Protecting Information Privacy Per U.S. Federal Law

Virginia A. Jones, CRM, FAI

Protecting the privacy of internal and external customers is a critical responsibility for those with records and information management responsibilities. This article provides a high-level overview of privacy issues and broadly applicable U.S. federal laws governing them.

Business and government entities must understand and apply increasingly complex laws and regulations to protect the data and records of their customers and citizens. Compliance with U.S. personal information protection laws is often difficult due to the number and interrelationship of federal and state laws and regulations that affect or relate to these issues.

In 2013, nearly 58 million records were reported compromised in the United States according to the Identity Theft Resource Center. With increased collection of data and easier methods of collection, protecting personal information has become a big issue in today's business and government environment.

Contributing Factors to Data Breaches

There is now prolific and far-reaching collection and distribution of personally identifiable information (PII) due to increased use of the Internet for a number of activities such as conducting business meetings, interacting with government, personal and business banking and other financial transactions, data vaulting, shopping, socializing, and even attending classes.

Online Transactions

There is a generational trust of and reliance on computerized data with a desire for easier and quicker methods to conduct these actions. The need to more quickly access information or activities leads many to submit personal information online and, in doing so, leave themselves open to unauthorized access to their personal information.

Often online submittal of PII either explicitly or implicitly authorizes data sharing between entities. While several U.S. federal laws require an "opt-out" opportunity to be provided by online businesses to allow consumers to choose not to have their data shared (or even marketed), it is not always obvious to the user that a choice exists or, in many cases, the user does not pay attention to the choice.

Data Sharing

To increase efficiency, data is frequently shared by those who collect it. In the private sector, acquired data is often shared or sold. Acquisitions and mergers of business entities also might provide useable data to disparate sectors of business. For example, an entertainment company might buy a mortgage company, giving it access to personal information it would not otherwise collect. In the government sector, collected data is often shared between agencies to expedite processes and to determine eligibility for a variety of programs and benefits. In fact, the EGovernment Act of 2002 encourages the sharing of various data between certain federal agencies when appropriate.

Ease of Access

Exposure to privacy information breaches is compounded by the ease of access to personal information. The use of Google, Yahoo, AnyWho, or other search engines and locators makes it easier to obtain the personal information of others through increased hacking into computer systems, Internet phishing, and just plain stealing hard media or information from hard media, such as credit cards, credit card statements, checks, and other documents containing PII thrown in the trash or recycling. This proliferation of accessible personal information has resulted in misuse of personal information by the unscrupulous through identity theft, spamming, stalking, or preying.

Increase in Social Security Numbers Issued

The most overused personal information is the Social Security Number (SSN). Originally established in 1935 by the federal government as part of the Social Security program requiring employees to contribute a portion of their earnings toward a national retirement fund, the issuance of SSN was expanded in the 1970s to include newborns and non-employed residents in the United States.

With the majority of the population having a centrally recorded identification number, the SSN became an accurate method of uniquely identifying individuals. Businesses and government required the SSN for a number of services and benefits, even for accepting personal checks. One of the earliest abuses of personal privacy was the stealing and misuse of SSN.

As breaches and misuse of personally identifiable information became more prevalent, laws became necessary to prevent misuse, to prevent unauthorized sharing, and to ensure protection of individual personal information. A variety of federal laws have been enacted that require organizations to be responsible for the privacy of certain records and data.

Right to Privacy Established

In Public Law 93-579, enacted in 1974 as the Privacy Act, Congress found that the right to privacy is a personal and fundamental right protected by the Constitution of the United States. The need for information privacy encom-

passes all segments of the population.

Citizens are affected by government data collection and dissemination, and a number of privacy laws apply directly to this sector. Employees are affected by employer data collection and dissemination and the use made of the data by employers. Customers/consumers are affected by business data collection and dissemination and how well the data may be protected. Medical care recipients are affected by data collection and dissemination by medical care, medicine, and medical supplies providers and how the data is protected, shared, and accessed.

There is no one definition of "personally identifiable information" in U.S. federal law. Where a definition is listed, there is some variance from law to law. For the most part, definitions of the term are based, in part or in whole, on the definition set by the Federal Trade Commission (FTC) in "Online Profiling: A Report to Congress":

> Data that can be linked to specific individuals, and includes but is not limited to such information as name, postal address, phone number, e-mail address, social security number and driver's license number.

Depending on the act, PII can also include medical information, financial information, political affiliation, educational records, social organization affiliation, video viewing preferences, and religious affiliation.

There is agreement in privacy laws in the need to protect the SSN. At least five federal laws restrict the use or disclosure of SSN, including the Fair Credit Reporting Act, the Fair and Accurate Credit Transactions Act, the Graham-Leach-Bliley Act, the Drivers Privacy Protection Act, and the Health Insurance Portability and Accountability Act.

