Requirements for Personal Information Protection
Part 1: U.S. Federal Law

Virginia A Jones, CRM, FAI

October 2008
Revised February 2017

The Honorarium for this author-donated Research Project provided by:
The ARMA International Educational Foundation

www.armaedfoundation.org

TABLE OF CONTENTS

Introduction

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 2015, more than 169 million records were reported compromised in the U.S. according to the Identity Theft Resource Center.[1] 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. 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.

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 the entities. While several federal laws require an "opt-out" opportunity be provided by online businesses to allow the consumer 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.

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 E-Government Act of 2002 encourages the sharing of various data between certain federal agencies when appropriate.

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 make it easier to obtain the personal information of others through increased hacking into computer systems, internet phishing, and just plain stealing

[1] Identity Theft Resource Center, ITRC Breach Statistics Report 2015, www.idtheftcenter.org last accessed 4/1/2016

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.

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 the SSN was expanded in the 1970's to include newborns and certain non-employed residents in the U.S. 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 the SSN. In 2014, there were 338 breaches involving social security numbers with more than 164 million records breached.[2]

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.

Privacy and Records Management

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.*[3] The need for information privacy encompasses 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.

[2] Identity Theft Resource Center, 2015 Data Breaches, http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databreaches.html last accessed 4/1/2016
[3] Public Law 93-579 §2(4)

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)[4]:

> *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, personally identifiable information 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 the 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[5] requires federal agencies to review their use of the SSN in their systems and programs to identify superfluous collection or use of the SSN, and to eliminate unnecessary collection and use by mid-2010. Agencies are 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.

Privacy can be categorized into four classes[6].

- Information privacy is concerned with establishing rules that govern the collection and handling of personal information, including financial information, medical information, government records, and records of a person's internet activity.
- Bodily privacy is focused on a person's physical being and any invasion thereof, such as genetic testing, drug testing, or body cavity searches. It also encompasses issues such as birth control, abortion, and adoption.
- Territorial privacy is concerned with placing limits on the ability to intrude into another individual's environment. This may be the home, workplace or public space. Invasion typically comes in the form of video surveillance, ID checks and use of similar technology and procedures.

[4] *Online Profiling: A Report to Congress*, Federal Trade Commission, June 2000, page 4, note 14.
[5] OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007, page 7.
[6] *Foundations of Information Privacy and Data Protection*, Peter P. Swire, CIPP/US and Kenesa Ahmad, CIPP/US, International Association of Privacy Professionals (IAPP), New Hampshire, 2012, page 2

- Communication privacy encompasses protection of the means of correspondence, including postal mail, telephone conversations, email, and other forms of communicative behavior and apparatus.

Information privacy is the class that directly relates to records and information management (RIM). Communication privacy also impacts records and information management 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.

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 (FERPA) requires a record to be kept of all access to or dissemination of a student's records[7] and the Privacy Act of 1974 requires agencies to keep an accounting of certain disclosures of personal data.[8] 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 (ADA), for example, states specifically that medical records must be filed separately from other records in an employee file.[9] 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."*[10]

The requirement to protect records and data containing personally identifiable information 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 prevent unauthorized access to PII by a person other than the subscriber or cable operator.[11] Most privacy laws set penalties for failure to protect personally identifiable information or for misuse or unlawful disclosure of PII.

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 to

[7] 20USC §1232g(b)(4)(A)
[8] 5USC §552a(c)(1)
[9] 42USC §12112(d)(3)(B)
[10] 5USC §552a(d)(1)
[11] 47USC §551(c)(1)

inspect records and to correct records about themselves. (A *data subject* is the person the collected data is about.) The Privacy Act of 1974, for example, requires an agency to allow a data subject to access their record or any information pertaining to them which is contained in the system, permit them to review the record, permit them to request amendment of their record, permit the data subject who disagrees with a refusal to amend their record to request a review of such refusal, and to clearly note any portion of the record which is disputed and, in any disclosure, provide copies of the dispute and the reason(s) for not making the requested amendments.[12] The Fair Credit Reporting Act requires consumer reporting agencies to disclose to a data subject all information in their file (with some exceptions) at the time of request, and the right of the data subject to dispute incorrect information and require it be corrected.[13]

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 redisclose 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.[14] Highly restricted personal information cannot be disclosed without the permission of the data subject.

