



# PRIVACY & SECURITY LAW



## REPORT

Reproduced with permission from Privacy & Security Law Report, Vol. 6, No. 48, 12/10/2007, pp. 1875-1878. Copyright © 2007 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

### Search and Seizure

By far the largest exception to the Fourth Amendment is for records individuals disclose to a third party, but that exemption makes little sense today, writes Indiana University Professor Fred H. Cate. Technological advances have significantly expanded the scope of a 1976 Supreme Court decision that excluded records held by third parties from the protection of the Fourth Amendment, meaning the government has the power under the Fourth Amendment to unrestricted access to private-sector records on personal details, Cate says. He concludes that the high court's third-party doctrine compromises our privacy.

## The Vanishing Fourth Amendment

By FRED H. CATE

*Fred H. Cate is a Distinguished Professor and director of the Center for Applied Cybersecurity Research at Indiana University, and a senior policy advisor to the Center for Information Policy Leadership at Hunton & Williams. He is a member of the National Academy of Sciences Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals and reporter for the American Law Institute's project on Principles of the Law on Government Access to and Use of Personal Digital Information. Previously, he served as counsel to the Department of Defense Technology and Privacy Advisory Committee.*

## The Fourth Amendment

**H**istorically, the primary constitutional limit on the government's power to obtain personal information is the Fourth Amendment. The Amendment reflects the Framers' hostility to "general searches"—searches not based on specific suspicion. It prohibits "unreasonable searches and seizures" and requires that warrants be issued only "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

The Supreme Court generally interprets the Fourth Amendment also to require that searches be conducted only with a warrant issued by a court, and that the government provide the target with contemporaneous notice of the search.

The Fourth Amendment is silent about what makes a search or seizure "unreasonable." In his 1967 concur-

rence in *Katz v. United States*, Justice Harlan wrote that reasonableness was defined by both the individual's "actual," subjective expectation of privacy and by an objective expectation that was "one that society was prepared to recognize as 'reasonable.'" 389 U.S. 347, 361 (1967) (Harlan, J., concurring). The Court adopted that test for determining what was "private" within the meaning of the Fourth Amendment in 1968 in *Terry v. Ohio* and continues to apply it today 392 U.S. 1 (1968).

While the protection afforded by the Fourth Amendment can be considerable, it is not absolute. The Supreme Court has determined, for example, that warrants are not required to search or seize items in the "plain view" of a law enforcement officer, for searches that are conducted incidental to valid arrests, and for searches specially authorized by the Attorney General or the President involving foreign threats of "immediate and grave peril" to national security.

Moreover, the Fourth Amendment poses no limits on how the government may use information, provided that it has been obtained legally. So personal data seized by the government in compliance with the Fourth Amendment may later be used in a context for which the data could not constitutionally have been obtained.

### **The Miller-Smith Exclusion of Third-Party Records**

By far the largest exception to the Fourth Amendment is for records in the possession of a third party. The Supreme Court held in 1976 in *United States v. Miller* that there can be no reasonable expectation of privacy in information held by a third party. 425 U.S. 435 (1976). The case involved copies of cancelled checks, to which, the Court noted, "respondent can assert neither ownership nor possession." Such documents "contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business," and therefore the Court found that the Fourth Amendment is not implicated when the government sought access to them:

The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government. 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. Id. at 443 (citation omitted).

The Court's decision in *Miller* is remarkably sweeping. The bank didn't just happen to be holding the records the government sought. Instead, the Bank Secrecy Act, 12 U.S.C. § 1829b(d), requires banks to maintain a copy of every customer check and deposit for six years or longer. The government thus compelled the bank to store the information, and then sought the information from the bank on the basis that since it held the data about its customer's checks, there couldn't be any reasonable expectation of privacy and the Fourth Amendment therefore did not apply.

A majority of the Supreme Court was not troubled by this end-run around the Fourth Amendment: "even if the banks could be said to have been acting solely as

Government agents in transcribing the necessary information and complying without protest with the requirements of the subpoenas, there would be no intrusion upon the depositors' Fourth Amendment rights." Id. at 444.

