To live in the modern world, we must enter into numerous relationships with other people and businesses: doctors, lawyers, merchants, magazines, newspapers, banks, credit card companies, employers, landlords, ISPs, insurance companies, phone companies, and cable companies. The list goes on and on. Our relationships with all of these entities generate records containing personal information necessary to establish an account and record our transactions and preferences. We are becoming a society of records, and these records are not held by us, but by third parties.

These record systems are becoming increasingly useful to law enforcement officials. Personal information can help the government detect fraud, espionage, fugitives, drug distribution rings, and terrorist cells. Information about a person’s financial transactions, purchases, and religious and political beliefs can assist the investigation of suspected criminals and can be used to profile people for more thorough searches at airports.

**Fourth Amendment, Records, And Privacy**

The U.S. Supreme Court held that there is no reasonable expectation in privacy for information known or exposed to third parties. In *United States v. Miller*, federal agents presented subpoenas to two banks to produce the defendant’s financial records. The defendant argued that...
the Fourth Amendment required a warrant, not a subpoena, but the High Court concluded that the amendment didn’t apply. There is no reasonable expectation of privacy in the records, the Court reasoned, because the information is “revealed to a third party.” Thus, “checks are not confidential communications but negotiable instruments to be used in commercial transactions. All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business.”

The Court used similar reasoning in Smith v. Maryland. Without a warrant, the police asked a telephone company to use a pen register, which is a device installed at the phone company to record the numbers dialed from the defendant’s home. The Court concluded that since people “know that they must convey numerical information to the phone company,” they cannot “harbor any general expectation that the numbers they dial will remain secret.”

Miller and Smith establish a general rule that if information is in the hands of third parties, then an individual lacks a reasonable expectation of privacy in that information, which means that the Fourth Amendment does not apply. Individuals thus probably do not have a reasonable expectation of privacy in communications and records maintained by ISPs or computer network administrators.

The third party record doctrine stems from the secrecy paradigm. If information is not completely secret, if it is exposed to others, then it loses its status as private. Smith and Miller have been extensively criticized throughout the past several decades. However, it is only recently that we are beginning to see the profound implications of the third party doctrine. Smith and Miller are the new Olmstead v. United States, where the Court in 1928 concluded that wiretapping was not protected by the Fourth Amendment.

For nearly 40 years until it was reversed in Katz v. United States, the government’s power to engage in wiretapping and other forms of electronic surveillance fell outside of the reach of the Fourth Amendment, and the legislation that filled the void was ineffective. Gathering information from third party records is an emerging law enforcement practice with as many potential dangers as the wiretapping in Olmstead. “The progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping.”

Justice Brandeis observed in his Olmstead dissent. “Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.”

That day is here. The government’s harvesting of information from the extensive dossiers being assembled with modern computer technology poses one of the most significant threats to privacy of our times.

**Emerging Statutory Regime And Its Limits**

Throughout the twentieth century, when the Supreme Court held that the Fourth Amendment was inapplicable to new practices or technology, Congress often responded by passing statutes that afforded some level of protection. Through a series of statutes, Congress has established a regime regulating government access to third party records. This regime erects a particular architecture significantly different from that of the Fourth Amendment. Unfortunately, this regime is woefully inadequate.

**Procedural Requirements To Obtain Information.** The most significant deficiency is that a majority of the statutes permit government access to third party records with only a court order or subpoena — a significant departure from the Fourth Amendment, which generally requires warrants supported by probable cause to be issued by a neutral and detached judge. Unlike warrants, subpoenas do not require probable cause and can be issued without judicial approval. Prosecutors, not neutral judicial officers, can issue subpoenas.

According to Stuntz: “[W]hile searches typically require probable cause or reasonable suspicion and sometimes require a warrant, subpoenas require nothing, save that the subpoena not be unreasonably burdensome to its target. Few burdens are deemed unreasonable.” According to legal scholar Ronald Degtan, subpoenas are not issued “with great circumspection” and are often “handed out blank in batches and filled in by lawyers.” As Stuntz contends, federal subpoena power is “akin to a blank check.”

