

## Transaction Surveillance

©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 data. Although we often willingly disclose these facts to the entities which store them, the disclosure is usually with the 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 these records private, vis-a-vis most of the world.

Thus, it may be surprising that law enforcement officials can 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, most records of the sort just described can be obtained any time they are “relevant” to a government investigation—a much lower, and much more diffuse, level of justification than probable cause—and some types of records are accessible on an even lesser showing.<sup>1</sup> The usual mechanism for acquiring this information is a subpoena, issued either by a grand jury (and called a subpoena duces tecum) or a government agency (using an

---

\*Stephen C. O’Connell Professor of Law, University of Florida Fredric G. Levin College of Law. This article is based on a presentation given at DePaul Law School in March, 2004, at the Symposium on Privacy and Identity.

<sup>1</sup>See infra text accompanying notes .

“administrative subpoena”). Subpoenas of either type are notoriously easy to obtain and execute. According to the Supreme Court, the Constitution places virtually no restrictions on subpoenas used to obtain records maintained by third parties, and is only minimally more protective when the records are held by the target of a subpoena.<sup>2</sup> Although various federal statutes purport to place extra-constitutional restrictions on law enforcement use of subpoenas, this legislation places no meaningful restraints on law enforcement efforts to obtain most records.<sup>3</sup> Even a strong claim of innocence or irrelevance is not a ground for quashing law enforcement demands for paper and digital documents.<sup>4</sup> And where the records are in the possession of a third party, the person whose activities they catalogue is often not *permitted* to challenge the records request.<sup>5</sup>

These positions might make sense when the focus of the subpoena is an organizational record, sought in an effort to investigate the organization and its members. In fact, that was the typical use of the administrative subpoena for many years,<sup>6</sup> and grand jury subpoenas *duces tecum* were also often directed at such targets.<sup>7</sup> But today, facilitated by the computerization of

---

<sup>2</sup>See *infra* text accompanying notes .

<sup>3</sup>See *infra* text accompanying notes .

<sup>4</sup>See generally, Roger B. Handberg, *The Enforcement of Investigative Subpoenas Issued by Administrative Agencies*, 76 Fl. Bar J. 40, 42 (2002) (“Courts do not require a detailed showing by the agency regarding the grounds for the investigation, nor do they attempt to determine at the outset whether the governmental entity eventually will be able to prove whether a suspected violation has occurred or is occurring.”). See also *infra* text accompanying notes .

<sup>5</sup>See *infra* text accompanying notes .

<sup>6</sup>See *infra* text accompanying notes .

<sup>7</sup>See *infra* text accompanying notes .

information and communication, subpoenas are routinely used to obtain *personal* medical, financial and email records, in connection with investigations that have nothing to do with administrative regulation or corporate or official crime. That practice is much more questionable.

This article explores the scope of what I will call “transaction surveillance” by the government. Transaction surveillance is to be distinguished from 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, the focus of this article, 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).<sup>8</sup>

Like physical and communications surveillance, transaction 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

---

<sup>8</sup>This tripartite division of surveillance was developed by the American Bar Association’s Task Force on Law Enforcement and Technology 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).

of activities inside the home or communications surveillance.<sup>9</sup> 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 criticism begins with an explanation of why we got where we are today, tracing how subpoenas were traditionally directed primarily at organizational crimes and have since morphed into a potent investigative tool for crimes committed by individuals. 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 entities and to the reasonable suspicion level for public records.

---

<sup>9</sup>As discussed *infra* text accompanying notes , 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, 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, with technology that only replicates such naked eye viewing, or with technology in general public use. *Kyllo v. United States*, 533 U.S. 27 (2001).

Part IV concludes by examining alternatives to the proposal (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 or virtually suspicionless records searches on condition that anything discovered is subject to strict limitations on disclosure. 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. Perhaps the most basic division is between target-based and event-based transaction surveillance. Using that categorization, 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 I'm a detective, who is suspicious of you for some vague reason—perhaps you are routinely seen at anti-war protests,<sup>10</sup> or you often pay for your airplane tickets with cash,<sup>11</sup> or you are a young, Arab male who goes to the local mosque on a daily basis.<sup>12</sup> Under these types of

---

<sup>10</sup>Cf. *Laird v. Tatum*, 408 U.S. 1, 24-28 (1972)(Douglas, J., dissenting)(describing compilation of dossiers on antiwar protestors and other political groups by the Army).

<sup>11</sup>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).

<sup>12</sup>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).

circumstances, I clearly do not have sufficient suspicion for an arrest, or even enough to bring you in for questioning.<sup>13</sup> On the other hand, I feel I would be neglecting my obligation as a crime-fighter if I did not investigate you a bit further. So how do I find out more about you?

I could confront your acquaintances and neighbors, but that might tip you off. Or 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 time on someone about whom I’m merely suspicious would usually be a waste of time. I could also 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.

There are, however, other, much more efficient ways I can covertly acquire information about you, without ever having to leave my desk. First, I can contact one of the many companies that use computers and the Internet to dig up “dirt” from public and quasi-public records.<sup>14</sup> One such company is Seisint, a concern based in Florida that operates a program known as Accurint (for accurate intelligence). According to its advertising, Accurint can, in mere seconds, “search[] more than 20 billion records . . . dating back 30 years and more,” armed with no more

---

<sup>13</sup>An arrest or prolonged questioning in the stationhouse requires probable cause, and even questioning in the field that lasts longer than a few minutes requires reasonable suspicion, the latter of which exists only if there are specific and articulable facts that the person is or has been engaging in criminal activity. Charles H. Whitebread & Christopher Slobogin, *Criminal Procedure: An Analysis of Cases and Concepts* 72-76 (4<sup>th</sup> ed. 2000).

<sup>14</sup>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.

than a name, address, phone number, or social security number.<sup>15</sup> Through this process, it can obtain information about a wide array of a person's transactions, including: bankruptcies and corporate filings; criminal conviction and criminal and civil court data (including marriage and divorce information); driver's license and motor vehicle information; firearms, hunting, fishing and professional licenses and permits; Internet domain names; property deeds and assessments; and voter registration information.<sup>16</sup>

All of this was recently made even more easily accessible to state law enforcement officials with the establishment of Matrix, a multi-state consortium funded in part by the federal government, which allows police to use Accurint for investigative purposes.<sup>17</sup> The FBI and other federal agencies rely on an even more powerful commercial data broker service called Choicepoint.<sup>18</sup> As a law enforcement official, these types of resources can provide me, completely clandestinely, with a virtual cornucopia of information about you if you have ever owned real estate, taken out a government-backed loan, driven a car, or done something else that is monitored by a government agency. If you think I wouldn't bother doing this, think again;

---

<sup>15</sup>[Www.accurint.com](http://www.accurint.com), in the link section entitled "What we do" (last accessed on March 28, 2004).

<sup>16</sup>Id. in the link section entitled "How we do it" (last accessed on March 28, 2004).

<sup>17</sup>See Duane Stanford & Joey Ledford, *Matrix Links Up Private Data*, Atlanta Journal-Constitution, October 3, 2003, at A1.

<sup>18</sup>Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, pp. 15-16.

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*.<sup>19</sup>

Using these services, or acting on my own, I can also accumulate information held by *non-governmental entities*. With your social security number and mother's maiden name, which Accurint or Choicepoint should be able to give me, I might be able to access your credit records, school records, and even bank accounts.<sup>20</sup> As one commentator put it, "those with unrestrained access to interconnected computer data networks can construct a complete mosaic of a person's characteristics based upon records of purchases, tax payments, relocations . . . records of newspaper and periodical subscriptions, mail order histories, travel reservations, payroll records, credit card usages [and] credit ratings . . . ." <sup>21</sup> As another commentator stated, "because data networks have become so concentrated and interconnected in the United States today, a 20 page dossier on every person in the United States could become available to a persistent seeker in a matter of only four minutes."<sup>22</sup> And that statement was written over twenty years ago, before most of the upgrades that have made data systems even more dependent on computers.

---

<sup>19</sup>Id. at 4-6. In 2001, the Immigration and Naturalization Service conducted approximately 23,000 such searches a month. Id. at 11.

<sup>20</sup>See Lynn M. LoPucki, *Human Identification Theory and the Identity Theft Problem*, 80 Tex. L. Rev. 89, 108-14 (2001)(noting that schools, financial institutions and other entities make personal information accessible by anyone with the right Social Security number, address, and mothers' maiden name).

<sup>21</sup>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).

<sup>22</sup> Halls, *Raiding the Databanks: A Developing Problem for Technologies and Lawyers*, 5 J. Contemp. L. 245, 246 (1979)).

These days, given the advent of the Internet, there is still more I can do to construct my mosaic of you, if I'm willing to invest in something called "snoopware." Bearing names like BackOrifice, Spyagent, and WinWhatWhere,<sup>23</sup> snoopware is to be distinguished from adware and spyware, which use "cookies" to tell the buyer of the program who visits 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 (some snoopware, using "key logger" technology, can even tell the user the content of your computer screen, but that is a form of communications surveillance that is beyond the scope of this article).<sup>24</sup> Although some transaction snoopware requires access to the computer to install, other types, called Trojan Horses, can electronically worm their way onto the system disguised as something useful.<sup>25</sup> The FBI has developed a similar device, once dubbed Carnivore, now called DCS-1000, that filters all emails that pass through a particular server.<sup>26</sup> If all of this is too fancy for me, I might simply ask your Internet service provider (ISP) for a record of every website you have visited (so-called "clickstream data"), which is information most ISPs keep as a matter of routine.<sup>27</sup> These various uses of technology can

---

<sup>23</sup>See Cade Metz, *Spyware: It's Lurking on Your Machine*, PC Magazine, April 22, 2003, at 85, 88.

<sup>24</sup>Id. at 86.

<sup>25</sup>Id. at 85.

<sup>26</sup>Jeremy C. Smith, *The USA Patriot Act: Violating Reasonable Expectations of Privacy Protected by the Fourth Amendment Without Advancing National Security*, 82 N.C. L. Rev. 412, 448-49 (2003)

<sup>27</sup>Gavin Skok, *Establishing a Legitimate Expectation of Privacy in Clickstream Data*, 6 Mich. J. Telecomm. & Tech. L. Rev. 61, 68-69 (2000).

provide a significant additional amount of information about you, at least if you like to surf the Net and conduct your business and social life via email. And, again, I can get all of this transactional data without you having a clue I'm doing it.

## B. Event-Based Transaction Surveillance

Now consider an entirely different type of scenario, one in which government has no suspicion with respect to a specific individual, but rather possesses information about a particular crime that either has been or will be committed. Say, for instance, that the police know that a sniper-killer is using a particular type of gun (thanks to ballistics tests), that he owns a particular type of sweater (because of threads found at a sniper 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 gun, clothing, and book stores as part of their 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.<sup>28</sup> The FBI wants 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 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, further investigation might take place.

---

<sup>28</sup>This imaginary scenario is borrowed from the "Markle Report." See Task Force on National Security in an Information Age, *Creating a Trusted Network for Homeland Security*, App. D (Vignette Four)(2003).

These types of law enforcement efforts are a form of “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.<sup>29</sup> A significant amount of data mining can be carried out using services like Matrix or Choicepoint, and technologies such as DCS-1000 could be programmed to sift out emails going through a particular server that are addressed to specified addresses. If the information sought is not digitized, which is likely with respect to records kept by ski-diving companies, for instance, then law enforcement may have to rely on good old-fashioned human snooping. Whether it relies on computers or humans, data mining, like transaction surveillance of particular individuals, can easily be conducted unbeknownst to those whose activities are surveilled.

## II. Current Legal Regulation of Transaction Surveillance

When conducted by private entities, some types of transaction surveillance are unregulated, a few are clearly illegal, and many exist in a regulatory gray area. Although lawmakers have expressed concern about the phenomenon, data collection with the hope of mining it for information—event-based transaction surveillance—is perfectly legal when carried out by private parties.<sup>30</sup> In contrast, private use of snoopware to carry out target-based

---

<sup>29</sup>For a general description of data mining and its prevalence, see Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Private Tort Response to Consumer Data Profiling*, 98 Nw. U. L. Rev. 63, 71-88 (2003).

<sup>30</sup>Prior to 9/11, Congress had considered several bills that would have severely restricted such data collection. See *id.* at 88 n. 165. The likelihood that such bills will succeed post 9/11 is slim. *Id.* Note also that, at present, a service provider may disclose transactional information such as customer lists to any private party. 18 U.S.C. § 2703(c)(1)(A).

surveillance may be prohibited under some circumstances; its legitimacy depends on a number of variables, including whether the user is the owner of or service provider for the computer, and whether websites visited have agreed to be snooped.<sup>31</sup> Similarly, the extent to which private entities can legitimately use companies such as Accurint or Choicepoint is unclear. Because the Privacy Act at the federal level and similar statutes in several states bar access to many types of public records unless the access is congruent with the purpose for which they are kept,<sup>32</sup> use of these services may be limited to insurance companies, credit agencies, and other entities that can promise to use the information only for specified purposes. The law speaks most clearly with respect to a third party's use of someone's social security number or other identifying information to gain access to his or her account; that conduct is "identity theft," if carried out with the intent to commit a crime.<sup>33</sup>

---

<sup>31</sup>Private individuals may not use devices designed to ascertain phone numbers and email addresses. 18 U.S.C. § 3121(a) ("no person may install or use a pen register or a trap and trace device without first obtaining a court order."). Additionally, the Computer Fraud and Abuse Act punishes anyone who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer if the conduct involved an interstate or foreign communication," although damages have to amount to \$5,000 in any single year. 18 U.S.C. § 1030(a)(2)(c). However, websites may set up, or authorize use of, cookies that monitor their clickstream data, which courts have held means that at least one party to their "use" has consented to it. In re DoubleClick Inc. Privacy Litigation, 154 F.Supp. 497, 510-11 (2001). Employers may intercept employee messages even if they are *not* parties to them, if the company reasonably believes that the monitoring is necessary to protect its "rights or property." 18 U.S.C. § 3121(b)(1).

<sup>32</sup>The federal Privacy Act permits disclosure of a record for "routine use," 5 U.S.C. § 552a(b)(3), i.e., a use "which is compatible with the purpose for which it was collected." 5 U.S.C. § 552a(7). For a general description of state privacy statutes, see Kurt H. Decker, *Employment Privacy Law for the 1990's*, 15 Pepperdine L. Rev. 551, 568-70 (1988).

<sup>33</sup>See Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 Hastings L.J. 1227, 1246-47 (2003) (describing federal and state statutes). See also Fl. Stat. § 119.0721 (making obtaining a social security number through false representation a felony).

Law enforcement, in contrast, can get all of this information without having to resort to the types of fraudulent practices used by identity thieves, and usually with very little oversight by any outside agency. To understand this point, a brief rehearsal of the typical constitutional restraints on police searches and seizures is necessary. Authorization for most searches and seizures requires probable cause, 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).<sup>34</sup> Some less invasive actions are permissible on 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*).<sup>35</sup> Finally, in circumstances where the government seeks records from a third party, the government can, and usually does, resort to the subpoena process, using either a grand jury, or so-called “administrative subpoenas” that agencies may resort to if a statute authorizes them. A subpoena can issue even in the absence of reasonable suspicion; the only requirement is that the information sought be relevant to a legitimate (statutorily-authorized) investigation.<sup>36</sup> However, the target of the subpoena can at least ask a court to quash it, before the records are handed over. The usual grounds for doing so are irrelevance and overbreadth.<sup>37</sup> Although subpoenas are

---

<sup>34</sup>See Whitebread & Slobogin, *supra* note , at 137-142.

<sup>35</sup>392 U.S. 1, 21, 30 (1968).

<sup>36</sup>See *infra* text accompanying notes .

<sup>37</sup>See *United States v. Gurule*, 437 F.2d 239, 241 (10<sup>th</sup> Cir. 1970). Other possible grounds for suppressing a subpoena include privilege (attorney-client, doctor-patient, journalist, etc.) and harassment. See *Powell v. United States*, 379 U.S. at 58 (stating that a court should refuse to enforce a subpoena that was issued for an improper purpose “such as to harass . . . or put pressure on [the subject] to settle a collateral dispute . . .”).

seldom found invalid on either ground,<sup>38</sup> official knowledge that investigative targets will learn about the government's interest in their records and can force the government to justify that interest probably acts as a brake on large-scale or frequent fishing expeditions-by-subpoena.<sup>39</sup>

That is the traditional three-tiered hierarchy of fourth amendment protection. But, as we shall see, the law does not require any of these authorizations for most types of transaction surveillance. Instead, the government, in particular Congress, has either invented new forms of authorization that are easier to obtain than any of these three, or has simply permitted unrestrained law enforcement access to transactional information, whether it is intercepted in real-time, found in public records, or found in records maintained 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

---

<sup>38</sup>See *infra* text accompanying notes . See also, Handberg, *supra* note , at 45 (“there are few recent cases where courts have concluded that an investigative subpoena was overly broad [and] in those cases where such a finding was made, courts have largely elected to narrow the scope of the subpoena as opposed to quashing it altogether.”).

<sup>39</sup>In the warrant context, police knowledge that a magistrate will check their application, even if only to rubberstamp it, increases their “standard of care.” Richard Van Duizend, L. Paul Sutton & Charlotte A. Carter, *The Search Warrant Process: Preconceptions, Perceptions, and Practices* 148-49 (1985). Also noteworthy in this regard is judicial antipathy toward “forthwith subpoenas,” subpoenas served by police that demand immediate compliance. In those jurisdictions where they are not prohibited, courts have insisted, relying on either the fourth amendment or due process considerations, that the target be permitted to contest the subpoena. See Wayne R. LaFave, Jerold H. Israel, Nancy J. King, *3 Criminal Procedure* 142-43 (2d ed. 1999). As one court stated in this context, the opportunity to oppose the subpoena before production of documents is “an extremely important feature of a subpoena duces tecum—one that might otherwise save it from being a warrantless search and seizure.” *Dean v. State*, 478 So.2d 38, 42 (Fla. 1985).

cause.<sup>40</sup> 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 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 phone numbers and email addresses a search, the Supreme Court has held that a *fourth amendment* search occurs only when a government action infringes a reasonable expectation of privacy.<sup>41</sup> More importantly for present purposes, the Court has determined that we do not have a 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.<sup>42</sup> Because it is generally known that Internet service providers maintain logs of our emails (albeit often only temporarily), the Court would probably also say that we assume the risk

---

<sup>40</sup>18 U.S.C. § 2518(3) (requiring that interception of oral, wire and electronic communications be authorized by a warrant after a judge has found there is “probable cause for belief that an individual is committing, has committed, or is about to commit [a listed offense]” and “probable cause for belief that particular communications concerning that offense will be obtained through such interception”). 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).

<sup>41</sup>*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)).

<sup>42</sup>*Smith v. Maryland*, 442 U.S. 735, 744 (1979) (“petitioner 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.”)

these providers will become government informants.<sup>43</sup> Accordingly, the government may ignore the fourth amendment when intercepting phone numbers and email addresses.

Congress has imposed some statutory restraints on this type of surveillance, but not serious ones. Under the Electronic Communications Privacy Act of 1986 (ECPA), authorization for use of a pen register (which obtains transaction information about outgoing phone calls) or a trap and trace device (which obtains information about incoming phone calls) is obtained simply by certifying to a court facts that show the information is “relevant to an ongoing investigation” and is “likely to be obtained by [the surveillance].”<sup>44</sup> If that certification is made, the court *must* issue the order.<sup>45</sup>

The USA Patriot Act of 2001 expanded the definition of pen registers and trap and trace devices to include all “dialing, routing, addressing, or signaling information utilized in the processing and transmitting of wire or electronic communications.”<sup>46</sup> Thus, as with pen

---

<sup>43</sup>Cf. *United States v. Hambrick*, 225 F.3d 656 (4<sup>th</sup> 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.”). *United States v. Kennedy*, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) (“*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 . . .”). 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 law enforcement. *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).

<sup>44</sup>18 U.S.C. § 3123(a)(1).

<sup>45</sup>*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.”).

<sup>46</sup>18 U.S.C. § 3121(c).

registers and trapping devices, to use snoopware, DCS-1000,<sup>47</sup> 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.<sup>48</sup> Again, if this certification is made, the court must issue an order authorizing the interception.

Those of us who teach fourth amendment law sometimes joke about supposedly "neutral and detached" magistrates rubberstamping warrant applications, but we also assume that judicial independence is theoretically possible.<sup>49</sup> 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.

---

<sup>47</sup>DCS-1000 can be configured to obtain either the entire email, content and addresses, or merely the latter, with the content X'ed out. Even in the latter configuration, agents can view the length of the email message, as well as routing information. Joseph F. Kampherstein, *Internet Privacy Legislation and the Carnivore System*, 19 Temp. Envtl. L. & Tech. J. 155, 167 (2001).

<sup>48</sup>Most courts have held that companies that acquire "clickstream data" about where a 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.*, 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 pen registers, trap and trace devices, or other 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 (11<sup>th</sup> Cir. 2003). If so, ironically, government may have to make a slightly greater showing than is required to operate pen registers and the like; as described infra text accompanying notes , accessing stored information requires an ex parte subpoena.

<sup>49</sup>See Richard Van Duizend et al, *supra* note , at 47-48 (1985) (describing study of warrant process indicating varying degrees of judicial rubberstamping across jurisdictions).

## B. Access to Publicly-held Records

Most transaction surveillance does not involve real-time interception of information, but rather the accessing of already-existing records, held either by public or private institutions. Information in public records is particularly easy to secure. Under current law, law enforcement does not need even a certification order to use Matrix, Choicepoint and similar vehicles for perusing public records. More bluntly, police need consult no other entity (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. Once the information is surrendered to an agency or institution, the Court stated in the important case of *United States v. Miller*,<sup>50</sup> one assumes the risk the third party will hand them over to the government.<sup>51</sup>

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.<sup>52</sup> But when *law enforcement* officials are after the records, the Act merely requires a

---

<sup>50</sup>425 U.S. 435 (1976).

