CRS Issue Statement on Privacy and Data Security

Gina Stevens, Coordinator
Legislative Attorney

June 9, 2010

Congressional Research Service
7-5700
www.crs.gov
IS40366

CRS Report for Congress
Prepared for Members and Committees of Congress

Issues likely to be of concern to Congress include online behavioral advertising, financial privacy, health information technology and privacy, social security number privacy, and data mining. Data security issues of possible interest to lawmakers are data breach notification requirements, customer access to and amendment of records, enhanced enforcement authority for the Federal Trade Commission and state attorneys general, and preemption of state data breach laws.

Privacy

Online Behavioral Advertising. The monitoring of consumers' web activity for marketing purposes will likely continue to be an important privacy issue in the 111th Congress. Technology has been developed which enables online advertisements to be targeted directly at individual users based on their web activities. This practice is widely known as online "behavioral" advertising. Gathering personally identifiable information about an individual's web activities without consent has raised privacy concerns. Some have alleged that online behavioral targeting by advertisers is a violation of certain privacy laws, such as the Electronic Communications Privacy Act and provisions within the Communications Act of 1934. There are no current federal regulations specific to online behavioral advertising. The Federal Trade Commission (FTC) has put forth guiding principles for industry self-regulation. Meanwhile, privacy advocates have called for government regulation in order to protect consumer privacy. Organizations such as the Network Advertising Initiative have created privacy policies for online advertising providers that represent industry best practices. Members have expressed interest in legislative action. Among the issues that might emerge for online behavioral advertising are: If legislation is enacted to require consent and disclosure of online behavioral advertising practices, what will the disclosure look like? How will consent be obtained? Will there be classifications of data that may be collected, and, if so, will there be different methods of obtaining consent for the collection of the different classes of data? How long may data be maintained? It is expected that the 111th Congress will address these issues through oversight and legislative proposals.

Financial Privacy. With modern technology's ability to gather and retain data, financial services businesses have increasingly found ways to take advantage of their large reservoirs of customer information. Not only can they serve their customers better by tailoring services and communications to customer preferences, but they can profit from sharing that information with others willing to pay for customer lists or targeted marketing compilations. Although some consumers are pleased with the wider access to information about available services that information sharing among financial services providers offers, others have raised privacy concerns, particularly with respect to secondary usage.

Title V of the Gramm-Leach-Bliley Act of 1999 (GLBA) (P.L. 106-102) covers financial institutions. Banks, thrifts, securities firms, insurance companies, credit unions and other providers of financial services are subject to the Gramm-Leach-Bliley Act's (GLBA) privacy regime covering disclosures of nonpublic personal information to third parties and standards for safeguarding such information. Subject to certain exceptions, it prohibits them from sharing nonpublic personally identifiable customer information with non-affiliated third parties without providing an opportunity to opt out and mandates various privacy policy notices. It requires financial institutions to safeguard the security and confidentiality of customer information. Among the issues that might emerge are: If general data breach bills are enacted, will entities subject to GLBA rules be given a safe harbor? Will additional enforcement tools, such as a private right of action or enforcement by states' attorneys general, be added to the GLBA regime?

Will there be statutory requirements for financial institutions to include in outsourcing contracts? It is expected that in the 111th Congress there will be legislative proposals to enhance the protection offered personal financial information.

Consolidation in one regulator of federal financial consumer protection authority—including rulemaking and enforcement authority over GLBA's privacy provisions—is a component of several 111th Congress bills.

Health Information Technology. Electronic health records are controversial among many privacy advocates and citizens, who are concerned about information security and the potential for the exploitation of personal medical information by hackers, companies, or the government, and the sharing of health information without the patients' knowledge. The American Recovery and reinvestment Act of 2009 (P.L. 111-5) incorporated the Health Information Technology for Economic and Clinical Health (HITECH) Act. The HITECH Act, based on legislation introduced in the 110th Congress, is intended to promote the widespread adoption of health information technology (HIT) for the electronic sharing of clinical data among hospitals, physicians, and other health care stakeholders. First, it codifies the Office of the National Coordinator for Health Information Technology (ONCHIT) within the Department of Health and Human Services (HHS). Second, the HITECH Act provides financial incentives for HIT use among health care practitioners. Finally, the HITECH Act includes a series of privacy and security provisions that amend and expand the current HIPAA requirements. Among other things, the HITECH Act extends application of the HIPAA Privacy and Security Rules to the business associates of health care entities, establishes a new federal data breach law for health information, and includes new tools for enforcement of the HIPAA Privacy and Security Rules.

In light of the fact the Congress has recently passed legislation to promote widespread adoption of HIT and use of electronic health records, congressional attention during the 111th Congress is likely to be focused on oversight activities.

Social Security Number Privacy. The privacy of a person's social security number is of significant concern to individuals both for security of personal information and for preventing identity theft. A patchwork of federal laws limits compulsory divulgence of social security numbers (SSNs)by federal, state, and local governmental entities. Private sector use of the social security number is, however, widespread and continues to be largely unregulated by the federal government. Recently Congress has sought to further limit uses of the social security number, and is likely to continue to examine such measures, including proposals to remove social security numbers from Medicare cards, and to limit or prohibit the sale or purchase of SSNs.