Congress reacted to the decision by enacting modest statutory protection for customer financial records held by financial institutions in the Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3422, but as a result of the *Miller* decision, there is no constitutional protection for financial records or other personal information that has been disclosed to third parties, even if the data are maintained by those third parties at the behest of the government.

The Court reinforced its holding in *Miller* in *Smith v. Maryland*, involving information about telephone calls. 442 U.S. 735 (1979). The Supreme Court found that the Fourth Amendment is inapplicable to telecommunications "attributes" (e.g., the number dialed, the time the call was placed, the duration of the call, etc.) because that information is necessarily conveyed to, or observable by, third parties involved in connecting the call. "[T]elephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes." Id. at 743.

As a result, under the Fourth Amendment, the use of "pen registers" (to record out-going call information) and "trap and trace" devices (to record in-coming call information) does not require a warrant because they only collect information about the call that is necessarily disclosed to others. As with information disclosed to financial institutions, Congress reacted to the Supreme Court's decision by creating a statutory warrant requirement for pen registers, 18 U.S.C. §§ 3121, 1841, but the Constitution does not apply.

### **The Third-Party Exemption and the Explosion in Digital Data**

The third party exemption from the Fourth Amendment made little sense in the cases in which it was created. Individuals who write checks and dial telephone calls do not "voluntarily" convey information to third parties. They have no choice but to convey the information if they wish to participate in modern economic and social life.

Moreover, and more importantly, personal information is collected and stored by banks and telephone companies subject to widely shared expectations that it will not be further disclosed beyond legitimate business purposes. The Court's decisions to the contrary, while they served important law enforcement objectives, made little logical or practical sense and did not reflect the expectations of either the public or policymakers, as demonstrated by the fact that Congress responded so quickly to both with gap-filling legislation.

Irrespective of whether *Miller* and *Smith* were correct when decided, however, excluding records held by third parties from the protection of the Fourth Amendment raises far more significant issues today. Dramatic advances in digital technologies and society's increased reliance on them mean that more and more of individuals' daily activities, transactions, and communications

are routinely captured and stored as digital data. This is especially true online, where merchants record data not only on what individuals buy and how we pay for our purchases, but also on every detail of what we look at, what we search for, how we navigate through web sites, and with whom we communicate.

These records are not only found in the Internet context. Computers track every moment of most employees' days. Digital time clocks and entry key cards record physical movements. Computers store work product, e-mail, and voice mail. Sensors monitor productivity—from check-out scanners at retail points-of-sale, which record how quickly a cashier processes a transaction, to key cards that monitor how long employees spend in the bathroom or break room each day.

Digital devices for paying tolls, computer diagnostic equipment in car engines, and global positioning services that are increasingly common on passenger vehicles record every mile driven. Cellular telephones and personal digital assistants record not only call and appointment information, but location as well, and transmit this information to service providers. Digital cable and satellite service providers record what we watch and when. Alarm systems record when we enter and leave our homes. ATMs and digital credit and debit card terminals record who and where we are, what we buy or how much money we withdraw, and where we bank.

Moreover, those records are held by more private parties than ever before. Digital transactions are likely to be observed by more parties. Data about online browsing or purchases are accessible not only to the consumer and merchants directly involved in the transaction, but also to their Internet service providers, the provider of the payment mechanism (for example, a credit card company), and the company that delivers the merchandise. The everyday use of a credit card or ATM card involves the disclosure of personal financial information to multiple entities.

In addition, digital networks have facilitated the growth of vigorous outsourcing markets, so information provided to one company is increasingly likely to be processed by a separate institution. Customer service may be provided by another; e-mail by another. And all of those entities may store their data with still another. Personal information is available from all of these.

The government would hardly need to visit all of these businesses separately, however, to gather personal information. Information aggregators in the private sector already combine personal data from thousands of private-sector sources and public records. These files are updated daily by a steady stream of incoming data. These businesses supply this information, for a fee, to private- and public-sector customers for a variety of valuable uses. They also provide a one-stop shop for the government.

