WASHINGTON
LEGISLATIVE OFFICE

ACLU Comments on "Exploring Privacy: FTC Privacy Roundtable"

Re: Privacy Roundtables – Comment, Project No. PO95416

Nov. 6, 2009

AMERICAN CIVIL LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

MICHAEL W.MACLEOD-BALL
ACTING DIRECTOR

NATIONAL OFFICE
125 BROAD STREE,ST 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

The American Civil Liberties Union hereby submits comments to the Federal Trade Commission on the Federal Trade Commission's "Exploring Privacy: A Roundtable Series."

The Commission's Privacy Roundtable seeks to answer the question, what "risks, concerns, and benefits arise from the collection, sharing, and use of consumer information?"

Clearly there are many risks involved in such activities. Chief among them are:

- The risk of facing adverse judgments such as the denial of insurance or unfavorable treatment by financial firms or other companies, based on information – true or false – in profiles maintained about one.
- The risk of embarassment through the unwanted disclosure or sharing of information with parties with whom one does not want to share information.
- The risk that the simple human right to control private information about oneself will not be honored.
- The chilling effects and inefficiencies that result from individuals' fear of adverse effects, which might lead them hold back and not exploit modern informational and communications technologies to their fullest.

The interaction between the private sector and security establishment

A crucial part of the privacy picture is the interaction between the private sector and the security establishment (law enforcement and national security agencies) in our government. These interactions create an overall context that must inform the calculus that individuals as well as policy makers (even those, such as at the FTC, principally concerned with consumer regulation) make when they form judgments about the risks and benefits of sharing personal information. That context is one in which privacy invasions from the private sector and privacy invasions from the security agencies are increasingly a distinction without a difference.

This aspect of the current privacy landscape will serve as the focus of these comments.

Acting under the broad mandate of the war on terrorism, the U.S. security establishment is making a systematic effort to extend its surveillance capacity by pressing the private sector into service to report on the activities of Americans. That effort colors all discussions of privacy focused on the private sector.

Public-private surveillance is not new. During the Cold War, for example, the major telegraph companies – Western Union, RCA and ITT – agreed to provide the federal government with copies of all cables sent to or from the United States every day – even though they knew it was illegal. The program, code named "Operation Shamrock," continued for decades, coming to an end only with the intelligence scandals of the 1970s.

Even such flagrant abuses as Operation Shamrock pale in comparison to the emergence of an information-age "surveillance-industrial complex." Nothing in our history compares to the efforts at distributed mass-surveillance now underway. Today's abuses combine the longstanding police impulse to expand private-sector information sources with awesome new technological capabilities for vacuuming up, storing and keeping track of vast oceans of information. The ongoing revolution in communications, computers, databases, cameras and sensors, combined with the private sector's increasingly insatiable appetite for consumer information, have created new opportunities for security agencies. These agencies are increasingly seeking to rely on mass sorting, sifting, and monitoring of populations as a means of stopping terrorism.

Most of the interactions and transactions in Americans' lives are not conducted with the government, but with corporations and other private entities, who therefore hold most of the details of Americans' lives – including much of what is private and most important to them. The combination of that rich detail with the awesome powers of the federal government is a prospect that ought to give every American pause, and which needs to figure prominently in evaluations of the privacy issues facing Americans today.

Security agencies have many options for accessing private-sector data

With the private sector tracking more and more of our activities for its own reasons, the government is free to leverage this private collection as a way of extending its own powers of surveillance.

Corporate compliance with government data-surveillance efforts ranges from unwilling resistance to indifferent cooperation to eager participation to

actual lobbying of the government to increase such activities. With an array of options at its disposal, the government can acquire a valuable stream of information about private activities from any source. These techniques add up to a startling advance in government monitoring of American life.

The security agencies' options for accessing third-party information include:

1. **Asking for data to be shared voluntarily.** At the request of a Homeland Security official, for example, JetBlue in 2002 gave a Pentagon subcontractor more than 5 million passenger records, which were combined with detailed personal files on each passenger purchased from a "data aggregator" company called Acxiom. JetBlue's action appeared to be in violation of its own privacy policy.[1] Similarly, in May 2002 the Professional Association of Diving Instructors voluntarily provided the FBI with a disk containing the names, addresses and other personal information of about 2 million people, nearly every U.S. citizen who had learned to scuba dive in the previous three years.[2]

2. **Buying information.** Security agencies are not the only organizations that are interested in creating high-resolution pictures of individuals' activities by drawing together data from a variety of sources. Commercial data aggregators do the same thing for profit. These companies are largely invisible to the average person, but make up an enormous, multi-billion-dollar industry. The Privacy Act of 1974 banned the government from maintaining information on citizens who are not the targets of investigations – but law enforcement agencies are increasingly circumventing that requirement by simply purchasing information that has been collected by data aggregators.[3]

3. **Demanding information, using legal powers granted by the Patriot Act and other laws.** Section 215 of the Patriot Act gives the FBI the power to demand customer records from Internet Service Providers (ISPs) and other communications providers, libraries, book stores or any other business – with inadequate judicial oversight.

