November 2, 2009

Chairman Patrick Leahy
Senate Judiciary Committee
United States Senate
Washington, DC 20510

Ranking Member Jeff Sessions
Senate Judiciary Committee
United States Senate
Washington, DC 20510

AMERICAN CIVIL LIBERTIES UNION
NATIONAL OFFICE
125 BROAD STREET 18TH FL
NEW YORK NY 10004-2400
T/212.549.2500
WWW.ACLU.ORG

Re: S. 1490 - Personal Data Privacy and Security Act

Dear Chairman Leahy and Ranking Member Sessions:

We are writing to express our support for S. 1490, the Personal Data Privacy and Security Act, which regulates the data aggregation industry and restricts the use of personal data from this industry by the government. These common sense regulations require the industry to be accurate and transparent as it handles the personal data of hundreds of millions of Americans and they require the government to be clear about how it's accessing and using that information.

The ACLU is America's largest and oldest civil liberties organization, with over half a million members, countless additional activists and supporters, and 53 affiliates nationwide. We frequently comment on privacy, surveillance, and the government's use of personal information collected by private parties.[1]

Data Aggregators

Data aggregators are companies interested in compiling detailed electronic dossiers of individuals' activities by drawing together data from a variety of sources and then selling that information for many purposes including marketing, background checks and law enforcement investigations. These companies, which include Acxiom, Lexis-Nexis (which recently purchased ChoicePoint), and many others, 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

[1] For more on this topic please see our report on the surveillance industrial complex available here: http://www.aclu.org/safefree/resources/18512res20040809.html.

requirement by simply purchasing information that has been collected by data aggregators.[2]

Data aggregators were originally fueled by the economic drive to make corporate marketing campaigns more efficient. Now, however, they exist in a world where their work is increasingly frightening and politically charged. The post-9/11 environment has spurred a government hunger to gather as much data as it can and the companies' success in gathering data has simply boosted the government's addiction.

Data companies collect information from courthouses and other public sources, as well as marketing data – sometimes including intensely personal information, such as lists of individuals suffering from incontinence, prostate problems and clinical depression.[3] Some databases are even co-operative endeavors in which companies agree to contribute data about their own customers in return for the ability to pull out rich profiles of their customers based on the data contributed by all members.

Use and misuse of these databases is causing serious harm to Americans:

- A drug store declined to hire an applicant for a management position because a ChoicePoint database contained a complaint from a former employer accusing the applicant of shoplifting. Although a state administrative proceeding exonerated the employee, ChoicePoint would not correct the database because the report "merely conveyed information provided by a former employer."[4]

- A company declined to hire an unemployed truck driver because a record maintained by USIS in its "Drive-A-Check" database—used by thousands of trucking companies—stated that he was fired by a former employer for making "excessive complaints" and a "company policy violation." A Department of Labor administrative law judge ruled the former employer wrongly terminated the driver for making legitimate safety complaints and ordered the employer to delete "any unfavorable work record information." Nevertheless, the record remained uncorrected for several years. A USIS spokesperson defended the record, saying it "was an accurate portrayal of what led to his termination."[5]

- A department store fired a woman because a background file maintained by USIS and a Florida screening firm, Merchants Security Exchange, stated she had stolen merchandise from a former employer. She denied the allegations. After she filed suit in federal court,

---

[2] 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).

[3] Chris Hoofnagle, "Barriers to the Constitutional Right to Privacy: Big Business is keeping an eye on you," *San Francisco Chronicle,* January 29, 2004, *available at* http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2004/01/29/EDGH14JBAN1.DTL .

[4] Chad Terhune , "The Trouble with Background Checks," *Business Week*, May 29, 2008, *available at* http://www.businessweek.com/magazine/content/08_23/b4087054129334.htm

[5] *Id.*

USIS corrected its file, and Merchant's Security Exchange changed her file so that it noted a company "policy violation" in connection with her use of an employee-discount card. She was unable to receive damages or get her file changed further and her suit was dismissed because the database had not violated any law.[6]

- Home Depot turned down a job applicant because of a serious error in a Choicepoint background check. Thirty years before, the applicant had served 60 days for a misdemeanor, but the report stated he had served 7 years for a felony. ChoicePoint and the state justice system blamed one another for the error. After many phone calls and emails, the error was corrected, but the applicant believes the error cost him many jobs before he learned of the problem.[7]

- A California man with a common name discovered that his file from backgroundchecks.com attributed to him a variety of serious crimes committed by other people with the same name, including a Florida prostitution charge committed by a woman. He spent considerable money and time clearing his record, which he believed prevented him from getting insurance and a number of jobs. The president of background checks.com stated, "We're not in the business of authenticating the identity of individuals. All we do is report the data that's supplied to us from the courts."[8]

Federal and State government

The government is a steady customer for the services of these aggregators. One of the biggest data aggregators, LexisNexis, claims to have clients in "insurance, law enforcement, government agencies, financial services firms, collection agencies, health care providers, and others".[9] According to FOIA records obtained by Wired News, the Federal Bureau of Investigation data warehouse contains more than 190 million records from data aggregator such as Accurint, ChoicePoint, LexisNexis and Acxiom.[10]

State fusion centers make extensive use of these databases.[11] According to media reports most of the centers have subscriptions to Accurint, ChoicePoint's Autotrack or LexisNexis.[12] In Maryland, authorities rely on a little-known data broker called Entersect, which claims it

---

[6] *Id.*
[7] Kim Zetter, "Bad Data Fouls Background Checks," *Wired*, March 11, 2005. http://www.wired.com/politics/security/news/2005/03/66856
[8] *Id.*
[9] LexisNexis website, last visited October 27, 2009. http://www.choicepoint.com/about/overview.html
[10] Ryan Singel, "Newly Declassified Files Detail Massive FBI Data-Mining Project," *Wired Magazine Threat Level*, September 23, 2009, *available at* http://www.wired.com/threatlevel/2009/09/fbi-nsac/.
[11] State fusion centers are offices which bring together federal, state and local police to share intelligence and law enforcement information.
[12] Robert O'Harrow Jr, "Centers Tap Into Personal Databases," *Washington Post,* April 2, 2008, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/04/01/AR2008040103049.html; Joseph Straw, "Fusion Centers Forge Ahead", *Security Management*, October 2009, *available at* http://www.securitymanagement.com/article/fusion-centers-forge-ahead-006223.

maintains 12 billion records involving about 98 percent of Americans.[13] Massachusetts and other states rely on LocatePlus, an information broker that claims it provides "the most comprehensive cell phone, unlisted and unpublished phone database in the industry." The state also taps a private system called ClaimSearch that includes a "nationwide database that provides information on insurance claims, including vehicles, casualty claims and property claims."[14]

The government is not just dipping into a pre-existing commercial marketplace to purchase data. Companies are actually creating and shaping their products to meet the needs of government security agencies.[15] Private companies are increasingly moving in to perform functions that used to be carried out by the police and can provide officers with information. However, in order to be competitive, these companies are collecting increasingly invasive information on individuals – such as a list of a person's past roommates – that would spark outrage if maintained directly by the police in their own files.

Regulation of data aggregators

Section 201 of the Personal Data Privacy and Security Act is an excellent beginning in the effort to reign in the out of control misuse of American's personal data by data aggregators. It contains three key requirements:

- **Transparency.** Currently data aggregators are not required to, and usually don't, provide consumers with access to the records and personal information that they hold on each individual. While these companies sell this information to the highest bidder and make it readily available to anyone running a background check, consumers remain in the dark. Section 201 changes this by allowing consumers to access their own records for a reasonable fee. This fee should be set very low by regulation (or even waived in some cases) because this process actually *benefits* data aggregators by allowing them to offer a better product – one that is more accurate and hence more effective.
- **Notice.** As many of the cited examples illustrate, consumers often do not know they are the victims of mistaken information. Section 201 requires entities to notify consumers when they take an adverse action based on information provided by a data broker.
- **Accuracy.** Under Section 201 consumers will be able to contest the accuracy of information and learn the source of that information. This basic right will help prevent some of the most troubling aspects of the current regime—anonymous reporting and the inaccuracies that it breeds

These three items are a baseline for any fair use of consumer information. It is startling that this industry has existed so long without these fundamental protections. These proposals are in fact very modest. S. 1490 does not even address the more basic question of whether it is appropriate for any company to acquire intimate and personal information about Americans without their permission. It fails to limit how long information can be held, with whom it can be shared or for

[13] *Id*, O'Harrow.
[14] *Id*.
[15] Hoofnagle "Little Helpers," *supra* n.3, at 611.

what purposes (aside from prohibiting identity theft) that it can be used. S. 1490 is an important and necessary set of protections for consumers but it is not radical or all-encompassing. It is merely basic consumer protection.

Safeguards on government use of the data

S. 1490 contains important protections and limitations for government access and use of information from data aggregators. The government has extensive and ongoing contracts with data aggregators including access to information on criminal history, DNA analysis, consumer purchasing habits and credit history, pilot and gun licenses, vehicle registration, marriage and death certificates, eviction notices, and even lists of family and associates.[16] Data aggregators are increasingly combining this information with online content such as consumers surf habits, web searches and online purchases.[17] This information is then shared with law enforcement and other agencies. The public has the right to know what data the government is accessing and deserves an assurance that data is being used in a responsible and carefully circumscribed way.

In addition to mandating that databases be secure and accurate, Title IV of S. 1490 requires that agencies using data aggregators must:

- Provide a full description of the databases, the data aggregators that provide them, and the agency personnel authorized to access them;
- Access only the minimum amount of personal information necessary to accomplish the legitimate purpose of the agency;
- Ensure that the data meets standards for accuracy, relevance and completeness;
- Limit the retention and re-disclosure of information from these databases;
- Audit the databases for security;
- Provide redress for errors; and
- Outline enforcement mechanisms for accountability.

These provisions would provide the first ever meaningful oversight of the government's extensive use of data aggregators. They would require data aggregator databases, which are operating as de facto government databases, to comply with many of the same requirements as real federal databases.

These are not radical proposals. They do not address the more fundamental issue of whether law enforcement should *ever* access a database about consumer preferences and purchasing habits. Instead S. 1490 simply advances the common sense principle that all

---

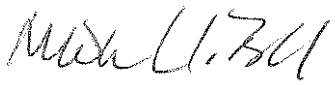
[16] *See* Shane Harris, "FBI, Pentagon pay for access to trove of public records," *National Journal*, November 11, 2005, *available at* http://www.govexec.com/story_page.cfm?articleid=32802; Robert O'Harrow Jr., "In Age of Security, Firm Mines Wealth Of Personal Data," *Washington Post*, January 20, 2005, *available at* http://www.washingtonpost.com/wp-dyn/articles/A22269-2005Jan19.html.

[17] 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." http://comscore.com/About_comScore/Why_comScore (last visited October 6, 2009)

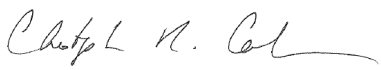
databases used by the government should have the same protections – whether they are created by the government or merely accessed by the government.

We support S. 1490 because it is a common sense effort to regulate an industry that desperately needs it. Data aggregators exploit Americans' privacy for profit and are able to do so because of poor existing data privacy laws. It is not only appropriate but necessary that these companies be regulated both in the information they gather and their transactions with the government.

Sincerely,



Michael W. Macleod-Ball
Acting Director, Washington Legislative Office



Christopher Calabrese
Legislative Counsel

cc: Senate Judiciary Committee