<sup>51</sup>Id. at 443 (“This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, 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.”).

<sup>52</sup>See 5 U.S.C. § 552a(b) (“No agency shall disclose any record which is contained in a system of records . . . unless [listing 12 exceptions]”).

letter detailing the reasons a particular person's records are needed.<sup>53</sup> 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*.” Because the Privacy Act only applies to federal records and because some states do not have analogous privacy statutes, even this minimal level of authorization is not necessary for many public records at the state level, which makes vehicles like Matrix even easier to use.<sup>54</sup>

### C. Access to Privately-held Records

Compared to the meager limitations on accessing public records, the restrictions on government surveillance 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

---

<sup>53</sup>5 U.S.C. 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”).

<sup>54</sup>One reason Florida is an attractive place to base an operation like Matrix is that its public records law is quite extensive. See Fl. Stat. § 119.01 et seq. (“It is the policy of this state that all state, county and municipal records 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*, ABA Journal 24 (April, 2004).

(in *Smith v. Maryland*)<sup>55</sup> and banks (in the aforementioned *Miller* decision).<sup>56</sup> 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 limitations on law enforcement access.<sup>57</sup> Although there are also statutory constraints 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 (HIPPA), the government can obtain medical records from HMOs and hospitals with a subpoena which, 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

---

<sup>55</sup> *Smith v. Maryland*, 442 U.S. 735, 744 (1979) (“petitioner 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.”).

<sup>56</sup> *United States v. Miller*, 425 U.S. 435, 443 (1976) (a “depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the government.”);

<sup>57</sup> Cf. *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001) (“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.”); *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”).

privilege grounds).<sup>58</sup> Furthermore, the same information, if surrendered to an Internet health website, is not protected by HIPAA,<sup>59</sup> meaning the government may be able to obtain it simply with an extrajudicial request.

Financial records receive similarly minimal protection. To get detailed information from credit agencies, a regular subpoena is required under the Fair Credit Reporting Act.<sup>60</sup> However, analogous to the situation with medical records, no law governs government requests for the same information from database companies and other companies that have obtained it from the credit agencies.<sup>61</sup> As a result, government routinely gets the financial information it wants directly from a commercial data broker, without bothering with a subpoena.<sup>62</sup> Bank records are also easily accessible. The Right to Financial Privacy Act generally requires a traditional subpoena to obtain financial records from a bank, but with one significant variation: 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

---

<sup>58</sup>45 C.F.R. § 164.512(f)(1)(ii). Some courts have required probable cause in order to obtain medical records. See, e.g., *Hawaii Psychiatric Soc., Dist. Branch of American Psychiatric Ass'n v. Ariyoshi*, 481 F.Supp. 1028 (D.Hawai'i Oct 22, 1979).

<sup>59</sup>See Pew Internet & American Life Project, Institute for Healthcare Research and Policy, Georgetown University, *Exposed Online: Why the New Federal Health Privacy Regulation Doesn't offer Much Protection to Internet Users* 14-17 (Nov. 2001).

<sup>60</sup>15 U.S.C. § 1681b(a)(1). Name, addresses, and places of employment can be obtained simply upon a request. *Id.* § 1681f.

<sup>61</sup>Solove, *supra* note , at 1146.

<sup>62</sup>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 , at 18..

compromise the government's investigation.<sup>63</sup> 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*.”

Under the Electronic Communications Privacy Act of 1986 (ECPA), a subpoena–delayed if necessary–is also adequate authorization for accessing the content of *emails*, if the email has sat on a server for longer than 180 days without being deleted or if it is kept by a “remote computing service” (i.e., a service that stores electronic data for the general public).<sup>64</sup> Apparently, the rationale behind permitting this access of content on less than probable cause is the assumption that a message stored by a third party becomes less private, more akin to a business record.<sup>65</sup>

ECPA also gives the government virtually unlimited access to 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 uses a pseudonym–can be obtained pursuant to still another sort of quasi-

---

<sup>63</sup>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, what this article calls an extrajudicial certification. *Id.* § 3408.

<sup>64</sup>18 U.S.C. § 2703(a); 2703(b)(1)(B). Note that if the storage takes place in a server not available to the general public, then ECPA does not apply at all. 18 U.S.C. § 2711(2) (defining remote computing service). See also, U.S. Dep’t of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 89 (July, 2002).

<sup>65</sup>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).

subpoena, what I will call an “*ex parte subpoena*.”<sup>66</sup> That label is apposite because only the third-party recordholder may try to quash a subpoena seeking subscriber information; subscribers themselves are not permitted to do so and may never even find out about the inquiry,<sup>67</sup> thus removing the only meaningful inhibition on fishing expedition-by-subpoena.

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.”<sup>68</sup> Apparently, this 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: this standard arguably does not require the quantum of certainty that reasonable suspicion does.<sup>69</sup> Furthermore, whereas *Terry* contemplated that reasonable suspicion

---

<sup>66</sup>18 U.S.C. § 2703(c)(1)(E).

<sup>67</sup>18 U.S.C. § 2703 (c )(3) (“A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.”). Sometimes this type of subpoena is called a “third party subpoena,” but that label merely suggests that the subpoena is addressed to the third party, not that only the third party can contest it.

<sup>68</sup>18 U.S.C. § 2703(c)(d)(describing requirements for a court order to obtain “records concerning electronic communication service or remote computing service”).

<sup>69</sup>See *U.S. v. R. Enterprises*, 498 U.S. 292, 301 (1991)(“where, as here, a subpoena is challenged on relevancy grounds, the motion to quash must be denied unless the district court determines that there is no reasonable possibility that the category of materials the Government

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, in at least one sense this kind of authorization is easier to obtain than a normal subpoena: the third party record-holder may not challenge the order on relevance grounds, but only argue that it is unduly burdensome.<sup>70</sup>

Post-9/11, government access to some sorts of privately-held records is even easier, at least if a significant purpose of the investigation is to nab terrorist or spies. Under the Patriot Act, the FBI can obtain business records, including those of phone companies, Internet service providers, libraries, video stores, schools and other private entities, simply by certifying that the information is required “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.<sup>71</sup> If such a certification is made, the court *must* issue an order authorizing the seizure; it exercises no independent judgment on the matter. In other words, a certification order, of the type discussed in connection with use of pen 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.<sup>72</sup>

---

seeks will produce information relevant to the general subject of the grand jury's investigation.”).

<sup>70</sup>Id. (providing that the court may quash or modify the order “if the information or records requests are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.”).

<sup>71</sup>18 U.S.C. § 2709(b)(wire or electronic service providers); 50 U.S.C. § 1861(a)(1) (“business records”); 20 U.S.C. § 1232g(j)(A)(school records).

<sup>72</sup>18 U.S.C. § 2709(c); 50 U.S.C. § 1861(d).

Finally, if the FBI is seeking financial records in connection with a national security investigation, it need not worry about any sort of challenge. Rather all it must do is issue a form of administrative subpoena, known as a “National Security Letter,” that certifies the information sought is relevant to a national security investigation to protect against international terrorism or clandestine intelligence activities.<sup>73</sup> 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. The Patriot Act allowed this extrajudicial process only when the financial information sought was held by banks. However, in December, 2003, that power was expanded by the Intelligence Authorization Act of 2003, which was enacted 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.<sup>74</sup> The 2003 Act allows the FBI to use extrajudicial 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.<sup>75</sup> All of this information is the government’s simply on its sayso.

#### D. Summary of Transaction Surveillance Law

---

<sup>73</sup>12 U.S.C. § 3414(a)(5)(A). Again, the record-holder is prohibited from informing the target of the request. *Id.* § 3414(a)(5)(D).

<sup>74</sup>Kyle O’Dowd, *Congress Hands FBI “Patriot II” Snooping Power*, 28 *Champion* 18 (Feb. 2004).

<sup>75</sup>31 U.S.C. § 5312.

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,<sup>76</sup> 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 called a *Terry* order, after *Terry v. Ohio*.<sup>77</sup> 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 (aimed at the record-holder rather than the target), which allows access to phone and ISP account records.<sup>78</sup> Then comes the certification (judicial rubberstamp) order, which authorizes use of pen registers, trap

---

<sup>76</sup>See supra note .

<sup>77</sup>392 U.S. 1 (1968).

<sup>78</sup>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 text accompanying notes , it is classified here as less protective than a regular subpoena, at least one that notifies the target.

and trace devices and other forms of transaction-oriented snoopware. Finally, there is the extrajudicial certification, which permits access to public records, and to financial and other records relevant to terrorist and espionage investigations. In those states without a privacy statute, police need no authorization to access public records. All of the authorization devices 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.<sup>79</sup>

The following chart depicts the foregoing summary, consisting of eight levels of “authorization”:

<b>Transaction</b>	<b>Auth’zation Req’d</b>	<b>Certainty Level</b>
-----	Warrant	Probable cause
-----	<i>Terry</i> Order	Reasonable suspicion
Medical and financial records; stored email	Subpoena	Relevance per court, 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 of phone companies & Internet service providers	Ex Parte Subpoena	Relevance, challengeable only by third party record-holder
Interception of transaction information re calls & email; business records re terrorism	Certification Order	Relevance per police, issued by court, not challengeable by any party

---

<sup>79</sup>For instance, there is no exclusionary sanction under ECPA. Whitebread & Slobogin, *supra* note , at 344-45, or under the Right to Financial Privacy Act. *United States v. Kington*, 801 F.2d 733 (5<sup>th</sup> 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 (4<sup>th</sup> 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 per police, not challengeable by any party
All other public records not protected by state law	None	None

#### IV. 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 relevance challengeable by the target. 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 or seizure be roughly proportionate to the intrusiveness of the search or seizure, and which suggests that the traditional probable cause/reasonable suspicion dichotomy is insufficient as a means of implementing that idea.<sup>80</sup> 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 (personal v. organizational; content v. catalogic) and where the information is held (private v. public records). More specifically, I propose that when government seeks access to

---

<sup>80</sup>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); *The World Without A Fourth Amendment*, 39 UCLA L. Rev. 1, 68-75 (1991);

information about the personal transactions of individual citizens (as opposed to the transactions of organizations), it should be required to obtain: (1) a warrant based on probable cause to access records maintained by “private entities” or that are otherwise presumptively private; (2) a *Terry* order based on reasonable suspicion when seeking records that are “public”; and (3) a traditional subpoena based on relevance—or when there is concern about tipping off a suspect, a delayed-notice subpoena based on relevance—to access information identifying a communication or linking a person to an activity (catalogic information). Authorization necessary for event-based transaction surveillance (data mining/profiling), ought to depend on which of the foregoing categories of information (content v. organizational, private or public) are accessed. Ex parte subpoenas, certification orders and extrajudicial certifications should *never* be sufficient authority to carry out nonconsensual searches and seizures for personal transaction information, except in emergencies, and then only if quickly subject to judicial review. The following chart represents my proposal:

<b>Transaction</b>	<b>Auth’zation Req’d</b>	<b>Certainty Level</b>
Content of privately-held personal records	Warrant	Probable Cause
Content of publicly-held personal records	<i>Terry</i> Order	Reasonable Suspicion
Content of organizational records; Catalogic data	Subpoena (delayed if need for covert surveillance)	Relevance
Data mining; Profile information	Court order	Dependent on Nature of Records Accessed

Under this scheme, communication “content” is distinguished from “catalogic data” that simply describes the nature of a transaction, with the acquisition of content requiring more

justification except when the record is an impersonal “organizational” document. Additionally, “privately-held records” are distinguished from “publicly-held records,” with the content of the latter receiving less protection. Finally, regulation of event-based transaction surveillance, involving data mining and profiling, would vary with the type of records accessed. 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

Under the current legal regime, government can obtain personal medical and financial information, as well as stored email correspondence, much more easily than it can search a living room, luggage or a car (all of which require probable cause). From a privacy perspective, that makes no sense. Empirical research suggests that most people view a search of records containing their medical facts, financial information, and (old) emails to friends and associates to be at least as intrusive as a search of their car.<sup>81</sup>

Why are these records so easy to obtain? The answer to that question requires a short history lesson. For a time at the end of the nineteenth century, government was prohibited from requisitioning most types of records, at least when held by the target. Then at the beginning of the twentieth century the courts began to reverse course. By World War II, the regulatory

---

<sup>81</sup>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, and less intrusive than search of a high school student’s purse)

demands of the New Deal led to rulings that made business records readily accessible to the government. The courts justified this lenient treatment primarily on two grounds: regulation of businesses would be impossible if their records were difficult to obtain, and corporations are entitled to less constitutional protection than individuals. These original rationales for permitting easy access to records have gradually faded from the judicial memory, however, as courts have permitted government to obtain personal records under the same relaxed standards developed in organizational cases. An account of the history is followed by an analysis of why the courts have gone astray.

#### 1. The Law of Subpoenas from *Boyd* to the Present

The short period during which records were almost immune from government access surrounded the Supreme Court's decision in *Boyd v. United States*,<sup>82</sup> decided in 1886. *Boyd* held that using a subpoena to force an individual to produce private documents violated the Fifth Amendment's prohibition on compelled testimony, as well as the Fourth Amendment's prescription against unreasonable searches and seizures.<sup>83</sup> The Court came to that conclusion even though the documents at issue in *Boyd* were merely invoices used to prove fraudulent importation of goods.<sup>84</sup> As Professor William Stuntz has noted, that holding, if allowed to stand, would have doomed the modern regulatory state.<sup>85</sup> Without the ability to readily obtain the

---

<sup>82</sup>116 U.S. 616 (1886).

<sup>83</sup>*Id.* at 621-22.

<sup>84</sup>*Id.* at 618.

<sup>85</sup>William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 Yale L.J. 393, 428 (1995).

records of corporations, partnerships and the like, government agencies could not have done their job of ensuring that corporate tax laws, bank laws, securities laws, and a host of other regulatory statutes were enforced.

For precisely that reason, within twenty years the Court had reversed itself. In *Hale v. Henkel*,<sup>86</sup> deciding in 1906, the Court rejected the interpretation of the Fifth Amendment that it had adopted in *Boyd*, and limited the Fourth Amendment's relevance in subpoena cases to a prohibition of overbroad requests. Acceptance of the corporation's Fifth Amendment claim, the Court stated, "would practically nullify the whole act of Congress. Of what use would it be for the legislature to declare these combinations unlawful if the judicial power may close the door of access to every available source of information upon the subject?"<sup>87</sup> For similar reasons, the Fourth Amendment did not prevent use of a subpoena duces tecum to compel the production of documentary evidence. Quoting an English decision, the Court stated, "it would be 'utterly impossible to carry on the administration of justice' without this writ."<sup>88</sup>

The move toward the current regime of virtually unlimited subpoena power was not immediate, however. In *FTC v. American Tobacco Co.*,<sup>89</sup> decided in 1924, a unanimous Court held that federal antitrust law required the Federal Trade Commission to provide "[s]ome evidence of the materiality of the papers demanded" by an administrative subpoena.<sup>90</sup> Although

---

<sup>86</sup>201 U.S. 43 (1906).

<sup>87</sup>*Id.* at 70 (quoted in Stuntz, *supra* note , at 429).

<sup>88</sup>*Id.* at 73 (quoting *Summers v. Moseley*, 2 Cramp. & M. 477).

<sup>89</sup>264 U.S. 298 (1924).

<sup>90</sup>*Id.* at 306.

the holding was based on an interpretation of a statute, the Court, per Justice Holmes, also stated that “[a]nyone who respects the spirit as well as the letter of the Fourth Amendment would be loath to believe that Congress intended to authorize one of its subordinate agencies to sweep all our traditions into the fire and to direct fishing expeditions into private papers.”<sup>91</sup> Other Supreme Court and lower court cases exhibited similar resistance to blind sanctioning of subpoenas administered by agencies.<sup>92</sup>

By the mid-1940s, however, the Court had carried through to its logical conclusion *Hale’s* assertion that significant restrictions on the government’s subpoena power would unduly stymie regulatory investigative efforts. In 1946 in *Oklahoma Press Co. v. Walling*,<sup>93</sup> the Court canvassed the relevant authorities and concluded that “the Fifth Amendment affords no protection by virtue of the self-incrimination provision, whether for the corporation or for its officers; and the Fourth, if applicable, at the most guards against abuse only by way of too much indefiniteness or breadth in the things required to be ‘particularly described,’ if also the inquiry is one the demanding agency is authorized by law to make and the materials specified are relevant.”<sup>94</sup> *Walling* even insinuated that a subpoena is not an “actual search” meriting fourth

---

<sup>91</sup>Id. at 305-06.

<sup>92</sup>See, e.g., *Jones v. Securities & Exchange Comm.* 298 U.S. 1, 27 (1936)(“An investigation not based upon specified grounds is quite as objectionable as a search warrant not based upon specific statements of fact.”); *FTC v. Smith*, 34 F.2d 323, 324-25 (S.D.N.Y. 1929)(requiring probable cause before a subpoena could be enforced); *FTC v. P. Lorillard Co.*, 283 F. 999, 1006 (S.D.N.Y. 1922), *aff’d* on other grounds, 264 U.S. 298 (1924)(same).

<sup>93</sup>327 U.S. 186 (1946).

<sup>94</sup>Id. at 208.

amendment protection.<sup>95</sup> Although this dictum was glossed over four years later in *United States v. Morton Salt Co.*,<sup>96</sup> the Court adhered to the notion that “it is sufficient if the inquiry is within the authority of the agency, the demand is not too indefinite and the information sought is reasonably relevant.”<sup>97</sup> Indeed, “[e]ven if one were to regard the request for information in this case 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.”<sup>98</sup> In *United States Powell*,<sup>99</sup> decided in 1964, the Court reiterated that a government agency subpoena for records is valid if the records are “relevant” to an investigation conducted for a “legitimate purpose” (meaning one authorized by statute).<sup>100</sup> As applied, the *Powell* relevance standard is extremely easy to meet.<sup>101</sup>

All of these cases involved government attempts to obtain corporate or other business documents. Throughout the first half of the twentieth century, the Court had intimated that

---

<sup>95</sup>Id. at 195 (“the records in these cases present no question of actual search and seizure, but raise only the question whether orders of court for the production of specified records have been validly made.”).

<sup>96</sup>338 U.S. 632, 651-52 (1950).

<sup>97</sup>Id. at 652.

<sup>98</sup>Id.

<sup>99</sup>397 U.S. 48 (1961).

<sup>100</sup>Id. at 57-58. See

<sup>101</sup>See, e.g., *United States v. Hunton & Williams*, 952 F.Supp. 843, 854 (3d Cir. 1995)(the *Powell* inquiry is more deferential than the “arbitrary and capricious” standard of review for agency action under the Administrative Procedure Act); *United States v. LaSalle Nat’l Bank*, 437 U.S. 298, 316 (1978)(bad faith on the part of an individual bureaucrat insufficient to invalidate administrative subpoena under *Powell*).

subpoenas for private records might have to meet a higher standard. For instance, in *Hale* the Court stated “there is a clear distinction [in cases involving demands for production of books and papers] between an individual and a corporation.”<sup>102</sup> While a corporation “is a creature of the state,” “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,” an individual “owes no such duty to the state, since he receives nothing therefrom, beyond the protection of his life and property.”<sup>103</sup> Thus, in contrast to the corporation, an individual retains the right to refuse “to criminate himself and *the immunity of himself and his property from arrest or seizure except under a warrant of the law.*”<sup>104</sup> Forty-five years later, in *Morton Salt*, the Court made similar statements.

[C]orporations can claim no equality with individuals in the enjoyment of a right to privacy. They are endowed with public attributes. They have a collective impact upon society, from which they derive the privilege of acting as artificial entities. The Federal Government allows them the privilege of engaging in interstate commerce. Favors from government often carry with them an enhanced measure of regulation.<sup>105</sup>

Nonetheless, in *Ryan v. United States*,<sup>106</sup> decided the same day as *Powell*, the Court made clear that the minimal *Powell* requirements governed subpoenas for private tax records as well.

---

<sup>102</sup>201 U.S. at 74.

<sup>103</sup>*Id.*

<sup>104</sup>*Id.* (emphasis added).

<sup>105</sup>338 U.S. at 652

<sup>106</sup>379 U.S. 61 (1964).

The Court reached this conclusion, it stated, “for the reasons given in [*Powell*],”<sup>107</sup> without further discussion. Unfortunately, *Powell*’s holding that probable cause need not be demonstrated to obtain corporate tax records rested solely on an interpretation of the relevant statutory language.<sup>108</sup> The opinion did not even mention the fourth amendment (although it did cite *Oklahoma Press* and *Morton Salt*).<sup>109</sup> Thus, with one perfunctory statement that did not purport to address constitutional concerns, the Court seemed to obliterate the distinction between corporate and private records.

The possibility of constitutional protection for personal records was further reduced by a pair of Supreme Court decisions in 1976. One of these decisions, *Miller*, has already been described;<sup>110</sup> it eliminated fourth amendment protection of documents held by institutional third parties. The second decision, *Fisher v. United States*,<sup>111</sup> dramatically reoriented the Court’s interpretation of the fifth amendment, in a way that further enhanced the government’s subpoena power vis-a-vis personal records. Earlier subpoena cases, it will be remembered, dismissed fifth amendment claims on the ground that they would make government regulation unfeasible.<sup>112</sup> In *Fisher*, the Court concocted a different reason for concluding that subpoenas normally do not violate the Fifth Amendment. According to the Court, subpoenas do not implicate that

---

<sup>107</sup>Id. at 62.

<sup>108</sup>Id. at 52-56.

<sup>109</sup>Id. at 57.

<sup>110</sup>See supra text accompanying notes .

<sup>111</sup>425 U.S. 391 (1976).

<sup>112</sup>See supra text accompanying notes .

amendment’s prohibition of compelled self-incrimination either because they do not compel information or because the information they compel is not self-incriminating.