---

[1] Ryan Singel, "JetBlue Shared Passenger Data," *Wired News*, Sept. 18, 2003; online at http://www.wired.com/news/privacy/0,1848,60489,00.html. Ryan Singel and Noah Shachtman, "Army Admits Using JetBlue Data," *Wired News*, Sept. 23, 2003; http://www.wired.com/news/privacy/0,1848,60540,00.html.

[2] Eunice Moscoso, "Feds demanding more info about companies' customers," *Atlanta Journal Constitution*, August 17, 2003; available online at http://www.ajc.com/business/content/business/0803/17patriot html.

[3] See Chris Jay Hoofnagle, "Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect, Process, and Package Your Data for Law Enforcement," *University of North Carolina Journal of International Law & Commercial Regulation*, Vol. 29 No. 4 (Summer 2004).

National Security Letters, which can be issued by FBI officials in field offices without the approval of a judge, give the government broad power to demand records with no judicial oversight. In both cases, businesses can be subject to a gag order prohibiting them from talking about the government's data demands.

4. **Using laws and regulations to dictate handling and storage of private-sector data in order to increase its surveillance value for the government.** The Communications Assistance for Law Enforcement Act of 1994 (CALEA) forced telecommunications providers to design their equipment according to the FBI's specifications in order to make eavesdropping easier and more convenient. Another law mandates that airlines collect identifying information from their passengers so that the government, among other things, can keep records of who is flying where. And there are proposals for mandatory retention of communications data, which has been enacted in Europe and which the security establishment would like to enact in the United States.[4]

5. **Creating systems for standing access to records of private activities.** The Patriot Act expanded systems for the regular feeding of financial data to the government through "suspicious" transaction reporting,[5] and a system for the government to conduct broad-ranging, nationwide "Google searches" through financial records by giving the security agencies the power to order a search of financial institutions across the nation for records matching a suspect.[6]

---

[4] See Declan McCullagh, "FBI director wants ISPs to track users," CNET News, Oct. 17, 2006; at http://news.cnet.com/2100-7348_3-6126877 html.

[5] The USA-Patriot Act, P.L. 107-56, Section 365, 115 Stat. 272 (Oct. 26, 2001). Scott Bernard Nelson, "Patriot Act would make watchdogs of firms," *Boston Globe*, November 18, 2001.

[6] "Financial Crimes Enforcement Network; Special Information Sharing Procedures to Deter Money Laundering and Terrorist Activity: Final Rule," 67 *Federal Register*, 60,579 (Sept. 26, 2002); the regulations stem from section 314 of the Patriot Act. Michael Isikoff, "Show Me the Money: Patriot Act helps the Feds in cases with no tie to terror," *Newsweek*, Dec. 1, 2003, online at http://www.msnbc.com/news/997054.asp.

Other examples

Other recent examples of close relationships between private-sector companies and government security agencies include:

- **The NSA spying scandal.** When it was revealed that the NSA was conducting illegal warrantless eavesdropping within the United States, it quickly became apparent that several telecommunications companies were active and willing participants in this illegal and unconstitutional mass invasion of Americans' privacy. Congress eventually granted retroactive immunity to the companies despite the pending claims of those wholly innocent individuals whose privacy had been breached.
- **Fusion centers.** Many proponents of these catch-all law enforcement data collection and analysis centers envision an active role for the private sector. Fusion Center guidelines crafted by the Department of Justice suggest the centers incorporate corporate participants, as well as private-sector data sources such as retail stores, apartment facilities, sporting facilities, hotels, supermarkets, restaurants, and financial companies.[7]

Conclusion

Many Americans are deeply suspicious of the ever-growing power of our security agencies. An explosion of technology that has outstripped existing legal privacy protections has allowed security agencies to move rapidly toward tapping the vast rivers of data now flowing into and through private sector companies. Meanwhile the post-9/11 focus on the threat of small terror cells has prompted those agencies increasingly to turn their focus inward upon the American population.

This situation greatly heightens the importance of privacy issues that come into play in the relationship between individuals and the companies with which they choose to do business (as well as those with which they do not choose to do business with but must nonetheless worry about, such as data aggregators).

The more information that the private sector collects and stores, the more individuals must worry. They will worry, for example, when they decide to exercise their rights to protest the policies of government or large private sector institutions, confront abusive police tactics, or otherwise make powerful enemies through the exercise of their rights. The larger the stores of data about the details of their lives that are available to such enemies, the more vulnerable such individuals will be – and the more hesitant they will be to exercise their rights.

[7] Bureau of Justice Assistance, Office Of Justice Programs, U.S. Dep't. Of Justice, "Fusion Center Guidelines: Developing And Sharing Information and Intelligence In A New Era," p. iii, (Aug. 2006).

The “Surveillance-Industrial Complex” is a fixture in today’s privacy landscape and a primary reason why Americans need strong privacy protections in the private sector.

Michael Macleod-Ball
Acting Director, Washington Legislative Office

Jay Stanley
Public Education Director, Technology and Liberty Program