Prosecutors can also use grand jury subpoenas to obtain third party records. Grand jury subpoenas are “presumed to be reasonable” and may only be quashed if “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 investigation.” As Stuntz observes, grand jury subpoenas “are much less heavily regulated” than search warrants.

As long as the material asked for is relevant to the grand jury’s investigation and as long as compliance with the subpoena is not too burdensome, the subpoena is enforced. No showing of probable cause or reasonable suspicion is necessary, and courts measure relevance and burden with a heavy thumb on the government’s side of the scales.

Therefore, courts “quash or modify” subpoenas only “if compliance would be unreasonable or oppressive.” Further, “judges decide these motions by applying vague legal standards case by case.”

Court orders under most of the statutes are not much more constrained than subpoenas. They typically require mere “relevance” to an ongoing criminal investigation, a standard significantly lower and looser than probable cause.

The problem with subpoenas and court orders is that they supply the judiciary with greatly attenuated oversight powers. The role of the judge in issuing or reviewing subpoenas is merely to determine whether producing records is overly burdensome. With this focus, financial hardship in producing information would give courts more pause when reviewing subpoenas than would threats to privacy. The role of the judiciary in court orders is also quite restricted. Instead of requiring probable cause, court orders require the government to demonstrate that records are “relevant” to a criminal investigation, a much weaker standard. In short, judicial involvement with subpoenas and court orders amounts to little more than a rubber stamp of judicial legitimacy.

**Wiretapping And Bugging.** When the Court held in Olmstead that the Fourth Amendment did not apply to wiretapping, Congress responded six years later by enacting § 605 of the Federal Communications Act of 1934. As discussed earlier, § 605 was far too narrow and limited. In 1968, a year after the Supreme Court in Katz declared that the Fourth Amendment applied to wiretapping, Congress enacted Title III of the
Although the Wiretap Act has substantial protections, it covers ground already protected by the Fourth Amendment. In areas not protected by the Fourth Amendment, the architecture of the statutory regime is much weaker and more porous.

**Stored Communications.** Communications service providers frequently store their customers’ communications. ISPs temporarily store e-mail until it is downloaded by the recipient. Many ISPs enable users to keep copies of previously read e-mails on the ISP’s server, as well as copies of their sent emails. Since a third party maintains the information, the Fourth Amendment may not apply.

The Wiretap Act covers wiretapping and bugging. It applies when a communication is intercepted during transmission. The act has strict requirements for obtaining a court order to engage in electronic surveillance. In certain respects, the Wiretap Act’s requirements are stricter than those for a Fourth Amendment search warrant. It also requires that the surveillance “minimize the interception of communications” not related to the investigation. The act is enforced with an exclusionary rule.

However, the interception of electronic communications not involving the human voice (such as e-mail) are not protected with an exclusionary rule.

---

**Financial Records.** Two years after *United States v. Miller*, Congress filled the void with the Right to Financial Privacy Act (RFPA) of 1978, which requires the government to obtain a warrant or subpoena to access records from banks or other financial institutions.

However, the subpoena merely requires a “reason to believe that the records sought are relevant to a legitimate law enforcement inquiry.” When subpoena authority is not available to the government, the government need only submit a formal written request for the information.

In addition to banks, credit reporting agencies have detailed records for...
nearly every adult American consumer. Under the Fair Credit Reporting Act (FCRA) of 1970, a consumer reporting agency “may furnish identifying information respecting any consumer, limited to his name, address, former addresses, places of employment, or former places of employment, to a government agency.” Thus, the government can simply request this information without any court involvement. And the government can obtain more information with a court order or grand jury subpoena. Since the FCRA focuses on credit reporting agencies, it doesn’t prohibit the recipients of credit reports from disclosing them to the government.

Although the RFPA and FCRA protect financial information maintained by banks and credit reporting agencies, the government can obtain financial information from employers, landlords, merchants, creditors, and database companies, among others. Therefore, financial records are protected based only on which entities possess them. Thus, the statutory regime merely provides partial protection of financial data.