The Court’s decision in *Fisher* is usefully divided into three holdings. First, the Court noted, a subpoena does not force the *creation* of documents, and thus the disclosure of document content that is demanded by a subpoena is not compulsion implicating the Fifth Amendment.<sup>113</sup> Second, *Fisher* held, while the act of *producing* documents *is* compelled by a subpoena, documents that are compelled from a third party, such as an accountant, does not compel the *target* to produce them, and thus does not implicate his Fifth Amendment rights.<sup>114</sup> Third, even if a subpoena is directed at the target, it does not compel any *incriminating* information when proof of the source of the documents is not an important element of the prosecution’s proof (which is often the case).<sup>115</sup> Although *Fisher* involved business documents of a sole proprietor, the Court later made clear that *Fisher*’s first holding eradicates fifth amendment protection for the contents of *all* papers, personal as well as business.<sup>116</sup> Likewise, the second and third holdings in *Fisher* indicate that the act of producing *any* papers, business-oriented or personal,

---

<sup>113</sup>Id. at 409-410.

<sup>114</sup>Id. at 397, 405. The Court did hold that compelling documents from a person’s attorney might implicate the attorney-client privilege, however. Id. at 404-05.

<sup>115</sup>Normally in tax cases, for instance, “[t]he existence and location of the papers are a foregone conclusion and the taxpayer adds little or nothing to the sum total of the Government’s information by conceding that he in fact has the papers.” Id. at 411.

<sup>116</sup>In *United States v. Doe*, 465 U.S. 605 (1984), which rejected a Fifth Amendment challenge of a subpoena for the defendant’s business records from the defendant himself, Justice O’Connor felt able to state that “the Fifth Amendment provides absolutely no protection for the contents of private papers of any kind.” Id. at 618 (O’Connor, J., concurring). Although *Fisher* had suggested its holding might not apply to “personal diaries,” 425 U.S. at 401 n. 7, it referenced only the fourth amendment in making this caveat.

does not implicate the Fifth Amendment when those papers come from a third party, or when the government can prove a link between the papers and the target in some other way.

Despite these decisions from the Supreme Court, in the 1990s a few lower courts signaled an unwillingness to equate corporate and private records. Most prominent in this regard was the First Circuit's opinion in *Parks v. FDIC*.<sup>117</sup> There a three-judge panel, relying on *American Tobacco*, held that the fourth amendment requires the agency to "articulate a reasonable suspicion of wrongdoing" by the target when the government seeks personal financial records.<sup>118</sup> However, the *Parks* decision was later withdrawn by the First Circuit,<sup>119</sup> and no other court has been willing to go as far, at least where private financial records are concerned.<sup>120</sup> The only situations in which the lower courts have placed more than minimal fourth amendment restrictions on subpoenas for personal records have involved government attempts to determine whether the targets have sufficient funds to justify pursuit of claims against them,<sup>121</sup> and

---

<sup>117</sup>65 F.3d 207 (1<sup>st</sup> Cir. 1995), withdrawn for N.R.S. 64 USLW 2166.

<sup>118</sup>*Id.* at \*8.

<sup>119</sup>64 USLW 2166.

<sup>120</sup>In dictum, the court in *FDIC v. Wentz*, 55 F.3d 905, 908 (3d Cir.1995), stated: "When personal documents of individuals, as contrasted with business records of corporations, are the subject of an administrative subpoena, privacy concerns must be considered." Yet, at least with respect to private financial records, courts have held otherwise. See *In re Administrative Subpoena John Doe, D.P.M.*, 253 F.3d 256, 269 (6<sup>th</sup> Cir. 2001).

<sup>121</sup>*Resolution Trust Corp. v. Walde*, 18 F.3d 943, 946 (D.C. Cir. 1994); *Freese v. FDIC*, 837 F.Supp. 22, 24 (D.N.H. 1993).

government attempts to obtain the records of third parties who are not the target of the investigation.<sup>122</sup>

The foregoing historical account has focused almost entirely on the legality of administrative subpoenas. Subpoenas issued by grand juries are subject to even fewer constraints. While overbreadth objections sometimes succeed, grand jury subpoenas are virtually never quashed on irrelevance grounds.<sup>123</sup> Some lower courts have required more substantial proof of relevance when the grand jury subpoena seeks a particularly intrusive action, such as a blood test.<sup>124</sup> And a few courts have imposed some limitations on subpoenas on non-constitutional grounds. For instance, the Third Circuit has invoked its supervisory power to require proof that documents and witnesses sought through grand jury subpoenas contain

---

<sup>122</sup>In re McVane, 44 F.3d 1127 (2d Cir. 1995) (“administrative subpoenas issued pursuant to an agency investigation into corporate wrongdoing, which seek personal records of persons who are not themselves targets of the investigation and whose connection to the investigation consists only of their family ties to corporate participants, must face more exacting scrutiny than similar subpoenas seeking records solely from corporate participants.”). Cf. Doe v. United States, 253 F.2d 256, 270-71 (6<sup>th</sup> Cir. 2001) (reluctantly approving subpoena for financial records of suspect’s children); United States v. Harrington, 388 F.2d 520, 523 (2d Cir. 1968) (“judicial protection against the sweeping or irrelevant order is particularly appropriate in matters where the demand for records is directed not to the [target] but to a third-party who may have had some dealing with the person under investigation”). Interestingly, cases dealing with issues outside the subpoena context have recognized a possible *fourteenth* amendment privacy interest in “medical, financial and other personally intimate data.” Vega-Rodriguez v. Puerto Rico Telephone Co., 110 F.3d 174, 183 (1<sup>st</sup> Cir. 1997).

<sup>123</sup>See Blair v. United States, 250 U.S. 273, 282 (1919) (a grand jury witness “is not entitled to urge objections of incompetency or irrelevancy, such as a party might raise, for this is no concern of his.”). Cf. United States v. Mara, 410 U.S. 19, 20-22 (1973) (rejecting lower court holding that the Fourth Amendment requires a showing of relevance or reasonableness in order to obtain handwriting exemplars).

<sup>124</sup>See, e.g., Woolverton v. Multi-County Grand Jury, Okla. Cty., 859 P.2d 1112 (Okla. Crim. App. 1993).

information that is reasonably relevant to a legitimate investigation.<sup>125</sup> Most courts have rejected even this relatively lenient standard, however, because grand jury secrecy would be compromised by forcing the prosecution to make a preliminary showing of relevancy and because relevancy may not always be demonstrable during the early stages of an investigation.<sup>126</sup>

The Supreme Court lent its weight to the latter point of view in *United States v. R. Enterprises, Inc.*,<sup>127</sup> where it held that, in light of its traditionally wide-ranging investigative powers and the need for secrecy, the grand jury “may compel the production of evidence or the testimony of witnesses as it considers appropriate.”<sup>128</sup> Thus, under the federal rules, a grand jury 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.”<sup>129</sup> Further, the target of the subpoena bears the burden of persuasion on the irrelevancy issue, although the prosecution may occasionally be required to reveal “the general subject of the grand jury’s investigation” to aid the challenging party in trying to meet that burden.<sup>130</sup>

To sum up the foregoing, with a few exceptions, substantive challenges to subpoenas are extremely unlikely to succeed. The fifth amendment is not a bar to government attempts to seek

---

<sup>125</sup>In re Grand Jury Proceedings (Schofield I), 486 F.2d 85 (3d Cir. 1973).

<sup>126</sup>See generally, LaFave et al., supra note , at 149.

<sup>127</sup>498 U.S. 292 (1991).

<sup>128</sup>Id. at 298 (quoting *United States v. Calandra*, 414 U.S. 338, 343 (1974)).

<sup>129</sup>Id. at 301.

<sup>130</sup>Id. at 302.

records unless the act of production is self-incriminating. The fourth amendment does not prohibit such attempts unless they seek only clearly irrelevant evidence or are unduly burdensome. Although some courts have imposed somewhat more stringent, non-constitutional limitations on subpoenas, most have not.

## 2. A Critique of Subpoena Law

The most common explanation for the relaxed standards associated with subpoenas is the one advanced originally in *Hale*: a higher standard would make government regulation impossible. This rationale appears most commonly in cases justifying administrative subpoenas issued by government agencies. Judge Selya's dissent in *Parks*, the subsequently-withdrawn First Circuit case which recognized greater protection for private papers, is a modern pronouncement of the claim:

Administrative investigations differ significantly from criminal investigations: government agencies typically investigate in order to enforce compliance with complicated structures of economic regulation. The ability to obtain information from regulated parties and those persons in privity with them typically is vital to the success of the regulatory scheme. See *United States v. Morton Salt Co.* . . . ; *Oklahoma Press* . . . . And 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. . . . This incipient problem--the need to hitch the horse in front of the cart--is frequently exacerbated because the subpoena power has great significance for most administrative agencies in the conduct of important public business.<sup>131</sup>

This rationale is a dangerous one, of course, for the government can always make pleas that the fourth amendment and other constitutional rights make its law enforcement job

---

<sup>131</sup>65 F.3d 207, \*11 (1<sup>st</sup> Cir. 1995).

difficult.<sup>132</sup> Even accepting the rationale on its face, however, it at most explains minimal restrictions on subpoenas for business records and—at a stretch—for private financial records of individuals associated with “complex economic activity” that is subject to administrative regulation. It does not explain why subpoenas as currently conceptualized should authorize compulsory record production in connection with ordinary “criminal investigations” (to use Judge Selya’s language).

Perhaps the justices and judges who adopt this rationale believe that administrative subpoenas are seldom used in such investigations. But the Department of Justice not only relies on such subpoenas to investigate antitrust violations,<sup>133</sup> government fraud,<sup>134</sup> and the like but also authorizes subpoenas to obtain records in connection with child kidnapping and pornography cases,<sup>135</sup> false claims and bribery,<sup>136</sup> health care fraud,<sup>137</sup> racketeering,<sup>138</sup> and possession or sale of controlled substances.<sup>139</sup> The Department is not shy about using this subpoena authority. In 2001, the Department issued almost 1,900 subpoenas seeking Internet records concerning child

---

<sup>132</sup>Cf. *United States v. Martinez-Fuerte*, 428 U.S. 523, 575 (1976) (Brennan, J., dissenting) (“There is no principle in the jurisprudence of fundamental rights which permits constitutional limitations to be dispensed with merely because they cannot be conveniently satisfied.”).

<sup>133</sup>15 U.S.C. §1311-1314

<sup>134</sup>5 U.S.C. App. 3, § 6(a)(4)

<sup>135</sup>18 U.S.C. § 348(a)(1)(A)(i)(II), (a)(1)(C)(email subscriber information only).

<sup>136</sup>31 U.S.C. § 3733

<sup>137</sup>18 U.S.C. § 3486

<sup>138</sup>18 U.S.C. § 1968

<sup>139</sup>21 U.S.C. § 876(a)

exploitation and abuse,<sup>140</sup> and a total of 2,102 subpoenas seeking bank, medical and other records in connection with health care offenses.<sup>141</sup> (Information about the number of DOJ subpoenas issued in connection false claims, bribery, racketeering, and controlled substance investigations is not available).