A 2007 memorandum from the Office of Management and Budget, required federal agencies to review their use of SSN in their systems and programs to identify superfluous collection or use of SSN and to eliminate unnecessary collection and use by mid-2010. Agencies were also asked to participate in government-wide efforts to explore alternatives to the SSN as a personal identifier for both federal employees and in federal programs.

Classes of Privacy

According to *Information Privacy, Official Reference for the Certified Information Privacy Professional (CIPP)* by Peter P. Swire, CIPP, and Sol Bermann, CIPP, privacy can be categorized into four classes.

- *Information privacy* is concerned with establishing rules that govern the collection and handling of personal information, including credit information, medical data, and government records.
- *Bodily privacy* is focused exclusively on a person's physical being and any invasion thereof, such as genetic testing, drug testing, or body cavity searches.
- *Territorial privacy* is concerned with placing limitations on the ability of one to intrude into another individual's environment. This may be the home, workplace, or public space and can extend to an international level. Invasion typically comes in the form of video surveillance, ID checks, and use of similar technology and procedures.
- *Communication privacy* encompasses protection of the means of correspondence, including postal mail, telephone conversations, electronic mail, and other forms of communicative behavior and apparatus.

Citizens are affected by government data collection and dissemination.

Impacts on RIM

Information privacy is the class that directly relates to records and information management (RIM). Communication privacy also impacts RIM through correspondence issues. The records management impacts of the laws and regulations discussed in this paper are based on the records management life cycle concept – from creation/receipt of the records and data to final disposition. Although not all laws have all elements, privacy law can impact records creation, file management for both active and inactive records, records protection, records access, and records retention and disposition.

Recordkeeping Requirements

The impact on records creation can be either specific or implied. Wording such as "a record shall be kept of," "a report shall be generated," "a written policy shall be created," or "data about [something] shall be collected," is frequently included in the laws.

For example, the Family Educational Rights and Privacy Act requires a record to be kept of all access to or dissemination of a student's records, and the Privacy Act of 1974 requires agencies to keep an accounting of certain disclosures of personal data.

Many of the laws require the generation of reports regarding PII disclosures or breaches. Some laws include wording that directs or implies how the record file should be managed. The Americans with Disabilities Act, for example, states specifically that medical records must be filed separately from other records in an employee file. The Privacy Act of 1974 requires agencies to allow a data subject to review a record about themselves and to "have a copy made of all or any portion thereof in a form comprehensible to him."

The requirement to protect records and data containing PII is implied, and often explicit, in every privacy law. For example, the Cable Communications Policy Act requires cable operators to take such actions as are necessary to

Broadly Applicable U.S. Federal Privacy Laws and Regulations

Name — Year Enacted	Scope	Applies to
Children's Online Privacy Protection Act (1998)	Governs personal information collected online that can serve to identify an individual child	Entities that collect personal information online (including websites or online services and persons who have an interest in the online collection of children's personal information)
Computer Fraud and Abuse Act (1986, amended 1990)	Governs unauthorized access to a protected computer to obtain information	Anyone accessing a computer to obtain information
Electronic Communications Privacy Act, Title 1 Wire And Electronic Communications Interception And Interception Of Oral Communications (1968)	Regulates the interception of wire, oral, and electronic communications to protect the privacy of innocent persons	Any employee or agent of the United States or any state or political subdivision thereof and any individual, partnership, association, joint stock company, trust, or corporation
Electronic Communications Privacy Act – Title II Stored Electronic Communications Privacy Act (1986)	Regulates the accessing of stored electronic communications	Any employee, or agent of the United States or any state or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation
Fair Credit Reporting Act (2003)	Addresses the use and disclosure of an individual's credit report information, including the use of credit report information by employers in making employment decisions	Consumer reporting agencies and persons who use consumer reports from such agencies, persons who furnish information to such agencies, and users of information that are subject to section 1681m
Fair and Accurate Credit Transactions Act (Amends the Fair Credit Reporting Act) (2003)	Governs opt-out notices, use of credit report information by employers in making employment decisions, and disposal of consumer credit information	Consumer reporting agencies and persons who use consumer reports from such agencies, persons who furnish information to such agencies, and users of information that are subject to section 1681m
Family Educational Rights & Privacy Act & Privacy Act	Governs privacy of student's education records	Applies to educational agencies or institutions
Financial Services Modernization Act (aka Gramm-Leach-Bliley Act) (1999)	Governs the privacy and security of personal financial information	Financial institutions
Health Insurance Portability & Accountability Act (1996)	Governs the disclosure of protected health information	Health plans, healthcare clearinghouses, and healthcare providers
Privacy Act of 1974	Governs third party access to personal information maintained by the federal government	U.S. federal executive branch
Computer Matching & Privacy Protection Act (Amends the Privacy Act of 1974) (1988, amended 1990)	Governs requirements federal agencies must follow when matching information on individuals with information held by other federal, state, or local agencies	U.S. federal executive branch
Privacy Protection Act (1980)	Governs the search for or seizure of work product or documentary materials in connections with dissemination to the public a newspaper, book, broadcast, or other similar form of public communication	Government officer or employee
Right to Financial Privacy Act (1978)	Governs access to financial records of any customer of a financial institution	Any U.S. government agency or department
Safe Harbor Data Privacy Framework (2000)	Governs transfer of personal information between the E.U. and third countries	Any organization subject to FTC jurisdiction wanting to do business with the EU, U.S. air carriers and ticket agents subject to Dept. of Transportation
Uniting & Strengthening America by Providing Appropriate Tools Required to Intercept & Obstruct Terrorism Act (aka USA Patriot Act) (Amends a number of statutes) (2001, amended 2006)	Governs the deterrent and punishment of terrorist acts in the United States and around the world and enhances law enforcement investigatory tools	Law enforcement, businesses that provide financial and communications services