Data Mining. Data mining technologies and related analysis programs can be used by government agencies to sift through information held in public and private databases; to find patterns and associations connected to terrorist threats and activities, such as money transfers and communications; and to identify and track terrorists, such as through travel and immigration records. As data mining technology advances in the quantity and scope of data that can be analyzed, and as data mining efforts by federal agencies continue to expand, concerns over individual privacy will likely be raised. Congressional oversight of such data mining programs may examine whether the programs maintain the information in a manner that insures privacy and protects against its loss and against inappropriate use or disclosure. Other considerations include access to commercial databases by government agencies and the retention of such data by the government, whether data is being used for purposes other than those for which it was originally collected, and the application of the Privacy Act of 1974 to these data mining initiatives.

Data Security

In the absence of a comprehensive federal data breach notification law, many states enacted laws requiring notice of security breaches of personal data. The majority of states have passed bills to require entities to notify persons affected by breaches involving their personal information, and in some cases, to implement information security programs to protect the security, confidentiality, and integrity of data. A few states have reportedly introduced bills designed to strengthen merchant security and/or hold companies liable for third party companies' costs arising from data breaches. In response to these laws, numerous data breaches and computer intrusions have been disclosed by the nation's largest data brokers, retailers, educational institutions, government agencies, health care entities, financial institutions, and Internet businesses. A data breach occurs when there is a loss or theft of, or other unauthorized access to, data containing sensitive personal information that results in the potential compromise of the confidentiality or integrity of data. Sensitive personal information generally includes an individual's name, address, or telephone number, in conjunction with the individual's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password.

Concerns about possible identity theft and financial crimes (e.g., credit card fraud, phone or utilities fraud, bank fraud, mortgage fraud, employment-related fraud, government documents or benefits fraud, loan fraud, and health-care fraud) resulting from such breaches are widespread. According to the Federal Trade Commission, identity theft is the most common complaint from consumers in all 50 states. Identity theft involves the misuse of any identifying information to commit a violation of federal or state law.

These public disclosures have heightened interest in the security of sensitive personal information; security of computer systems; applicability of existing federal laws to the protection of sensitive personal information; adequacy of enforcement tools available to law enforcement officials and federal regulators; regulation of data brokers; liability of retailers, credit card issuers, payment processors, banks, and furnishers of credit reports for costs arising from data breaches; remedies available to individuals whose personal information was accessed without authorization; prosecution of identity theft crimes related to data breaches; and criminal liability of persons responsible for unauthorized access to computer systems.

Congress continues to consider the creation of a legal framework to respond to improper disclosures of personally identifiable information; and whether to require covered entities to implement information security plans. Key areas of attention involve data breach notification requirements; safe harbors for entities regulated under federal privacy laws; customer access to and amendment of records; creation of a private right of action; the right to place a credit freeze or fraud alert on one's credit report; restrictions on the sale and use of social security numbers; enhanced enforcement authority for the Federal Trade Commission and state attorneys general; and preemption of state data breach laws.

Computer Security

Cybercrimes. With the proliferation of potential uses and abuses of the Internet, the crime of Internet harassment presents challenges for law enforcement, legislators, educators, and parents. These challenges are exacerbated by a lack of uniformity in defining the terms cyberharassment and cyberbullying. In addition, jurisdictional limits and the anonymity of the Internet sometimes

make it difficult for law enforcement personnel to identify, locate, arrest, and prosecute alleged offenders. As Internet harassment may cause its victims emotional harm as opposed to physical harm, legislators must determine what level, if any, of harassment should be criminalized.

Issue Team Members

Gina Stevens, Coordinator
Legislative Attorney
gstevens@crs.loc.gov, 7-2581

Charles Doyle
Senior Specialist in American Public Law
cdoyle@crs.loc.gov, 7-6968

Kathleen S. Swendiman
Legislative Attorney
kswendiman@crs.loc.gov, 7-9105

M. Maureen Murphy
Legislative Attorney
mmurphy@crs.loc.gov, 7-6971

Kathleen Ann Ruane
Legislative Attorney
kruane@crs.loc.gov, 7-9135

Margaret Mikyung Lee
Legislative Attorney
mmlee@crs.loc.gov, 7-2579

Jody Feder
Legislative Attorney
jfeder@crs.loc.gov, 7-8088

Patricia Moloney Figliola
Specialist in Internet and Telecommunications Policy
pfigliola@crs.loc.gov, 7-2508

John D. Moteff
Specialist in Science and Technology Policy
jmoteff@crs.loc.gov, 7-1435

Rita Tehan
Information Research Specialist
rtehan@crs.loc.gov, 7-6739

Vastine D. Platte
Information Research Specialist
vplatte@crs.loc.gov, 7-7975

Amanda K. Sarata
Analyst in Health Policy and Genetics
asarata@crs.loc.gov, 7-7641

Anna C. Henning
Legislative Attorney
ahenning@crs.loc.gov, 7-4067

Alison M. Smith
Legislative Attorney
amsmith@crs.loc.gov, 7-6054

John F. Sargent Jr.
Specialist in Science and Technology Policy
jsargent@crs.loc.gov, 7-9147

Kristin M. Finklea
Analyst in Domestic Security
kfinklea@crs.loc.gov, 7-6259

For detailed information select from the following topical links.

Privacy and Data Security

Data Security

Federal Information Security and Data Breach Notification Laws

Identity Theft: Trends and Issues

Privacy

Privacy Law and Online Advertising

Advertising Industry in the Digital Age

Spyware: Background and Policy Issues for Congress

Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping

U.S. Initiatives to Promote Global Internet Freedom: Issues, Policy, and Technology

Privacy Protection for Customer Financial Information

The Social Security Number: Legal Developments Affecting Its Collection, Disclosure, and Confidentiality

Compulsory DNA Collection: A Fourth Amendment Analysis

The Family Educational Rights and Privacy Act (FERPA): A Legal Overview

Computer Security

Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations

Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws