v. Rose, 425 U.S. 352, 381-82 (1976). *See generally* Annotation, *When Are Government Records "Similar Files" Exempt from Disclosure under Freedom of Information Act Provision (5 U.S.C.A. § 552(b)(6)) Exempting, Certain Personnel, Medical, and "Similar" Files*, 106 A.L.R. FED. 94 (2004).

[106] *Id.* at 552(b)(7)(c). Thus, for instance, a person's rap sheet may be exempt from disclosure. See U.S. Dep't of Justice v. Reporter's Comm. for Freedom of Press, 489 U.S. 749, 774 (1989). *See generally* James O. Pearson, Annotation, *What Constitutes "Unwarranted Invasion of Personal Privacy" for Purposes of Law Enforcement Investigatory Records Exemption of Freedom of Information Act (5 U.S.C.A. sec. 552(b)(7)(C))*, 52 A.L.R. FED. 181 (2004).

[107] FLA. STAT. § 119.07(aa).

[108] *Id.* at (bb), (cc), & (hh).

[109] *Id.* at (dd).

[110] FLA. STAT. § 1002.22(d).

[111] *See, e.g.,* Mager v. State Dep't of Police, 595 N.W.2d 142, 143 (1999) (hold-

When federal or state law indicates that information found in government records should be withheld despite the strong interest in freedom of information, it ought to be considered private for Fourth Amendment purposes as well. That should mean that law enforcement must demonstrate probable cause to obtain it. For other records held by public entities, reasonable suspicion is sufficient.

Recall, however, that even this latter level of justification demands more than the current legal regime, which usually does not even require a subpoena in such situations, but rather permits law enforcement access to public records with a simple extrajudicial certification. A curious law enforcement officer should not be able to sift through the personal data found in divorce papers, real estate documents and court proceedings without articulating a specific need for it. That articulation should take place beforehand to a judge or, in the manner typical of a subpoena, after notification and challenge.[112]

A common complaint about such an approach is that it places more limits on government officials than on members of the public, who can access public records at will and, with the advent of Google and other Internet search services, can do so more easily than ever before. But most of the time the public only seeks public information when it has a specific need for it (akin to the reasonable suspicion standard).[113] More importantly, government's resources and power are so much more significant, and its hunger for information so much more voracious, especially post-9/11, that its potential for abusing per-

---

ing that "gun ownership is information of a personal nature'" requiring exemption from the state freedom of information act); *see also* OR. REV. STAT. § 656.702(1) ("[t]he records of the State Accident Insurance Fund Corporation, *excepting employer account records and claimant files*, shall be open to public inspection.") (emphasis added).

[112] Note that this procedure is no more onerous, from the law officer's perspective, than the current pen register regime. *See supra* notes 43-47 and accompanying text.

[113] Noah Rothbaum, *Spies Like Us*, SMART MONEY (Feb. 2005) at 89-92 (describing the various ways people might and do use new search engines, including investigating job applicants and real estate for sale).

sonal information far exceeds anything individuals or even corporations might do.[114]

C. Catalogic Data

By "catalogic data" I mean information that classifies and describes a transaction, as distinguished from the content of the transaction. Catalogic data includes descriptors of communications and transmissions, such as phone numbers dialed, the addresses that route emails, and the duration of phone calls and Internet session times. This category of transactional information also includes membership lists; plane, train and ship passenger manifests; business records listing who purchased what and when; and other archives that describe the identities of those who have participated in a particular activity or communication.

This listing overlaps with some of the information that ECPA permits the government to obtain with an ex parte subpoena or a certification order. However, I would not include within the rubric of catalogic data other types of personal information ECPA currently allows government to obtain with an ex parte subpoena, such as the URLs of websites visited or the identity of those using pseudonyms.[115] This kind of information is more akin to content: the URLs can be used to visit the same websites the target visits, and disclosure of the person behind the pseudonym will often allow government to link that person to particular messages.[116]

So limited, catalogic data should not be entitled to as

---

[114] *See infra* notes 142-46 and accompanying text (describing concerns about government's ability to obtain and abuse information); *see also* SOLOVE, *supra* note 102, at 168-75 (describing current government efforts to obtain information about millions of citizens and concluding that "we are already closer to Total Information Awareness than we might think") & 175-87 (describing possible abuses of information-gathering, including "creeping totalitarianism," inhibition of freedom of association, and J. Edgar Hoover's misuse of surveillance against alleged communist party members and people like Martin Luther King).