prevent unauthorized access to PII by a person other than the subscriber or cable operator. Most privacy laws set penalties for failure to protect PII or for misuse or unlawful disclosure of PII.

Rights to Access Personal Info

Almost every privacy law sets some requirement for access to personal information and data. This includes requirements for who may or may not access the data, who may or may not receive the data, and the right of a *data subject* – the person the collected data is about – to inspect records and to correct records about themselves.

The Privacy Act of 1974, for example, requires an agency to allow data subjects to:

- Access their record or any information pertaining to them that is contained in the system
- Review their record
- Request amendment of their record
- Request a review of a refusal to amend their record and to clearly note any portion of the record that is disputed and, in any disclosure, provide copies of the dispute and the reason(s) for not making the requested amendments

Some of the privacy laws set requirements for records or data retention.

The Fair Credit Transaction Act requires consumer reporting agencies to disclose to data subjects all information in their file (with some exceptions) at the time of request and the right of data subjects to dispute incorrect information and require it be corrected.

Some privacy laws address permitted selling or disclosure of personal data. The Driver's Privacy Protection Act, for example, allows an authorized recipient of personal information in a motor vehicle record to resell or re-disclose the information only for a use permitted under the act, generally for motor vehicle-related reasons such as safety and theft, emissions, product alterations or recalls, and performance monitoring of vehicles. Highly restricted personal information cannot be disclosed without the permission of the data subject.

Data Retention

Some of the privacy laws set requirements for records or data retention and/or records or data disposition, although most retention requirements are usually covered in rules and regulations that are part of the Code of Federal Regulations.

Those laws that do cover retention or disposition include provisions on how long to retain records or data, how to dispose of records or data containing PII, or when to dispose of the records or data.

For instance, the Stored Electronic Communications Privacy Act (Title II of the Electronics Communications Privacy Act) requires records authorizing disclosure of a subscriber or consumer record be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

The Driver's Privacy Protection Act requires any authorized recipient that resells or re-discloses motor vehicle information to keep, for a period of five years, records identifying recipients of the information and the permitted purpose for which the information will be used.

Examples of disposal requirements include the Fair and Accurate Credit Transaction Act which requires federal banking agencies, the National Credit Union Administration, and the FTC to issue final regulations requiring the "proper disposal" of consumer information or any compilation of consumer information derived from consumer reports for a business purpose.

The Cable Communications Policy Act requires a cable operator to destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected and there are no pending requests or orders for access to such information as allowed by law or pursuant to a court order.

Responsibility for Privacy Protection

Because information privacy is integral to RIM, it should be the responsibility of the records manager (or the person whose function includes records management) to assist or advise in the establishment of processes, procedures, and monitoring for compliance with applicable laws and regulations.

Records managers should be aware of laws pertinent to their organizations, the requirements of those laws, and any pertinent rules or regulations generated under the authority of the laws. All RIM procedures and policies should include provisions for protecting personally identifiable information.

Learn More

For an extensive discussion of more than 30 U.S. federal privacy laws, as well an expanded version of the sidebar with this article, read the ARMA International Educational Foundation (AIEF) research report by this author, "Requirements for Personal Information Protection, Part 1: U.S. Federal Law," which is available for free download from the ARMA International online bookstore at *www.arma.org/bookstore*.

To learn about U.S. state privacy laws, you can also download the free AIEF research report by this author, "Requirements for Personal Information Protection, Part 2: U.S. State Laws," also available at *www.arma.org/bookstore*. **END**

Virginia A Jones, CRM, FAI, can be contacted at vjones@nngov.com. *Her bio is on page 47.*