



Written Statement of the
American Civil Liberties Union

Laura W. Murphy
Director, Washington Legislative Office

Christopher Calabrese
Legislative Counsel

before the
Senate Committee on Commerce, Science and Technology
July 27, 2010

Hearing on Consumer Online Privacy

Chairman Rockefeller, Ranking Member Hutchison and Members of the Committee:

On behalf of the American Civil Liberties Union (ACLU), a nonpartisan public interest organization dedicated to protecting the constitutional rights of individuals, and its more than half a million members, countless additional activists and supporters, and fifty-three affiliates nationwide, we applaud you for turning your attention to the important question of consumer online privacy. The ACLU has long been concerned about the growing collection of personal information by private entities. In our 2004 report “Surveillance-Industrial Complex: How the American Government Is Conscripting Businesses and Individuals in the Construction of a Surveillance Society” we wrote about the widespread collection of information by the private sector.¹

To identify the policy issues related to consumer interactions with corporations and other private parties, it is crucial to understand the larger context of information sharing throughout our society, including sharing with the government. Rapid technological advances and a lack of updated privacy law make information sharing between private parties and the government easier than ever, which in turn means that privacy invasions from the private sector can quickly become privacy invasions from the security agencies as well. This broader context must be considered when policymakers form judgments about the risks and benefits of sharing personal information and establish necessary protections to safeguard online consumer privacy.

This statement includes a brief description of this problem and two concrete measures – data retention limits and bars to third party access to personal information – that the committee can take to limit it.

Background

Acting under the broad mandate of the so-called 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.²

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 mass surveillance now underway. Today’s abuses combine the longstanding police impulse to utilize private-sector information sources with awesome new technological

¹This report is available at: <http://www.aclu.org/national-security/combating-surveillance-industrial-complex>

² See Dana Priest and William Arkin, *A hidden world, growing beyond control*, Washington Post, July 19, 2010.

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 relying 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. From social networking to email to photo sites, the more consumers learn, share, and connect online, the more personal information they leave behind. For example, as more people switch from hard-copy photographs in albums at home to online photo websites to develop and store digital photos, many do not realize that these photographs are stored in corporate databases, where they can be easily searched to compile information about consumers, their family and friends, and their private activities. As more people move information from hard copy calendars, address books, filing cabinets and home computers to online services, many do not realize that detailed information about who we know, where we go, and what we do in our personal lives could end up being collected and ultimately used in ways that we did not intend.

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 that 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:

Asking for data to be shared voluntarily. For example, in 2003, the online retailer eBay stated that it would be willing to give over all its information and everything it knows to law

enforcement on request.³ The C.I.A., via its investment arm In-Q-Tel, has invested in a software company that specializes in monitoring blogs and social networks.⁴

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.⁵ For example, the Department of Defense, the C.I.A., and the F.B.I. have all purchased use of private databases from Choicepoint, one of the largest aggregators of personal data.⁶

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. 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.

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

³ <http://lawmeme.research.yale.edu/modules.php?name=News&file=article&sid=925>. This policy seems to remain largely in force: according to eBay's current privacy policy, in response to a "verified request relating to a criminal investigation or alleged illegal activity," eBay will disclose "information relevant to the investigation, such as name, city, state, zip code, telephone number, email address, User ID history, IP address, fraud complaints, and bidding and listing history."

⁴ Noah Shachtman, *U.S. Spies Buy Stake in Firm That Monitors Blogs, Tweets*, WIRED, Oct. 19, 2009 at <http://www.wired.com/dangerroom/2009/10/exclusive-us-spies-buy-stake-in-twitter-blog-monitoring-firm/> (last visited October 23, 2009).

⁵ 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).

⁶ Shane Harris, *FBI, Pentagon Pay For Access to Trove of Public Records*, NAT'L J., Nov. 11, 2005, available at http://www.govexec.com/story_page.cfm?articleid=32802 (last visited October 7, 2009); Robert O'Harrow Jr., *In Age of Security, Firm Mines Wealth Of Personal Data*, WASHINGTON POST at A01, Jan. 20, 2005, available at <http://www.washingtonpost.com/wp-dyn/articles/A22269-2005Jan19.html> (last visited October 7, 2009).

communications data, which has been enacted in Europe and which the security establishment would like to enact in the United States.⁷

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,⁸ 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.⁹

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.¹⁰

Solutions

There are at least two key areas for possible legislation or regulation which would not only protect consumer privacy but also limit the widespread collection of information by the government: data retention and third party access.

Data Retention

Currently, there is no uniform practice or industry standard regarding data retention limitations for information detailing consumers’ online habits. The Federal Trade Commission

⁷See Declan McCullagh, “FBI director wants ISPs to track users,” CNET News, Oct. 17, 2006; at http://news.cnet.com/2100-7348_3-6126877.html.

⁸The 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.

⁹“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>.

¹⁰Bureau 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).

has declined to regulate in the area of data retention, instead adopting a hands-off policy “[s]o long as self-regulation is making forward progress.”¹¹ Other uses of online information likewise remain unregulated. The result has been disparate approaches to data retention among online industry leaders.

For example, Facebook collects a wide range of information about its users, including not only content created by the users themselves but also “[i]nformation we collect when you interact with Facebook”. However, Facebook does not specify how long such information will be retained. Facebook also collects information when any logged-in user visits a third party website that contains a “like button” or “social plugin” the company’s current policy allows it to retain this information for up to 90 days in identifiable format and to retain “aggregate and anonymized data” indefinitely.¹²

Search engine giants also have widely varying policies about data retention. Google retains a complete record of every search, including the user’s complete IP address and cookie data if the user is logged into a Google account, for a full nine months. It deletes part of the IP address after nine months and deletes any associated cookie data after 18 months.¹³ Microsoft retains complete search records for six months, deletes the entire IP address after six months, and deletes any associated cookie data after 18 months.¹⁴ Yahoo! retains complete records for three months and deletes part of the IP address¹⁵ as part of a “multi-step process to replace, truncate, or delete identifiers in order to de-identify data” after three months¹⁶ before it completes an “anonymization,” in which it deletes the last octet of the IP address. Google’s cookie data used to track and analyze user search logs are retained for a full 18 months.¹⁷

These data retention limits are particularly important because they often apply to other services offered by the same company. Google, for example, offers not only a search function but also Gmail, Calendar, Maps, Picasa, YouTube, and various other services. Thus Google’s data retention policy means that Google is able to retain and analyze data about users’ web page visits, searches, online purchases, videos watched, posts on social networks, and other activities, for up to a year and a half. This creates an overwhelming, comprehensive, and intrusive picture of a user and his or her online behavior.

¹¹John Eggerton, *Liebowitz: FTC Not Interested In Regulating Behavioral Ads*, MULTICHANNEL NEWS (May 12, 2010), available at <http://www.multichannel.com/article/452585-Liebowitz-FTC-Not-Interested-In-Regulating-Behavioral-Ads.php>.

¹²Facebook Help Center, Social Plugins and Instant Personalization, <http://www.facebook.com/help/?faq=17512>. In addition, Facebook publicly announced this policy only after the press revealed the fact that the like button and social plugins allowed Facebook to collect this information. See Declan McCullagh, *Facebook 'Like' Button Draws Privacy Scrutiny*, CNN.com, June 2, 2010, <http://www.cnn.com/2010/TECH/social.media/06/02/cnet.facebook.privacy.like/index.html>.

¹³See Google privacy FAQ at: http://www.google.com/intl/en/privacy_faq.html#toc-anonymize.

¹⁴See Bing Community, Updates to Bing Privacy, at <http://www.bing.com/toolbox/blogs/search/archive/2010/01/19/updates-to-bing-privacy.aspx>.

¹⁵N.Y. Times, *Yahoo Limits Retention of Personal Data*, <http://www.nytimes.com/2008/12/18/technology/internet/18yahoo.html>.

¹⁶See Yahoo! Privacy Policy, Data Storage and Anonymization, at <http://info.yahoo.com/privacy/us/yahoo/datastorage/>.

¹⁷See Google privacy FAQ at: http://www.google.com/intl/en/privacy_faq.html#toc-anonymize.

Imagine then if this vast amount of information were turned over to law enforcement or other government agencies. This would give the government unprecedented access to the lives and actions of law-abiding Americans and provide opportunities for government surveillance more intrusive than ever before. With access to the records held by online entities, the government could compile both broad and incredibly detailed profiles of people's activities and behaviors: not only who your friends are but where you met and how often you interact; not only which books you read but how you found them and which page you read most recently; not only which religion you claim but how often you actually attend services. The list of information that could be derived by government actors from data stored by private entities spans the entire spectrum of modern life.