[115] *See supra* notes 69-72 and accompanying text.

[116] *See generally* John Alan Farmer, Note, *The Specter of Crypto-Anarchy: Regulating Anonymity—Protecting Peer-to-Peer Networks*, 72 FORDHAM L. REV. 725 (2003).

much protection as the content of communications, because it is not as personal as the substance of communications made during the transaction. That is not to say, as the Supreme Court has said, that the Fourth Amendment is irrelevant when something other than content is at issue. *Smith v. Maryland* notwithstanding,[117] most of us would not expect the people who work at our phone company (or Internet service provider) to care who we call (or write to), an expectation that is undoubtedly correct.[118] But the evidence that catalogic data provides about content is, at best, circumstantial. Catalogic data is to the substance of the contact as the visage is to personality. Thus, while it is entitled to some protection, catalogic data should not be treated in the same way the associated content is.

The analysis changes, however, when the government uses technologically-enhanced transaction surveillance to *aggregate* catalogic data. When information from pen registers, snoopware programs, and commercial data broker programs is combined, it can identify all of our surreptitious connections with the world, providing powerful evidence of our activities and beliefs.[119] To use the words of the commentator quoted earlier, law enforcement can construct a "complete mosaic of a person's characteristics" through this type of transaction surveillance. Under these circumstances, the information the government accumulates is more akin to content than mere cataloguing. The visage analogy no longer applies.

This distinction between aggregated and isolated catalogic data roughly maps onto the distinction between target-based and event-based transaction surveillance described earlier.

---

[117] *See supra* notes 40-41 and accompanying text.

[118] *Cf.* Wayne LaFave, *The Forgotten Motto of Obsta Principis in Fourth Amendment Jurisprudence*, 28 ARIZ. L. REV. 291, 302 (1986) (bank officials do not have "direct, significant contact with the underlying transactional information" in the same way law enforcement officers who collect all of an individual's financial information would) (quoting Note, 83 YALE L.J. 1439, 1463-64 (1974)).

[119] *See generally* Stan Karas, *Privacy, Identity, Databases*, 52 AM. U. L. REV. 393, 398 (2002) ("What we buy is how we present ourselves to the outside world; it represents how we choose to interact with it . . . . These preferences are expressive, revealing and private.").

When government has identified a target, it will tend to accumulate as much information as possible about the target. Under such circumstances, the transaction surveillance will produce a personality "mosaic" that is deserving of maximum protection.

Event-based transaction surveillance of catalogic data is usually different. Recall the example given earlier of the sniper investigation in which police find a sweater thread and footprint they believe belong to the sniper, and also know that the sniper reads a particular type of detective novel. Law enforcement attempts to identify the sniper through accessing the records of local clothing, shoe and bookstores are likely to disclose the names of numerous innocent people who have purchased items similar to those thought to be owned by the criminal. But this information, while personal, is merely a piece of the mosaic, not nearly the complete picture that target-based surveillance is likely to produce. In this situation, a relevance showing should be enough, at least when the access does not infringe First Amendment interests.[120]

However, ex parte subpoenas, certification orders and extrajudicial certifications, which are the current means of regulating access to catalogic data when there is any regulation at all, are insufficiently restrictive despite their reliance on the relevance standard. These devices leave the transaction surveillance decision about personal data entirely or almost entirely in the discretion of law enforcement even when no exigent circumstances exist, a notion that is antithetical to the Fourth Amendment.[121] Instead, in non-emergency situations

---

[120] The Supreme Court has indicated that requiring an individual engaged in advocacy to surrender anonymity without good cause can infringe First Amendment interests. *See, e.g.*, NAACP v. Alabama *ex. rel.* Patterson, 357 U.S. 449, 462 (1958) ("It is hardly a novel perception that 'compelled disclosure of affiliation with groups engaged in advocacy may constitute [an] effective . . . restraint on freedom of association.'"); Shelton v. Tucker, 364 U.S. 479, 490 (1960) (prohibiting compelling teachers to disclose group memberships).