Electronic Media Entertainment Records. The statutory regime protects records pertaining to certain forms of electronic media entertainment. Under the Cable Communications Policy Act (Cable Act) of 1984, a government official must obtain a court order in order to obtain cable records. The government must offer “clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case.” People can “appear and contest” the court order. This standard is more stringent than the Fourth Amendment’s probable cause and warrant requirements. However, there is no exclusionary rule under the Cable Act.

In addition to cable records, the statutory regime also protects videotape rental records. The Video Privacy Protection Act (VPPA) of 1988 states that a videotape service provider may disclose customer records to law enforcement officials “pursuant to a warrant . . . , an equivalent state warrant, a grand jury subpoena, or a court order.” Unlike the Cable Act, the level of protection under the VPPA is much less stringent.

Although the statutory regime protects the records of certain forms of electronic media entertainment, it fails to protect the records of many others. For example, records from music stores, electronics merchants, and Internet media entities are afforded no protection.

Medical Records. Our medical records are maintained by third parties. Could the third party doctrine extend to medical records? On the one hand, given the considerable privacy protection endowed upon the patient-physician relationship, the third party doctrine may stop at the hospital door. On the other hand, the doctrine applies to records of financial institutions, which also have a tradition of maintaining the confidentiality of their customers’ information. Unless the patient-physician relationship is distinguished from banks, the third party doctrine logically could apply to medical records. However, the Supreme Court has yet to push the doctrine this far.

The federal health privacy rules under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 apparently view medical records as falling under the third party doctrine. The rules permit law enforcement officials to access medical records with a mere subpoena. Health information may also be disclosed “in response to a law enforcement official’s request for such information for the purpose of identifying or locating a suspect, fugitive, material witness, or missing person.”

Moreover, not all health records are covered by HIPAA. Only records maintained by health plans, health care clearinghouses, and health care providers are covered. Although doctors, hospitals, pharmacists, health insurers, and HMOs are covered, not all third parties possessing our medical information fall under HIPAA. For example, the sale of nonprescription drugs and the rendering of medical advice by many Internet health Websites are not covered by HIPAA. Therefore, while certain health records are protected, others are not.

Holes In The Regime. Federal statutes provide some coverage of the void left by the inapplicability of the Fourth Amendment to records held by third parties. Although the statutes apply to communication records, financial records, entertainment records, and health records, these are only protected when in the hands of particular third parties. Thus, the statutory regime does not protect records based on the type of information contained in the records, but protects them based on the particular types of third parties that possess them.

Additionally, there are gaping holes in the statutory regime of protection, with classes of records not protected at all. Such records include those of merchants, both online and offline. Records...
Privacy's Problem


Privacy in the Digital Age: Work in EYEWITNESS IDENTIFICATION EVIDENCE


that are “relevant” to an investigation, the role of the judge in the process is diminished to nothing more than a decorative seal of approval. And since there are numerous holes in the regime, there are many circumstances when neither court orders nor subpoenas are required. The government can simply ask for the information. An individual’s privacy is protected only by the vague and toothless privacy policies of the companies holding their information.

Notes

2. Id., 442.
5. Id., § I.C.1(b)(iv).
14. Grand juries are still used in some states as well as in the federal system. See Degnan, Obtaining Witnesses, 229.
21. Id. § 2518.
24. This conclusion is debatable, however, because telephone companies can also store telephone communications, and it is unlikely that the Court would go so far as to say that this fact eliminates any reasonable expectation of privacy in such communications.
26. Kerr, Searching and Seizing, § III.B.
27. Id., § III.D.1.
32. 18 U.S.C. § 3123(a).
33. “Upon application made under § 3122(a)(1), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device....” Id. §3123(a)(1).
34. United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995). See also Kerr, Searching and Seizing, § IV.B.
42. 47 U.S.C. § 551(h)(2).
46. 45 C.F.R. § 164.512(f)(1)(ii).
47. Id. § 164.512(f)(2).
48. 45 C.F.R. § 160.102.


About the Author


For permission to reproduce this article, in whole or in part, contact Nicholas Taylor, NYU Press, (212) 992-9998.

Daniel J. Solove
Associate Professor of Law
George Washington Univ. Law School
2000 H Street NW
Washington, DC 20052
202-994-9514
E-MAIL dsolove@law.gwu.edu