Unfortunately, this “imaginary” scenario is all too real, as the line between commercial data and the government becomes increasingly indistinct. For example, in 2003 the online retailer eBay stated that “if you are law enforcement agency you can fax us on your letterhead to request information: who is that beyond the seller ID, who is beyond this user ID. We give you their name, their address, their e-mail address and we can give you their sales history without a subpoena.” (sic)¹⁸ Google reported that it received over 3,500 demands for information in the last six months of 2009.¹⁹ If Google is receiving thousands of demands digging into the intimate details of individual lives captured in emails, search histories, reading and viewing logs, and elsewhere, how many more are going out to Yahoo, Microsoft, Facebook and the thousands of other online services that Americans use every day?

Reducing the amount of information held by private parties can address this threat without severely impacting internet commerce. Recent research suggests that data reaches its maximum potential for marketing purposes in approximately twenty-four hours.²⁰ Forward-thinking companies have started to set data retention policies that reflect the reality that business needs do not require long retention times, while continuing to store data unnecessarily increases the privacy risks to consumers. Ask.com developed the AskEraser, allowing users to conduct online searches without the company logging any information. In 2008, Yahoo! announced an anonymization policy to de-identify most user log files records after three months. Yahoo!’s policy applies to user’s web search data, information that tracks user’s web page and advertisements views, and mouse click data.²¹

¹⁸ See Lawmeme, Ebay to Law Enforcement, <http://lawmeme.research.yale.edu/modules.php?name=News&file=article&sid=925>. This policy seems to remain largely in force: according to eBay's current privacy policy, in response to a “verified request relating to a criminal investigation or alleged illegal activity,” eBay will disclose “information relevant to the investigation, such as name, city, state, zip code, telephone number, email address, User ID history, IP address, fraud complaints, and bidding and listing history.”

¹⁹ Government Requests Tool, <http://www.google.com/governmentrequests>. Note this does not include National Security letters or demands received outside of criminal investigations. It also does not count the actual number of users whose records disclosed pursuant to each demand. All of this means this number likely only reflects a fraction of the number of users whose records were demanded.

²⁰ See Jun Yan, Ning Liu, Gang Wang, Wen Zhang, Yun Jiang & Zheng Chen, *How much can Behavioral Targeting Help Online Advertising?* (2009), available at <http://www2009.eprints.org/27/1/p261.pdf>.

²¹ See Yahoo.com, Yahoo! Privacy Policy: Data Storage and Anonymization, <http://info.yahoo.com/privacy/us/yahoo/datastorage/details.html> (last visited July 26, 2010).

These consumer friendly policies demonstrate that it is possible to balance the need for innovative services and technological advances with the important priority of giving users adequate privacy protections. The ACLU encourages this committee to safeguard consumers by enacting mandatory data retention limitations for online service providers.

Third-Party Access

Online behavioral advertising and other online information services involve the collection of a staggering amount of information about people's online activities and the aggregation of that information in a few central locations.²² For example behavioral marketers seek to form a thorough picture of users. They do so by combining information gleaned from different web sites over time, including web page visits, searches, online purchases, videos watched, posts on social networking, and other sources.²³ Any particular website may provide little information, but when a large number of these data points are aggregated, the result is an extremely detailed picture.²⁴

A striking recent development involves the potential to collect data from social networking sites like MySpace, Facebook, Twitter, and LinkedIn. Many of these sites explicitly allow third parties, including advertisers, to access information about their users through various means.²⁵ In addition, a scholarly paper reports that eleven of twelve sites studied had the potential to "leak" personally identifiable information about users unintentionally to advertisers and other third parties, including information such as name, address, phone number, gender, and birthday.²⁶

The collection of this online information is frequently being matched with real-world, offline identities. One expert, Professor Ed Felton, recently discussed the process by which an

²²*Behavioral Advertising: Industry Practices and Consumers' Expectations: Hearing before the H. Subcomm. on Communications, Technology and the Internet of the H. Comm. on Energy and Commerce, and the H. Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce*, 111th Cong. (2009) (Statement of Edward W. Felton, Professor of Computer Science and Public Affairs, Princeton University), available at http://energycommerce.house.gov/Press_111/20090618/testimony_felton.pdf (last visited October 7, 2009); *id.* (Statement of Jeff Chester, Executive Director, Center for Digital Democracy).