[121] As Justice Jackson stated in *Johnson v. United States*, 333 U.S. 10, 13-14 (1948):

> The point of the Fourth Amendment, which often is not grasped by zealous officers, is not that it denies law enforcement the support of the

the government should be able to obtain catalogic data in connection with event-based surveillance only when a judge finds it is relevant to an investigation, an assertion the record-holder should have the opportunity to challenge unless notification would undermine the investigation.

D. Data Mining / Profile Information

Data mining is event-based transaction surveillance–the use of records searches to discern patterns of behavior that can be linked to past or future crime, without having a specific individual or individuals in mind. Several formal data mining programs exist. For instance, the Homeland Security Department runs something called the Electronic Surveillance System for Early Notification of Community-Based Epidemics (ESSENCE), which gathers personally identifiable information from emergency rooms, health plans, clinical laboratories, 911 calls, pharmacies, and veterinary clinics in an effort to discern unusual or suspicious symptoms and events.[122] The Enhanced Border Security and Visa Entry Reform Act of 2002 requires aircrafts and sea vessels to submit departure and arrival manifests indicating the names of all alien passengers,

---

> usual inferences which reasonable men draw from evidence. Its protection consists in requiring that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime. . . . When the right of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer, not by a policeman or Government enforcement agent . . . .

Jackson then went on to list the "exceptional circumstances in which, on balancing the need for effective law enforcement against the right of privacy, it may be contended that a magistrate's warrant for search may be dispensed with: when a "suspect was fleeing or likely to take flight"; "[t]he search was of . . . a movable vehicle"; or "evidence or contraband was threatened with removal or destruction." *Id.* at 15.

[122] *See* Katherine McIntire Peters, *Pattern Recognition*, Sept. 19, 2003, *available at* http://www.govexec.com/features/0903/0903s2.htm (describing ESSENCE). ESSENCE is a much reduced version of the maligned Total Information Awareness program, now labeled Terrorism Information Program, that was restricted by Congress in 2002. 10 U.S.C. § 2241 (limiting scope and appropriations for total information awareness program).

which can be combed for suspicious travel patterns.[123] The much more sophisticated Computer Assisted Passenger Prescreening System (CAPPS) purportedly combines airline passenger lists with travel reservations, rental car status, travel companions, and address.[124] Data mining comes in many forms, but all varieties have one thing in common: they rely on dragnet perusal of transaction information.

One way of analyzing the Fourth Amendment implications of data mining would be to focus on the nature of the records that are mined. Under this approach, if ESSENCE accesses the contents of personally identified medical records for criminal investigation purposes, its algorithm ought to identify only people who are highly likely to be perpetrators of crime, while if all of its information comes from "public" records or is composed of isolated catalogic sources, then its ability to identify criminals need not be as potent. A second way of analyzing data mining would be to look at the extent to which it aggregates information about the individuals it investigates and tags. If one accepts the concern about creation of "personality mosaics" described earlier, data mining would need a high hit rate to the extent it accumulates a significant amount of identifiable data about individuals, even if, as with CAPPS, all of the information is catalogic in nature.

Either way, data mining does not fare well. From what we know, the profiles used in the programs are very unlikely to identify even a small number of terrorists or other criminals. In other words, they may not even be successful enough to pass the relevance test (which requires that the investigative technique do better than chance), much less reach a level of success commensurate with reasonable suspicion or probable cause. Perhaps if such a data mining program relied only on a small amount of catalogic data to identify potential targets, it

---

[123] 8 U.S.C. §1731(a)(2) (requiring the establishment of a database for all arrivals and departures).

[124] *See* Charu A. Chandrasekhar, *Flying While Brown: Federal Civil Rights Remedies to Post-9/11 Airline Racial Profiling of South Asians*, 10 ASIAN L.J. 215, 221 (2003) (describing a profile using roughly 40 items which, although secret, are likely to include those listed).

would be permissible under the interpretation of the Fourth Amendment put forward here.[125] But once government begins using multiple databases to put together detailed dossiers on the activities of its citizens, it would have to show more than just a possibility that something useful might turn up.