All indications are that this is just the beginning. Broadband Internet access into homes has not only increased the personal activities we now engage in online, but also created new and successful markets for remote computer back-up and online photo, e-mail, and music storage services. With Voice Over IP telephone service, digital phone calls are becoming indistinguishable from digital documents: both can be stored and accessed remotely. Global positioning technologies are appearing in more and more products, and radio frequency identification tags are beginning to be used to identify high-end consumer goods, pets, and even people.

Advances in technologies, and the development of new products and services in response to those changes, have significantly expanded the scope of the *Miller* exclusion of records held by third parties from the protection of the Fourth Amendment. Today there are vastly more personal data in the hands of third parties, they are far more revealing, and much more readily accessible than was the case in the 1970s. As a result, the scope of the *Miller* decision has been greatly expanded and the balance between the government's power to obtain personal data and the privacy rights of individuals fundamentally altered.

## The Fourth Amendment and Data Mining

Technological developments have put increasingly powerful tools in the hands of the government to be able to use those data. Millions of records stored on microfilm were not likely to be of much value to the government. The cost of duplicating, transporting, storing, and using them would have been in most cases prohibitive. In electronic format, however, those costs are comparatively negligible. So while the impact of *Miller* in 1976 was primarily limited to government requests for specific records about identified individuals, today *Miller* allows the government to obtain the raw material for broad-based data mining.

This is a significant difference. The searches at issue in the 1970s involved demands for information about individuals who had already done something to warrant the government's attention. Whether or not the suspicious activity amounted to "probable cause," there was at least some reason to suspect a particular person. Today, because of major technological and related changes, the government not only has the power under the Fourth Amendment to ask for everything about everybody, but increasingly the practical ability to do something with that information.

As a result, as part of its on-going efforts to fight terrorism (as well as deal with illegal immigration, organized crime, money laundering, drug trafficking, dead-beat dads, and other issues), the government increasingly desires access to broad swaths of information about people who have done nothing to warrant suspicion. This new practical power offers potentially valuable new tools, but that power expands the impact of the *Miller* exception and the volume of personal data accessed by the government without constitutional oversight.

The government has adopted hundreds of additional record-keeping requirements that compel the private sector to collect, store, and, in many cases, report extensive personal information to the government. For example:

- Over the past decade, the government has collected and stored more than 75 million federally mandated Suspicious Activity Reports and Currency Transaction Reports from banks and credit unions, money service businesses, securities and commodities firms, Post Office branches, casinos, travel agencies, pawnbrokers, real estate agents, automobile and boat retailers, insurance companies, jewelers, and anyone who accepts a check, travelers' check, or money order.
- The Transportation Security Administration's Automated Targeting System and Advance Passenger Information System require carriers of passengers, ve-

hicles, and cargo to collect and share with the government personal data including name, passport number, birth date, gender and other identifying information, credit card number and other payment data, complete itinerary information, frequent traveler records, baggage information, and travel agent information.

- According to lawmakers who have been briefed on the program, under the National Security Agency's domestic Terrorist Surveillance Program, the government has installed sophisticated surveillance equipment in domestic telephone company switching facilities to siphon off records on domestic phone calls. The data to which the NSA program has access reportedly include phone company records on the numbers dialed and the length of calls about potentially billions of U.S. telephone calls.
- The Defense Department's Total Information Awareness—later renamed "Terrorism Information Awareness"—research and development program included technologies to search personally identifiable commercial transaction records and recognize patterns across separate databases for the purpose of combating terrorism. Congress purported to terminate funding for TIA, but excepted "processing, analysis, and collaboration tools for counterterrorism foreign intelligence" specified in a classified annex to the Act.

Recent experience has shown that the government has no practical or legal difficulty accessing personal data held by the private sector. In the absence of any constitutional limit, Congress has granted the government broad authority to seize or compel the disclosure of data, and the administration has interpreted that authority more broadly still.