²³Felton, *supra* note 15, at 3-4; CENTER FOR DIGITAL DEMOCRACY, ET AL., ONLINE BEHAVIORAL TRACKING AND TARGETING: LEGISLATIVE PRIMER 2009 3, available at <http://www.uspirg.org/uploads/s6/9h/s69h7ytWnmbOJE-V2uGd4w/Online-Privacy---Legislative-Primer.pdf> (last visited October 5, 2009); see also OMNITURE, THE RISE OF ONSITE BEHAVIORAL TARGETING 1 (May 2008) ("On-site Behavioral Targeting leverages each individual Web visitor's observed click-stream behavior, both on the current Web visit and from all previous visits, to decide what content is likely to be most effective to serve to that visitor."), available at <http://www.omniture.com/offer/281> (last visited October 7, 2009).

²⁴Felton, *supra* note 15, at 3-4; Chester, *supra* n.15, at 8-10; Electronic Frontier Foundation, How Online Tracking Companies Know Most of What You Do Online (and What Social Networks Are Doing to Help Them), Sept. 21, 2009, <http://www EFF.org/deeplinks/2009/09/online-trackers-and-social-networks> (last visited October 7, 2009).

²⁵ These sites ordinarily provide some form of user control over this data sharing. However, approximately 90% of users do not take advantage of privacy controls to limit access by third parties. Chester, *supra* note 15, at 3. In addition, even when available and used, these controls often prove ineffective against technically-savvy snoopers. *Id.*

²⁶ BALACHANDER KRISHNAMURTHY & CRAIG E. WILLS, ON THE LEAKAGE OF PERSONALLY IDENTIFIABLE INFORMATION VIA ONLINE SOCIAL NETWORKS (2009) available at <http://conferences.sigcomm.org/sigcomm/2009/workshops/wosn/papers/p7.pdf> (last visited October 6, 2009).

online ad service might combine its user profile with information purchased from a commercial database: “If the ad service does know the identity, then third party services can provide a wealth of additional information, such as the user’s demographics, family information, and credit history, which can be incorporated into the ad service’s profile of the user, to improve ad targeting.”²⁷ While Professor Felten was careful to make clear that “the fact that something is possible as a technical matter does not imply that reputable ad services actually do it,”²⁸ it seems likely the process is not uncommon. For example, the company Comscore, a leading provider of website analytic tools, boasts that “online behavioral data can... be combined with attitudinal research or linked with offline databases in order to diagnose cross-channel behavior and streamline the media planning process.”²⁹

This aggregated information can then be much more easily accessed by the government. This risk is certainly not theoretical. The FBI has admitted that it purchases information from “a lot of different commercial databases. . . ,” and stated that once that information is collected by those databases, “we legitimately have the authority to obtain ‘that information’.”³⁰ Given the government’s demonstrated drive to access both online data and commercial databases of personal information, it seems nearly certain that law enforcement and other government actors will purchase or otherwise access the type of detailed profiles of online behavior compiled by behavioral marketers and others.

The best solution to this widespread surveillance of the American population is to limit the sharing of personal information with third parties and the aggregation of information into central databases. Limits on third party sharing would not hinder legitimate law enforcement investigations. Subpoenas and other law enforcement information gathering techniques would still be available to access records as part of an investigation. However, because personal information on innocent Americans would not be centralized, it would be harder to access and mass surveillance on the entire population would be more difficult. This is appropriate and necessary in our democracy. Innocent Americans have the right to be left alone. Detailed profiles of their interests, reading habits, and medical and financial information should not be readily available to their government.

Conclusion

As you consider the important issue of collection of personal information for business purposes, we hope that you will not lose sight of the government use of information collected online. As intrusive as this data collection and use of information may be when performed by individual online advertisers and service providers, it is even more alarming when this information is disclosed to the government. The current legal framework offers little meaningful protection against such surveillance. Therefore, it is crucial that new laws addressing online privacy create a framework for data retention limitations and bars on third party data collection that help limit unwarranted government access of this information.

²⁷Felten, *supra* n.15 at 4.

²⁸*Id.*

²⁹Why Comscore?, http://comscore.com/About_comScore/Why_comScore (last visited October 6, 2009).

³⁰Harris, *supra* n.5 (quoting F.B.I. spokesman Ed Cogswell).