IV. COUNTER-PROPOSALS

What does this set of proposals mean for our detective friend, described in Part I of this article? If he is investigating a particular person (the frequent flyer, the free-spender or the young Arab man), he needs a *Terry* order to access public records through Choicepoint or one of the other commercial data brokers. And he needs a warrant based on probable cause to access the contents of the suspect's financial, school, medical and similar personal records, as well as to obtain aggregated catalogic information such as addresses of the person's email messages. If instead he is engaging in event-based investigation, the nature of the records sought determines the justification needed. If, as in the hypotheticals described in Part I, the focus is store records (in an effort to track down a sniper-killer), or skydiving club membership lists and cookies of websites (in an effort to identify terrorists planning to bomb a mall), he would be on solid ground if this catalogic data is likely to increase the probability of identifying the perpetrators. If instead access is sought to the content of personal records or to catalogic data that implicates First Amendment interests, individualized suspicion would be required.[126]

---

[125] A recently released report by a Department of Defense advisory committee requires court approval of data mining that will obtain "personally identifiable information" from records not readily available to the public. *See* Report of the Technology and Privacy Advisory Committee, Safeguarding Privacy in the Fight Against Terrorism 49, 51 (March 2004). However, it requires the court to find only that the information obtained be "reasonably related" to the investigation purpose–a relevance standard?–and does not otherwise distinguish between types of records. *Id.* at 51-52. The report makes several good suggestions regarding "anonymizing" data, record-keeping and other means of monitoring data mining. *Id.* at 48-59.

[126] The analysis should not change if government seeks personal information from records acquired by a commercial data broker that has obtained the infor-

While this set of rules is not uncomplicated, it recognizes fewer types of authorizations than the current regime. The officer need merely make distinctions between personal and public records when conducting target-based transaction surveillance, and between content and catalogic data when conducting event-base surveillance. Moreover, since transaction surveillance should generally only proceed pursuant to court order, any confusion on the detective's part can be cleared up by a judge.

One can imagine numerous alternative methods of regulating transaction surveillance. Professor Daniel Solove has put forth the most coherent alternative to current law and the proposal presented here.[127] He points out that technology has made it easier both to maintain information about people and to aggregate it.[128] Thus, he proposes that, rather than attempt to figure out a privacy hierarchy and match authorization requirements to it (the proportionality approach that informs this article), we should adopt a uniform regulatory regime for government access to any "system of records."[129] Specifically, Solove proposes that, outside of emergency situations, government should not be able to obtain information in records–whether it is content or catalogic data, whether it is held by private or public agencies–unless it can obtain what he calls a "regulated subpoena."[130] To obtain such a subpoena the government would have to demonstrate it has probable cause to believe the person whose records are sought is involved in criminal activity, and that the specific records targeted are of "material importance" to the investigation, which he describes as a standard that is "slightly more permissive

---

mation from the original record-holders. Otherwise, much of this regulation could be avoided. Data does not become less personal simply because it has been shifted from one entity to another. The crucial questions are whether it is content or catalogic/organizational information, and whether it was originally collected for private or public purposes.

[127] Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2002).

[128] *Id.* at 1090-95.

[129] *Id.* at 1152-59.

[130] *Id.* at 1164.

than that of a warrant," though more demanding than the relevance standard required for a subpoena (and, presumably, the reasonable suspicion required for a *Terry* order).[131] As with traditional subpoenas, the regulated subpoena would be challengeable by the target.[132]

Solove makes interesting arguments as to why his approach is superior to a proportionality approach. First, he points to the difficulty of differentiating between degrees of privacy and intimacy,[133] a difficulty illustrated by my attempts to distinguish content from catalogic information, personal from organizational records, and private from public records. Second, even if we could resolve these definitional problems, Solove believes that making privacy the linchpin of analysis is conceptually bankrupt. He notes, for instance, that we would never think of requiring the police to obtain a warrant in order to obtain a description of a suspect's genitals from his sexual partner, yet that information is probably as "private" as anything found in one's medical records.[134] Privacy, Solove argues, is a contextual concept that cannot form the basis for uniform regulation.[135] Rather, in the transaction surveillance setting, the focus should be whether the information is maintained in a system of records.[136] So, to return to his example, the police could interview the sexual partner without restriction, but would need a regulated subpoena to access the medical record of the suspect for the same information.

I agree with the premise of both of Solove's arguments, but am less persuaded that they lead to his conclusion. Solove

---

[131] *Id.* at 1164-65.

[132] *Id.* at 1165.

[133] *Id.* at 1152-53.

[134] *Id.* at 1154.

[135] *Id.* at 1153-54. Solove develops this point in much more detail in Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1088-99 (2002).

[136] Solove, *supra* note 127, at 1157 ("Focusing on 'systems of records' targets the type of information flow that raises concern. Because the problem of modern government information-gathering is caused by the increasing dossiers maintained in private sector record systems, the architecture targets those third parties that store data in record systems.").

is right that making the subtle distinctions demanded by a proportionality approach is difficult and can result in over or under protection of information at the margins. But requiring a uniform standard of probable cause for all record searches, as Solove would, provides far too much protection for some types of information. For instance, data mining of any sort would be almost impossible; if probable cause were required, the sniper-killer and terrorist investigations described above would probably never get off the ground. Or imagine that police want to find out from the phone company who called a murder victim in the two weeks prior to the murder (a scenario often depicted on TV shows like Law & Order). While they would certainly be able to demonstrate the relevance of this catalogic data, they would not have probable cause with respect to any of the callers, and thus would not be able to obtain the regulated subpoena for the phone company's records that Solove would demand. Creating a hierarchy of privacy, as tricky as it is, is important as a means of enabling the balancing of government and individual interests that the Supreme Court has sanctioned since the 1960s.[137]

I also agree that the extent to which we are willing to protect private information is contextual, as Solove's example of the sexual partner interview demonstrates. However, that conclusion does not mean that privacy should be discarded as the baseline consideration in determining the government's authority to obtain information about its citizens. The reason we should treat interviews differently from records requests is not because privacy somehow is irrelevant in the former situation, but because the target's interest in privacy is countered by an even stronger interest–the third party's autonomy. Human information sources, such as the sexual partner, should have a right to decide what to do with the information they possess; in such cases, the subject's privacy interest is outweighed by the source's autonomy interest.[138] When the

---

[137] *See* Camara v. Mun. Ct., 387 U.S. 523, 536-37 (1967) ("[T]here can be no ready test for determining reasonableness other than by balancing the need to search against the invasion which the search entails.").

[138] Mary Irene Coombs, *Shared Privacy and the Fourth Amendment, or The*

third party is an impersonal record-holder, on the other hand, concerns about denigrating "personhood" through limitations on when information may be revealed are non-existent.[139] It is the absence of a legitimate third party interest in surrendering the target's private information, not the bare fact that the information happens to reside in a record, that distinguishes the records request scenario from the interview setting.

These considerations lead me to conclude, contrary to Solove, that privacy concerns should be the fundamental consideration in analyzing transaction surveillance. While information generally should be accorded privacy protection when recorded, the extent of that protection should depend on the degree of privacy associated with the information, not simply on whether it exists in record form. Thus, some transactional information–i.e., that found in truly public records and catalogic data–should be accessible on less than probable cause.

Another alternative to the proportionality approach advanced here evades the issue of whether it is under or over protective of privacy by asserting that it focuses on the wrong sort of privacy invasion. Professor William Stuntz concedes that "secret searches" of our transactional information create risks that "are worth worrying about."[140] But he contends that we would not be particularly bothered by easy government access to such information *if* we never find out it has occurred except in connection with prosecutions for serious

---

Rights of Relationships, 75 CAL. L. REV. 1593, 1643-44 (1987).

[139] For further development of this point, see Slobogin, *supra* note 89, at 834-35. Of course, the employees of the record-holder might want to reveal private information. *See, e.g.*, Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. CAL. L. REV. 949, 1013 (1996) ("As the president of the United States Telephone Association put it in explaining that telephone companies are interested in acceding to law enforcement requests for assistance, the companies want to be 'good local citizen[s].'"). But limiting that ability is not denying the employee's "personhood," because the information is maintained by the institution, not the person.

[140] William J. Stuntz, *Local Policing After the Terror*, 111 YALE L.J. 2137, 2181 (2002).

crime.[141] In other words, covert access to and stringent control over use of transaction information should permit relaxation of the rules as to how we obtain it.