Administrative, investigative, and grand jury subpoenas, all of which are issued without judicial oversight, are routinely used to obtain access to private-sector records. Between 2001 and 2006, for example, the Treasury Office of Foreign Assets Control issued 65 administrative subpoenas to the Society for Worldwide Interbank Financial Telecommunication (SWIFT) to obtain access to as many as 3 billion messages about individuals' international financial transactions.

Similarly, four federal statutes authorize the FBI to issue "National Security Letters" to telephone companies, financial institutions, ISPs, and consumer credit agencies, which require the recipients to produce the records that the government seeks. In 2006, the Department of Justice Inspector General found that the FBI had issued 143,074 NSLs between 2003 and 2005, instead of the 52,199 NSLs reported by the FBI. Each request may seek records concerning many people. In fact, nine NSLs in one investigation sought data on 11,100 separate telephone numbers.

Sometimes, the government obtains access to third-party records even without statutory authorization. In the immediate aftermath of the 9/11 attacks, for example, the FBI collected as much as a full year's worth of passenger data—including sensitive information such as credit card numbers—from all major U.S. airlines.

## Conclusion

The Supreme Court's failure to extend the protections of the Fourth Amendment to personal data maintained by third parties, combined with the technological

changes that result in more and increasingly revealing information necessarily being disclosed to and stored by third parties, threaten to eliminate those protections entirely. The exception threatens to swallow the rule.

Moreover, the government's practical ability to analyze vast amounts of disparate data obtained from the private sector rapidly and affordably threatens to extend government surveillance to every aspect of daily life. The Supreme Court's third-party exception removes constitutional protection from the very activity—the indiscriminate search—that the Fourth Amendment was written to restrict.

The third-party doctrine dramatically reduces judicial oversight for government searches, thus compromising the protection that the separation of government power into executive, legislative, and judicial branches was intended to provide. And the Court's opinion in *Miller*, *Smith*, and similar cases reflects a binary approach to privacy—information is either private or it is not—that is inconsistent with the modern world, popular expectations, and the Court's decisions in non-Fourth Amendment privacy cases.

Statutory responses, while important, are insufficient to fill the gap created by the Court, because they do not have the force of constitutional law and because they can—and, experience has shown, will—be compromised in the face of perceived threats or political pressure. In addition, privacy laws and regulations apply to only limited areas of commerce.

Moreover, recent "privacy" enactments have been more noteworthy for the extent to which they facilitate, rather than restrict, government access to sensitive data. For example, the privacy regulations adopted under the Health Insurance Portability and Accountability Act permit law enforcement access to health records with a warrant, a subpoena, an administrative request, an investigative demand, or even a law enforcement official's request.

In sum, the Court's third-party doctrine compromises our privacy. It may also threaten our security, because as government officials routinely acknowledge, by making the government stop and justify its effort to a federal judge, the Fourth Amendment's warrant requirements help bring focus and precision to law enforcement and national security efforts.

The private sector should be concerned because the Court's exclusion of its customer records from the Fourth Amendment threatens to turn industry into the government's data center. By statute and regulation, the government requires industry to collect and keep the data that the government needs, subject to significant financial and other penalties for failing to do so, and then by exclusion of those records from the scope of the Fourth Amendment, the Court will permit the government to demand those records at will, irrespective of privacy policies or contractual commitments, and without requiring compensation.

Moreover, the fact that the government has constitutionally unrestricted access to commercial records has already contributed to calls for greater privacy regulation applicable to the private sector on the basis that if industry cannot collect the data then they will not be available for the government to seize. Similarly, the government's voracious appetite for private-sector data, unrestrained by the Fourth Amendment, is at the heart of most recent disputes with European Union member

---

states, Canada, and other countries over multinational data flows.

The Supreme Court's exclusion from the Fourth Amendment of personal data held by third parties leaves us all vulnerable. It allows the government constitutionally unrestricted access to private-sector records on every detail of how we live our lives. The

government's demands for data, and the burdens imposed on individual privacy or the private-sector custodian, need not be reasonable, and no judicial authorization or oversight is required. The exclusion thus threatens to fundamentally alter the relationship between the government and the people.