Whatever might be the case with respect to complex economic wrongdoing, the claim that these latter types of crimes are “impossible” to investigate without subpoena power is not true. In most such cases, documents are secondary to other evidence obtained through interviews and interrogations, searches of homes and effects, and other non-documentary investigative techniques.<sup>142</sup> Even with respect to those individual crimes that depend on transactional proof, such as fraud, tax evasion, and computer hacking, development of individualized suspicion is generally easier than in regulatory cases where the chain of command hides responsibility, proof can involve very complex, technical evidence, and non-documentary evidence of crime may literally be non-existent.<sup>143</sup>

---

<sup>140</sup>U.S. Dep’t of Justice, Office of Legal Policy, Report to Congress on the Use of Administrative Subpoena Authorities by Executive Branch Agencies and Entities 37 (2002).

<sup>141</sup>Id. at 34-35. Note, however, that many subpoenas for medical records are in aid of investigations aimed at pharmacists or doctors for violations of controlled substances or health fraud laws. In such cases, privacy concerns may well be absent, because the information sought need not be linked to a particular patient.

<sup>142</sup>Even in business investigations, this is often the case. See, e.g., *U.S. v. Goldfine*, 538 F.2d 815, 818-819 (9<sup>th</sup> Cir. 1976) (where court notes that agency carrying out administrative inspection had developed probable cause to believe pharmacists were violating the Comprehensive Drug Prevention and Control Act based on reports of large shipments of controlled substances to the pharmacy, tracing of certain shipments, surveillance of the pharmacy, and arrest of some of the pharmacy’s customers).

<sup>143</sup>Compare this recent summary of the problems associated with corporate investigation to investigation of “ordinary” crime:

A version of the impossibility rationale is also found in cases justifying the even more relaxed standards for subpoenas issued by grand juries. A constant refrain in grand jury cases is the notion that “the public has a right to every man’s evidence.”<sup>144</sup> In *United States v. Dionisio*,<sup>145</sup> the Supreme Court baldly stated that this right exists simply because it is “necessary to the administration of justice.”<sup>146</sup> Thus, the Court concluded, grand jurors must have the capacity to “run down every available clue” and to examine “all witnesses . . . in every proper way.”<sup>147</sup>

Put in historical perspective, however, this statement should not be interpreted to eliminate restrictions on grand jury subpoenas for personal documents. The early focus of grand juries was government misconduct and corruption,<sup>148</sup> which later expanded to business crime

---

Despite the seemingly broad liability made possible by respondeat superior, it is notoriously difficult to prosecute corporations for violations of specific intent crimes. First, corporate crime is highly concealable, typically because victims are unaware of their injury. Even when crime is revealed, it is challenging to identify within an organization a particular guilty actor.

Stacey Neumann Vu, *Corporate Criminal Liability: Patchwork Verdicts and the Problem of Locating a Guilty Agent*, 104 Colum. L. Rev. 459, 467-68 (2004). See also F. Cullen, W. Maakestad & G. Cavender, *Corporate Crime Under Attack* 352 (1987) (“the labyrinthian structure of many modern corporations often makes it extremely difficult to pinpoint individual responsibility for specific decisions”).

<sup>144</sup>*Branzburg v. Hayes*, 408 U.S. 665, 688 (1972), citing *United States v. Bryan*, 339 U.S. 323, 331 (1950); *Blackmer v. United States*, 284 U.S. 421, 438 (1932); *Blair v. United States*, 250 U.S. 273, 281 (1919).

<sup>145</sup>410 U.S. 1 (1973).

<sup>146</sup>*Id.* at 10.

<sup>147</sup>*Id.* at 13.

<sup>148</sup>See LaFave et al., *supra* note , at 13-14 (describing the “public watchdog” function of the grand jury during the eighteenth and nineteenth centuries).

(*Hale* involved a grand jury subpoena). Like the administrative inquiries discussed above, these types of investigations involve attempts to obtain *organizational* rather than personal information. As *Hale* demonstrated, early on the Court did not think that grand jury access to personal records should be so simple. And *Dionisio* itself cited *Boyd* in affirming that the grand jury “cannot require the production by a person of private books and records that would incriminate him.”<sup>149</sup> Thus, while the Court was willing to approve the use of subpoenas to compel non-testimonial voice exemplars, which was the practice challenged in *Dionisio*,<sup>150</sup> it strongly implied that documents should be treated differently.

*Fisher*, decided three years after *Dionisio*, has changed the legal landscape, however. While the witness that *Dionisio* states can be examined “in every proper way” can still avoid testifying by claiming the fifth amendment privilege,<sup>151</sup> that privilege is pretty much eliminated for documents. Information that the government could obtain from a witness only through a grant of immunity, or from a search of a residence or business only if it has probable cause, can now be obtained through a subpoena issued on the sayso of the prosecutor or agency bureaucrat running the investigation.

Perhaps conscious of this loophole even back when only organizational documents could be subpoenaed, some courts have felt the need to bolster the impossibility rationale with other justifications for the lack of standards connected with subpoenas *duces tecum*. The most

---

<sup>149</sup>410 U.S. at 11.

<sup>150</sup>*Id.* at 7 (“The voice recordings were to be used solely to measure the physical properties of the witnesses' voices, not for the testimonial or communicative content of what was to be said.”).

<sup>151</sup>*Counselman v. Hitchcock*, 142 U.S. 547, 586 (1892); *United States v. Washington*, 431 U.S. 181, 186 (1977)(reaffirming *Counselman* after *Fisher*).

prominent such justification was suggested in *Oklahoma Press*. Subpoenas do not trigger “actual searches,” the Supreme Court said in that case, because they do not require a physical intrusion; rather, they are at most “constructive” searches carried out by the target him or herself.<sup>152</sup> In his concurrence in *Hale*, which concluded that the fourth amendment should not even prohibit overbreadth, Justice McKenna made a similar contention. He argued that, in contrast to a traditional search, the subpoena does not involve “trespass or force” and “cannot be finally enforced except after challenge.”<sup>153</sup>

If the scope of the fourth amendment is to be determined with reference to reasonable expectations of privacy, this second, lesser-intrusion rationale for the paltry restrictions on subpoenas also fails. The fact that it is the target (or a third party) rather than the police who locates the documents does not change the nature of what is revealed, which can often be very intimate information. And the target’s ability to challenge a subpoena, while it may inhibit some fishing expeditions, at most will only delay government access to the records, unless something beyond the current relevance standard is applicable; recall also that, for many types of transaction surveillance, the target has *no* right of challenge.<sup>154</sup> The reasoning in *Oklahoma Press* and Justice McKenna’s *Hale* concurrence assumes that one only feels violated or embarrassed when the government physically invades one’s property. If that were true, most modern communications and physical surveillance would not be a search, since neither usually

---

<sup>152</sup>327 U.S. at 195, 202.

<sup>153</sup>201 U.S. at 80.

<sup>154</sup>See supra text accompanying notes .

requires a trespass or use of force. As the Supreme Court has recognized, however obliquely,<sup>155</sup> subpoenas duces tecum are searches that implicate the fourth amendment.

That should not mean that all subpoenas need to be based on probable cause. Not all records are equally private. In particular, business records—precisely the type of records involved in all but one of the Supreme Court’s subpoena cases—are much less personal than individual medical, financial and email records. As noted earlier, the Court recognized as much in *Morton Salt*, when it stated “corporations can claim no equality with individuals in the enjoyment of a right to privacy.”<sup>156</sup> The Court has made similar statements about the impersonal nature of business records in several other cases.<sup>157</sup> Records of other types of entities—labor unions, for example—would probably fit in the same category.<sup>158</sup> If these observations are

---

<sup>155</sup>U.S. v. Morton Salt Co., 338 U.S. 632, 651-52 (1950) (“the 'right to be let alone . . . is not confined literally to searches and seizures as such, but extends as well to the orderly taking under compulsion of process.”); *Hale v. Henkel*, 201 U.S. 43, 76 (1906) (“we do not wish to be understood as holding that a corporation is not entitled to immunity, under the 4th Amendment, against unreasonable searches and seizures.”).

<sup>156</sup>*Id.* at 652.

<sup>157</sup>U.S. v. Biswell, 406 U.S. 311, 316 (1972) (“When a dealer chooses to engage in this pervasively regulated business and to accept a federal license, he does so with the knowledge that his business records, firearms, and ammunition will be subject to effective inspection.”); *Bellis v. U.S.*, 417 U.S. 85, 90, 100 (1971)(describing organizational information as “impersonal records and documents,” although noting the distinction between “group” and “personal” interests is difficult and not particularly helpful, at least in fifth amendment cases).

<sup>158</sup>*Cf.* *Braswell v. United States*, 487 U.S. 99, 107-08 (1988) (“the test . . . is whether one can fairly say under all the circumstances that a particular type of organization has a character so impersonal in the scope of its membership and activities that it cannot be said to embody or represent the purely private or personal interests of its constituents, but rather to embody their common or group interests only. . . . Labor unions--national or local, incorporated or unincorporated--clearly meet that test.”).

accepted, however, *Ryan* is wrongly decided; private tax records should not be equated with corporate records.<sup>159</sup>

A third and final reason sometimes given in support of a relaxed standard for subpoenas duces tecum relies on a comparison with subpoenas ad testificandum. As one court put it, since a witness who is subpoenaed to testify has “no right of privacy . . . absent some recognized privilege” and thus must often put up with “unwelcome disclosure of his personal affairs”, “a witness subpoenaed to produce his records . . . may not assert his Fourth Amendment expectation of privacy in such records.”<sup>160</sup> Resistance to disclosure of records, this rationale states, should be countenanced only to the extent resistance to answering questions is permitted. But, as noted above (and as the quoted court itself recognizes), grand jury and other subpoenaed witnesses *can* resist testifying, by asserting the Fifth Amendment, whereas after *Fisher* there is no significant privilege protection for documents. Even if we assume testimony can be compelled under certain circumstances, the comparison between testimony and documents proves too much. The fact that the government may be able to compel a witness to describe the

---

<sup>159</sup>One of the principal assumptions Professor Stuntz relies on to bolster his argument that privacy should not be the linchpin of Fourth Amendment analysis is the assertion, noted above, that a privacy-orientation would stultify the regulatory state. See *supra* text accompanying note . . . See also William J. Stuntz, *Privacy’s Problem and the Law of Criminal Procedure*, 93 Mich. L. Rev. 1016, 1032 (1995). Yet if business records are considered less private than personal ones, the regulatory state can easily co-exist with a regime that values privacy and that protects individual’s records more fully than it does business records. Stuntz is particularly concerned that reversal of *Ryan* would mean the end of tax audits. *Id.* at 1019, 1035, 1037, 1039, 1042, 1046. That would depend on whether the audits are truly random. If instead they are based on factors that correlate with fraud or involve clear miscalculations, probable cause would usually exist. See discussion of data mining, *infra* text accompanying notes . . . Privacy should remain the linchpin of the fourth amendment because, among other reasons, that focus provides an important distinction between organizational and individual records.

<sup>160</sup>*State ex rel., Pollard v. Criminal Court*, 263 Ind. 236, 329 N.E. 573 , 585 (1975).

contents of his house and effects does not mean it can search those areas without a warrant, yet the latter result is precisely what the current law on subpoenas duces tecum allows.<sup>161</sup>

Of course, many witnesses subject to subpoena are not the targets of the investigation and thus will not want or need to assert the Fifth Amendment. Thus, a variation of the foregoing justification for the current subpoena regime that would apply when records are requisitioned from a source other than the target is as follows: Because the government can compel third party witnesses to reveal information about a target without demonstrating any suspicion regarding the target, it should be able to obtain records from a third party under the same circumstances. If this amended attempt to compare subpoenas ad testificandum and subpoenas duces tecum works, it would justify the lion's share of grand jury and administrative subpoenas, since most are directed at third parties.

But this comparison does *not* work. The first difference between a third party witness and a record-holder is the way they come by their knowledge of "private" information. The witness will be describing information that the target could have refrained from revealing, simply by not talking or by avoiding being seen. In contrast, the record-holder will have information that the target had no meaningful choice but to reveal. As critics of *Miller* and similar decisions have pointed out,<sup>162</sup> participation in modern society *requires* giving information

---

<sup>161</sup>Of course, a subpoena is not the investigative tool of choice in many situations, given the possibility that the subpoenaed target is likely to destroy the sought items rather than hand them over. But that does not change the fact that a subpoena, when obeyed, does permit government to spy on the content of one's home. And when a citizen obeys the demand for evidence incorporated in subpoena, the outcome is little different from a compelled confession, as *Boyd* recognized.

<sup>162</sup>See, e.g., *United States v. Miller*, 425 U.S. at 451 (Brennan, J., dissenting) ("the disclosure by individuals or business firms of their financial affairs to a bank is not entirely

to banks and phone companies, hospitals and government agencies. The reason record-holders possess the information about us that they do is because we have to give it to them; that fact hardly supports the conclusion that we have surrendered our privacy interest in it.

The second difference between a witness and a record-holder focuses specifically on the institutional nature of the latter. Professor Coombs has persuasively argued that people in possession of information about others, even if the information is “private” and is obtained through an intimate relationship, have “an autonomy-based right to choose to cooperate with the authorities.”<sup>163</sup> As Professor Coombs notes, “[t]o deny even the possibility of such a decision [to cooperate] is to turn a freely chosen relationship into a status, denying one person’s full personhood to protect another’s interests.”<sup>164</sup> In other words, the autonomy interest of a putative witness trumps the privacy interest of a putative target when a witness decides to reveal information about the target.

That analysis makes sense when the third party is a person. But most records are held by institutions, not people. And institutions do not have autonomy interests. A bank, hospital, or Internet provider is not denied its “personhood” when its ability to turn information over to the government is restricted. Accordingly, the analogy between third party witnesses and third party record-holders fails.

---

volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account.”)

<sup>163</sup>Mary Irene Coombs, *Shared Privacy and the Fourth Amendment, or The Rights of Relationships*, 75 Cal. L. Rev. 1593, 1643 (1987).

<sup>164</sup>*Id.* at 1644.

This view of how third party autonomy interests are relevant to Fourth Amendment analysis also provides a different perspective on the Supreme Court's decisions in *Miller* and *Smith*. In concluding in those two cases that people have no expectation of privacy in information surrendered to banks and phone companies, the Court relied on earlier decisions which had held that one assumes the risk one's acquaintances are government informants.<sup>165</sup> Many commentators have argued that both sets of decisions are wrong, because we should be able to expect that government will not turn either our social or our business relationships into investigative tools without some justification.<sup>166</sup> Even if, relying on Professor Coombs analysis, one accepts the "social undercover agent" cases as valid precedent, however, they are distinguishable from the "institutional undercover agent" cases like *Miller* and *Smith*, because social agents have an autonomy interest that institutional agents lack. In cases involving the latter scenario, there is no third party interest to trump the target's interest in privacy, which should therefore be accorded greater respect than it is under current subpoena jurisprudence.

\* \* \*

---

<sup>165</sup>Miller, 425 U.S. at 443 ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, 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.") (citing *United States v. White*, 401 U.S. 745 (1971); *Hoffa v. United States*, 385 U.S. 293 (1966); *Lopez v. United States*, 373 U.S. 427 (1963)).

<sup>166</sup>See, e.g., James J. Tomkovicz, *Beyond Secrecy for Secrecy's Sake: Toward an Expanded Vision of the Fourth Amendment Privacy Province*, 36 *Hastings L.J.* 645, 728 (1985) (describing the logic of the "false friend" cases as "fundamentally defective and exceedingly dangerous to liberty."). I have made similar arguments, at least when the false friend is a person who has been importuned by the government to be an informant rather than, as discussed in the text, one who makes contact with the police after the legally relevant event occurs. See Slobogin, *supra* note , at 103-06.

If the contents of personal records are entitled to more Fourth Amendment protection than the contents of organizational records, then subpoenas demanding personal records issued on a mere relevance showing or something less should be unconstitutional. That conclusion only sets the justificatory floor, however. It does not tell us whether subpoenas for papers must be based on probable cause. While the Fourth Amendment usually requires that standard for searches of “persons, houses, papers, and effects,” when it comes to demands for “papers,” a distinction should be made depending upon whether they are “private” or “public” papers.

#### B. Private v. Public Records

If personal papers are held by the target, probable cause should be required before the government can obtain them, a rule the fourth amendment would seem to require on its face. For the reasons just suggested, the same protection is warranted for documents held by institutional third parties, with one significant exception. When the records can justifiably be called “public” records—records that belong to the public—then 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. Public entities include hospitals, schools and libraries, as well as courthouses and government agencies. And even government agencies can house records that are more personal than public.

How can we determine when public records are not really public and therefore deserving of full fourth amendment protection? Fortunately, litigation in connection with the federal Freedom of Information Act and similar state statutes has already ploughed this ground. While these laws establish a presumption in favor of disclosure of records held by government agencies, 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,”<sup>167</sup> “personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy,”<sup>168</sup> and law enforcement records to the extent they include information that “could reasonably be expected to constitute an unwarranted invasion of personal privacy.”<sup>169</sup> 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

---

<sup>167</sup>5 U.S.C. 552(b)(4). Many circuits have held that voluntarily submitted information 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 F.2d 871, 872 (D.C. Cir. 1992), cert denied 507 US 984 (1992). See generally 139 ALR Fed 225.

<sup>168</sup>5 U.S.C. §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; redaction of identifying names may be sufficient. *Department of Air Force v Rose*, 425 US 352, 381-82 (1976). See generally 106 ALR Fed 94.

<sup>169</sup>*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.*, 489 U.S. 749, 774 (1989). See generally 52 ALR Fed 181.

disclosure some types of motor vehicle registration information,<sup>170</sup> identifying information relating to health care provided by the state,<sup>171</sup> credit information held by state agencies,<sup>172</sup> and educational records.<sup>173</sup> In many states, some types of licensing information are also often exempt from disclosure.<sup>174</sup>

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 marriage and divorce papers, real estate documents and court proceedings without articulating a

---

<sup>170</sup>Fl. Stat. § 119.07(aa)

<sup>171</sup>Id. at (bb), (cc), & (hh).

<sup>172</sup>Id. at (dd).

<sup>173</sup>Fla. Stat. § 1002.22(d)

<sup>174</sup>See, e.g., *Mager v. State Dep't of Police*, 595 N.W.2d 142, 143 (1999) (holding that “gun ownership is information of a personal nature” requiring exemption from the state freedom of information act).

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.<sup>175</sup>

### 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 include descriptors of communications and transmissions, such as phone numbers dialed, the addresses that route emails, the Uniform Resource Locators (URLs) of websites visited, 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.

On the other hand, 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 billing records, credit card and bank account numbers used for payment, and the true identity of those using pseudonyms.<sup>176</sup> This kind of information does not describe the communication but rather represents the business deal that is made between the customer and the service providers, and as such is content about that relationship. Furthermore, some of this information will reveal information about communication content. For instance, law enforcement

---

<sup>175</sup>Note that this procedure is no more onerous, from the law officer’s perspective, than the current pen register regime. See supra text accompanying note .

<sup>176</sup>See supra

may already know that a particular anonymous chat room message came from a particular computer, so that finding out the identity of the person behind the pseudonym will allow it to link that person to the message.<sup>177</sup>

Even so limited, this type of information can be quite revealing. In the aggregate, it could identify all of a person's connections with the world.<sup>178</sup> Even so, catalogic data should probably not be entitled to as much protection as the content of communications, for two reasons.

First, as a general matter, catalogic data are 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,<sup>179</sup> 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.<sup>180</sup> And there is no doubt that pen registers, programs such as DCS-1000,

---

<sup>177</sup>See generally Note, John Alan Farmer, *The Specter of Crypto-Anarchy: Regulating Anonymity-Protecting Peer-to-Peer Networks*, 72 Fordham L. Rev. 725 (2003). One might argue that Uniform Resource Locators (URLS) and other websurfing addresses should constitute content for the same reason. Once government is able to link a person with a URL it can visit the website itself to see precisely the type of content the person has viewed. In this situation, however, the content is not created by the target but by the website owner. What government learns is analogous to what it would discover following a person as he or she travels from one building to another and observing the newspapers, magazines and organizational correspondence that one has delivered to one's home.

<sup>178</sup>See generally Stan Karas, *Privacy, Identify, 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.")

<sup>179</sup>See supra text accompanying note .

<sup>180</sup>Cf. Wayne LaFave, *The Forgotten Motto of Obsta Principis in Fourth Amendment Jurisprudence*, 29 Ariz. L. Rev. 291, 302 (1986) (bank officials do not have "direct, significant

and membership records can give the government useful evidence of our activities and beliefs.<sup>181</sup> But that evidence 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, it should not be treated in the same way content is.

The second reason for according catalogic data less fourth amendment protection than content rests on a reciprocity notion: If technological advances should not diminish our privacy, they should not enhance them either. As a wide array of thinkers have recognized,<sup>182</sup> the development of devices that can see through walls, monitor conversations from a mile away and peruse billions of records in seconds should not mean we surrender fourth amendment protection of our homes, conversations and records, regardless of our subjective expectations. If that is so, however, neither should technological advances be a basis for *increasing* fourth amendment protection by diminishing the government's ability to obtain private information. Yet that would be the impact of equating catalogic data with communication content. Before the

---

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., 1463-64 (1974)).

<sup>181</sup>Cf. *Smith v. Maryland*, 442 U.S. at 751 ("Many individuals, including members of unpopular political organizations or journalists with confidential sources, may legitimately wish to avoid disclosure of their personal contacts.") (Brennan, J., dissenting).