This ignorance-is-bliss notion is superficially attractive. But limiting information flow, which is essential to Stuntz' scheme, can be very difficult. The notion that data gathered by law enforcement will be restricted to a small group of government employees is particularly naive in the wake of 9/11, when literally hundreds of thousands of law enforcement officers are charged with fighting "terrorism," an amorphous threat to say the least.[142] And ensuring that the information government officials acquire through covert surveillance is used only for the purpose of prosecuting serious crime could be equally difficult, precisely because the surveillance is covert.[143] Finally, abandoning all suspicion requirements, as Stuntz would do, virtually guarantees that data would be gathered about large numbers of innocent people, which in turn is likely to increase the chances of government files containing misleading information about its citizens.[144]

Even if the information gathered is somehow confined to a limited and discrete group and is not misused or inaccurate in any way, routine suspicionless and covert transaction surveillance can eat away at whatever trust is left between government and its citizenry. As I wrote in a discussion of Stuntz' proposal in the context of public camera surveillance:

---

[141] *Id.* at 2184-85.

[142] *See generally*, Gabriel Soll, *Terrorism: The Known Element No One Can Define*, 11 WILLAMETTE J. INT'L L. & DISP. RESOL. 123 (2004). *See also* Peter Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1371 (2004) (stating that "the history of previous cycles shows the temptation of surveillance systems to justify an ever-increasing scope of activity, in the hopes that just a little bit more surveillance will catch the terrorists or prevent an attack").

[143] *Id.* at 1366 (discussing "a long-run concern that secret . . . orders" allowing "access to entire databases of records . . . will be used expansively to intrude into a wide array of domestic matters").

[144] The recent exemption of the FBI's Central Records System database from the provision in the Privacy Act that requires government records to be accurate, 68 Fed. Reg. 14140 (Mar. 24, 2003) (to be codified as 28 C.F.R. pt. 16), will not help matters.

> once the public becomes aware that random covert surveillance is occurring, as it inevitably would after a few prosecutions in which the covertly gleaned information is used, the panoptic effect of this regime will be greater than occurs with overt [surveillance]. . . . [W]e would assume that secret surveillance was pervasive, not just incidental. . . . Probably no passage in Orwell's novel *1984* is more chilling than the [following]: "there was of course no way of knowing whether you were being watched at any given moment. . . It was even conceivable that they watched everybody all the time."[145]

With the power of today's computers, government could monitor the transactions of everybody, all the time. A regulatory regime that explicitly *endorsed* that sort of process would destroy any sense of security people might have in today's technological society. Indeed, if government is to be allowed to find out details of our lives whenever it is interested in doing so, we would probably be more comfortable knowing precisely when the surveillance is occurring, rather than being left in the dark.[146]

A final means of regulating transaction surveillance is to leave the task up to the legislature, specifically Congress. Professor Orin Kerr has made the most powerful argument for this approach.[147] He correctly points out that congressional statutes have provided more protection against transaction surveillance than the Supreme Court's construal of the Fourth Amendment in cases like *Miller*,[148] and that, in theory, legislatures are better equipped than courts to craft clear rules

---

[145] Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 305 (2002); *see also* The Council for Excellence in Government, From the Home Front to the Front Lines, America Speaks Out About Homeland Security 6 (March 2004) *available at* http://www.excelgov.org (poll indicating that 72% of Americans have "some" or "very little" trust in the government to "use personal information appropriately").

[146] *Cf.* DAVID BRIN, THE TRANSPARENT SOCIETY (1998) (arguing that "watching the watchers" is the only workable method of regulating government intrusion in the age of technology).

[147] Orin S. Kerr, *The Fourth Amendment and the New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004).

[148] *Id.* at 856.

governing transaction surveillance in an era of rapidly changing, complicated technology.[149] But his arguments fail to negate two crucial facts, documented in this article, about the transaction surveillance rules that Congress has enacted to date: The rules have *not* been particularly clear[150] and, more importantly, they do not provide *adequate* protection against government access to our personal records. Especially in the wake of 9/11, Congress is unlikely to alter its stance unless the courts, relying on the Fourth Amendment, nudge it in the right direction.

Will the courts be willing to engage in such nudging? Certainly, *Miller*, *Smith* and like cases indicate that the Supreme Court is reticent about doing so. But in more recent decisions applying the "special needs" doctrine, which raises parallel issues, the Court has backed off its nonchalant attitude toward nontraditional searches and seizures. In *Ferguson v. City of Charleston*,[151] the Court declared unconstitutional a policy that authorized hospital drug testing of pregnant patients for the purpose of detecting illegal drug use, over a dissent by Justice Scalia arguing that, under *Miller*, the patients voluntarily assumed the risk the results of such tests would be used for investigative purposes.[152] The majority in *Ferguson* ignored Scalia's complaint, reasoning that a reasonable patient would assume the test results would be used for diagnostic purposes and that otherwise they would be kept confidential.[153] In both *Ferguson* and *Indianapolis v. Edmond*,[154]

---

[149] *Id.* at 857-87.

[150] Kerr himself has noted that much of the legislation governing transaction surveillance is complicated. *See, e.g.*, Kerr, *supra* note 90, at 1208 ("[C]ourts, legislators, and even legal scholars have had a very hard time making sense of the [Stored Communications Act of ECPA]."); Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 820 (2003) (the "law of electronic surveillance is famously complex, if not entirely impenetrable.").

[151] 532 U.S. 67 (2001).

[152] *Id.* at 95 (Scalia, J., dissenting) ("Until today, we have *never* held—or even suggested—that material which a person voluntarily entrusts to someone else cannot be given by that person to the police, and used for whatever evidence it may contain.").

[153] *Id.* at 78 ("The use of an adverse test result to disqualify one from eligibili-

which held invalid a roadblock set up to interdict narcotics, the Court also emphasized that individualized cause requirements may not be relaxed if the only "special need" pleaded by the government is a "general interest in law enforcement."[155]

Ferguson signals that the Court is hesitant about granting the government an exemption from traditional Fourth Amendment standards simply because information relevant to a criminal investigation has been handed over to a third party (thus undermining *Miller*'s premise). And both *Ferguson* and *Edmond* suggest that strong government allegations that relaxation of those standards is necessary to detect criminal activity will not always prevail (thus undermining the "heightened need" rationale as a ground for reducing Fourth Amendment protections). These decisions provide a glimmer of hope that, when confronted with cases challenging subpoenas for personal records about medical treatment, personal finances and the contents of email messages, the Court will withdraw from its broad pronouncements in *Miller*. If it does so, further, more detailed rule-making along the lines suggested here might best be left to Congress, for the reasons Kerr suggests. The goal is meaningful protection of personal information. The source of that protection is not so important.

CONCLUSION

Analysis of government surveillance has tended to focus on communications and physical surveillance. Yet transaction surveillance is at least as pervasive as these other types of

---

ty for a particular benefit, such as a promotion or an opportunity to participate in an extracurricular activity, involves a less serious intrusion on privacy than the unauthorized dissemination of such results to third parties. The 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.").

[154] 531 U.S. 32 (2000).

[155] *Ferguson*, 532 U.S. at 79; *Edmond*, 531 U.S. at 47 ("When law enforcement authorities pursue primarily general crime control purposes at checkpoints such as here, however, stops can only be justified by some quantum of individualized suspicion.").

investigative techniques, and can be as inimical to privacy interests. Public and private records contain information regarding virtually every aspect of our lives. In the past few decades, technology has made that information infinitely more easily aggregated and accessible.

Nonetheless, neither legislatures nor courts have evidenced much concern about transaction surveillance. Congress appears to think of transaction information as "business records," and thus at most entitled to the protection afforded by subpoenas, while the Supreme Court tells us we must assume the risk that record-holders will betray us. These positions ignore the obvious fact that medical, financial and other types of private and public records contain much personal information. They also fail to acknowledge that disclosure of that information to record-keepers–disclosure that those of us who live a modern lifestyle cannot avoid–is no different, in expectation of privacy terms, than communicating with others by phone or email or interacting with others inside one's home, both activities clearly protected by the Constitution. As Senator Sam Ervin recognized in 1974, "[g]overnment has an insatiable appetite for power, and it will not stop usurping power unless it is restrained by laws they cannot repeal or nullify."[156] When it comes to transaction surveillance, only the Fourth Amendment provides that type of restraint.

---

[156] Introductory Remarks of Senator Sam J. Ervin on S. 3418, H.R. REP. NO. 93-1416 (1974), *reprinted in* U.S. CONGRESS, LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974, at 3-8 (1976).