<sup>182</sup>Electronic Communications Privacy Act, Senate Report No. 99-541, at 3 (1986) reprinted in 1986 U.S.C.C.A.N. 3555, 3557 ("[T]he law must advance with the technology to ensure the continued vitality of the fourth amendment. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances."); *Kyllo v. United States*, 533 U.S. 27, 34 (2002) ("To withdraw protection of this minimum expectation [of privacy in the interior of the home] would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment."); James J. Tomkovicz, *Technology and the Threshold of the Fourth Amendment: A Tale of Two Futures*, 72 Miss. L.J. 317, 437 (2002) ("Technological increases in human abilities to breach confidentiality are an insufficient reason to compromise the effort to preserve original values.").

twentieth century, the government could find out virtually everything it needed to know about the nature of people's personal connections (as opposed to the substance of their communications) simply by observing which homes and businesses they visited, people to whom they talked in public, meetings they attended, and the addresses on their envelopes. The fact that technology—phones and the Internet—has made it much easier to engage in these types of contact *surreptitiously* should not automatically require government to produce more justification for finding out about them.<sup>183</sup>

Admittedly, this line of reasoning might lead to the conclusion that the fourth amendment does not apply at all to catalogic data. Because this type of information *does* have some privacy significance and *is* so easily accessible, I think otherwise. Ex parte subpoenas, certification orders and extrajudicial certifications, which are the current means of regulating access to this information if there is any regulation at all, are insufficiently restrictive because they leave the transaction surveillance decision entirely in the discretion of law enforcement, a notion that is antithetical to the fourth amendment. Because of its less sensitive nature and the reciprocity rationale, however, catalogic data ought to be accessible on less than probable cause or reasonable suspicion, at least when the access is time-limited and does not infringe First Amendment interests.<sup>184</sup> Instead, the government should be able to obtain catalogic data

---

<sup>183</sup>In the communications content context, the analogue to the impact of technology on communication descriptors is encryption. It is now possible to preclude access to a message to all but the holder of the decryption key. Sandy Sandfort, *Security Through Obscurity*, *Wired*, March 1994, at 29. Following the reasoning in the text, however, the government should still be able to access the message with a valid warrant, because it could do so before the advent of encryption.

<sup>184</sup>If the government wants to obtain catalogic information over a prolonged period, different considerations may come into play, as the Supreme Court itself has recognized in the

whenever it is articulably relevant to an investigation, an assertion the target should have the opportunity to challenge before the record is accessed unless notification would undermine the investigation.

#### D. Data Mining/Profile Information

The final transaction surveillance scenario involves data mining, where government uses 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. 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, work absenteeism, and veterinary clinics in an effort to discern unusual or suspicious symptoms and events.<sup>185</sup> The Enhanced Border Security and Visa Entry Reform Act of 2002 requires aircrafts

---

context of tracking. See *U.S. v. Knotts*, 460 U.S. 276, 284 (1983) (stating, in response to an argument that long-term tracking using an electronic beeper should constitute a search, that “if . . . dragnet type law enforcement practices should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable.”). Similarly, 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).

<sup>185</sup>See [www.geis.ha.osd.mil/GEIS/SurveillanceActivities/ESSENCE/ESSENCE.asp](http://www.geis.ha.osd.mil/GEIS/SurveillanceActivities/ESSENCE/ESSENCE.asp) (describing ESSENCE II). ESSENCE is similar to the much 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).

and sea vessels to submit departure and arrival manifests indicating the names of all alien passengers, which can be combed for suspicion travel patterns. The much more sophisticated Computer Assisted Passenger Screening System (CAPPS) combines airline passenger lists with travel reservations, rental car status, travel companions, and address.<sup>186</sup> Data mining comes in many forms, but all varieties have one thing in common: they rely on suspicionless perusal of transaction information.

The fourth amendment problem, obviously, is that once these data are linked to a particular person, the government has knowledge of information that should, under the proposals made in this article, only be accessible on demonstration of some level of cause. If the profiles that supposedly justify these programs are worthy of the name, they should meet the necessary justification standards. Thus, if ESSENCE accesses the contents of medical records for criminal investigation purposes, its algorithm ought to identify only people who are highly likely to be perpetrators of crime.<sup>187</sup> If all of its information comes from public records, then its ability to identify criminals need not be as potent. And if instead it merely accesses information about who has been where or been associated with whom—catalogic data—its use would be permissible

---

<sup>186</sup>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).

<sup>187</sup>8 U.S.C. §1731(a)(2) (requiring the establishment of a database for all arrivals and departures).

if the information is articulably relevant to an investigation.<sup>188</sup> The degree of intrusion ought to determine the required success rate of the data mining operation.<sup>189</sup>

## V. 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 protester or the young Arab man), he needs a subpoena, notification of which can be delayed if necessary, to get the addresses of the person's email messages and URLs visited. He needs a *Terry* order to use Matrix, as it accesses the content of public records. And he needs a warrant based on probable cause to access the suspect's financial, school, medical and similar personal records.<sup>190</sup> If

---

<sup>188</sup>Furthermore, since such profiling might involve scanning information about hundreds or thousands of people, individual notice of the type required for individual-based surveillance would be impractical, and of limited usefulness in terms of inhibiting abuse. Rather, a better practice, recommended by the American Bar Association in connection with physical surveillance, would be to require periodic reports on the extent of data mining, with sufficient detail that privacy and other advocates can meaningfully monitor its use. See American Bar Association, Standards Relating to Technologically-Assisted Physical Surveillance, Standard 2.7(f)(v) ("Government officials should be held accountable for use of regulated technologically-assisted physical surveillance technology by means of . . . (v) maintaining and making available to the public general information about the type or types of surveillance being used and the frequency of their use.").

<sup>189</sup>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 of data mining. *Id.* at 48-59.

<sup>190</sup>The analysis should not change if government seeks personal information from records acquired by a commercial data broker that has obtained the information from the original record-holders. Otherwise, all of this regulation could be avoided. Data do not become less personal

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 who might be planning to bomb a mall), he would be on solid ground if this catalogic data increases 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.

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.<sup>191</sup> He points out that technology has made it easier both to maintain information about people and to aggregate it.<sup>192</sup> 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.”<sup>193</sup> 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

---

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 surrendered to a public or a private entity.

<sup>191</sup>Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S.Cal.L.Rev. 1083 (2002).

<sup>192</sup>*Id.* at 1090-95.

<sup>193</sup>*Id.* at 1152-59.

calls a “regulated subpoena.”<sup>194</sup> 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 sought are of “material importance” to the investigation, which he describes as a standard that is “slightly more permissive 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).<sup>195</sup> As with traditional subpoenas, the regulated subpoena would be challengeable by the target.<sup>196</sup>

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,<sup>197</sup> 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.<sup>198</sup> Privacy, Solove argues, is a contextual concept that

---

<sup>194</sup>Id. at 1164.

<sup>195</sup>Id. at 1164-65.

<sup>196</sup>Id. at 1165.

<sup>197</sup>Id. at 1152-53.

<sup>198</sup>Id. at 1154.

cannot form the basis for uniform regulation.<sup>199</sup> Rather, in the context of transaction surveillance, the focus should be whether the information is maintained in a system of records.<sup>200</sup> 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 to find out 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 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 probable cause for all record searches, as Solove would, provides protection far beyond the margins for information that ought to be more easily available to the government. Data mining of any sort would be almost impossible; the sniper-killer and terrorist investigations described above might never get off the ground. As another example of the difficulties posed by a uniform probable cause requirement, imagine the 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 the Law & Order TV show). They would certainly be able to demonstrate the relevance of this catalogic data, but would not have probable cause with respect to any of the callers, and thus would not be able get the regulated subpoena for the phone company's records that Solove would demand. Creating a hierarchy of privacy, as tricky as it is,

---

<sup>199</sup>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).

<sup>200</sup>Solove, *supra* note , 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 important as a means of enabling the balancing of government and individual interests that the Supreme Court has sanctioned since the 1960s.<sup>201</sup>

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. But, to pursue that example, the difference between getting the intimate information through an interview and through the suspect's medical records is as dependent on concepts of privacy as it is on the bare fact that one source is a person and the other source is a record. Consider these variations of the example. Would we allow the government to ask questions about *anyone's* private parts, or only when that information is important to an investigation? Would we allow the police to coerce this type of information from the suspect's sexual partner if she were his wife? What if she were working as an agent for law enforcement at the time she engaged in sexual relations with the suspect? The reason we don't impose restrictions on the type of interview that Solove describes is that, by hypothesis, the police have good reason to ask her questions about private information, she is exercising her autonomy in giving them the information, and she did not obtain the information under false pretenses. When the information is handed over by a hospital pursuant to a subpoena, on the other hand, it is cajoled into breaching a confidential relationship that the suspect assumed would be kept that way, at least until there is a very good reason to disclose it (which a subpoena does not require).<sup>202</sup> As I argued earlier,<sup>203</sup> when the third party is

---

<sup>201</sup>See *Camara v. Municipal Court*, 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”).

<sup>202</sup>One might distinguish the hospital from other third party institutions like phone companies, where the tradition of confidentiality is minimal. Indeed, many third party institutions would probably want to disclose information to law enforcement. See Susan

an impersonal record-holder, as is the case when transaction surveillance occurs, autonomy interests are minimal, if not non-existent; at the same time, the target's privacy interests are at least as significant because the information is surrendered to the record-holder only because it is demanded in order to receive services and the record-holder purports to use it *solely* for that purpose. These considerations lead me to conclude that we should protect transactional information, but the degree to which we do so should be dependent on its presumptive privacy, not whether it exists in record form.

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."<sup>204</sup> 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 when in connection with prosecutions for serious crime.<sup>205</sup> 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.

---

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 this fact makes the third party institution even less like a third party individual, who will often have much to lose (a relationship, for instance) if disclosure occurs.

<sup>203</sup>See supra text accompanying notes .

<sup>204</sup>William J. Stuntz, *Local Policing After the Terror*, 111 Yale L.J. 2137, 2181 (2002).

<sup>205</sup>Id. at 2184-85.

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 thousand of law enforcement officers are charged with fighting "terrorism," an amorphous threat to say the least.<sup>206</sup> And, as I have discussed elsewhere, ensuring that the information government officials acquire through covert surveillance is used only for the purpose of prosecuting crime could be equally difficult, precisely because the surveillance is covert.<sup>207</sup> 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.<sup>208</sup>

Even if the information gathered is somehow confined to a limited and discreet 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:

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

---

<sup>206</sup>See generally, Gabriel Soll, *Terrorism: The Known Element No One Can Define*, 11 Willamette J. Int'l L. & Disp. Resol. 123 (2004).

<sup>207</sup>Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 Miss. L.J. 213, 304-05 (2002) (noting that finding the "poisonous tree" for evidence used in prosecutions for non-serious crimes and law enforcement actions that do not result in prosecutions will be difficult when the tree is secret).

<sup>208</sup>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), would not help matters.

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."<sup>209</sup>

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 when it is occurring, rather than being left in the dark.<sup>210</sup>

## 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 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

---

<sup>209</sup>Slobogin, *supra* note , at 305. 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) (poll indicating that 72% of Americans have "some" or "very little" trust in the government to "use personal information appropriately"), available at <http://www.excelgov.org>.

<sup>210</sup>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).

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.”<sup>211</sup> When it comes to transaction surveillance, only the Fourth Amendment provides that type of restraint.

---

<sup>211</sup>Introductory Remarks of Senator Sam J. Ervin on S. 3418, in Legislative History of the Privacy Act of 1974 s. 3418 (Public Law 93-579), Comm. on Gov’t Operations (U.S. Senate), and Comm. on Gov’t Operations’ (House of Representatives) Subcommittee on Gov’t Information and Individual Rights, May 1, 1974.