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 (CFR). 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 personally identifiable information, or when to dispose of the records or data. For instance, the Stored Wire and Electronic Communications and Transactional Records Access (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.[15] The Driver's Privacy Protection Act requires any authorized recipient that resells or rediscloses motor vehicle information to keep, for a period of 5 years, records identifying recipients of the information and the permitted purpose for which the information will be used.[16]

Examples of disposal requirements include the Fair and Accurate Credit Transaction Act which requires the Federal banking agencies, the National Credit Union Administration, and the Federal Trade Commission to issue final regulations

[12] 5USC §552a(d)(1-4)
[13] 15USC §1681g(a)
[14] 18USC §2721(c)
[15] 18USC §2703(f)(2)
[16] 18USC §2721(c)

requiring the "proper disposal" of consumer information or any compilation of consumer information derived from consumer reports for a business purpose.[17] 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.[18]

Because information privacy is integral to records and information management, 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. The records manager should be aware of laws pertinent to their organization and the requirements of those laws, and the records manager should also be aware of 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.

Privacy laws reference or set definitions for several RIM terms, such as "record(s)," "system of records" or "record keeping system", and "record keeping." Several laws also similarly define "information" and "information system" when setting privacy protection requirements. 36CFR (National Archives and Records Administration (NARA) regulations) defines "records"[19] as including:

> *… "all books, papers, maps, photographs, machine readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations or other activities of the Government or because of the informational value of the data in them (44 U.S.C. 3301).*

36CFR also defines "recordkeeping requirements"[20] as *"all statements in statutes, regulations, and agency directives or authoritative issuances, that provide general and specific requirements for Federal agency personnel on particular records to be created and maintained by the agency,"* and defines "recordkeeping system"[21] as "*a manual or automated system in which records are collected, organized, and categorized to facilitate their preservation, retrieval, use, and disposition*."

[17] 15USC §1681w(a)(1)
[18] 47USC §551(e)
[19] 36CFR §1220.18
[20] *ibid*
[21] *ibid*

The Privacy Act of 1974 defines "record" as "*any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol or other identifying particular assigned to the individual, such as a finger or voice print or a photograph*." This law also defines "system of records" or "record keeping system" as "*any group of records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual*."[22] There are a number of other privacy laws that refer to or repeat these definitions.

U.S. Federal Laws

U.S. federal law is established in a three or four step process. After introduction in the House or Senate as a bill, Congress passes a public law, usually referred to as an "Act." A Public Law results in a new section or changes to existing sections of the U.S. Code. Some Public Laws change more than one section of the U.S. Code and the requirements of the Act are generally better understood if the Public Law is referenced rather than various sections of the Code. The USA Patriot Act, for example, changes numerous sections of the U.S. Code. Sometimes a Public Law will amend an existing Act with another Act, such as the Fair and Accurate Credit Transaction Act (FACTA) amending and becoming a part of the Fair Credit Reporting Act. Similarly, the Computer Matching and Privacy Protection Act amended and became a part of the Privacy Act of 1974.

Sometimes the Act instructs an agency or agencies to generate a rule or rules. These rules are drafted, go through a public review period, and are published as "final" rules in the Federal Register. The final rules are usually compiled in the Code of Federal Regulations (CFR) which contains the rules and regulations generated under the authority of a law. Some privacy regulations are established as directives from the Executive Branch, such as the Office of Management and Budget (known as OMB Circulars) or the President (known as Executive Orders). Both the Privacy Act of 1974 and the E-Government Act of 2002 have OMB Circulars regarding data or information privacy protection.

There are four primary legislative models of data privacy:[23]

- Comprehensive laws govern the collection, use, and dissemination of personal information in both the public and private sectors. These laws are usually

[22] 5USC §552a(a)(4)

[23] *Foundations of Information Privacy and Data Protection*, Peter P. Swire, CIPP/US and Kenesa Ahmad, CIPP/US, International Association of Privacy Professionals (IAPP), New Hampshire, 2012, pages 31-33

regulated under the authority of a government official or agency that has enforcement oversight. Enforcement and funding are two critical issues in this model as they differ in authority from country to country, and some countries are inadequately funded to meet the stated laws and rules. The European Union (EU) and some other countries use this model.

- Sectoral laws protect personal information that specifically addresses a particular industry sector (public or private) such as consumer financial transactions, credit records, and medical records. There is no central government oversight authority to enforce the laws. This model is followed by the U.S. and Japan.
- Co-regulatory model is a variant of the comprehensive law model. Industry develops enforcement standards for privacy and data protection which are then enforced by the industry with oversight by a government agency. Canada, New Zealand, and Australia follow this model.
- Self-regulatory model requires the private sector to abide by codes of practice as set by a company or groups of companies, industry bodies, and/or independent bodies to protect data. Generally, there is no central data protection law that creates a legal framework to follow. Japan, Singapore, and the U.S. use this model.

The U.S. takes a sectoral and self-regulatory approach to privacy legislation and protection. This approach causes some issues with international business, especially internet commerce. The European Union Data Protection Directive forbids the transfer of personal data to countries that lack "adequate" data protection, which they believe the US does not. To address this issue the US, in consultation with the European Commission, developed the Safe Harbor Data Privacy Accord, established by the U.S. Department of Commerce as authorized by Public Law 107-347.

In October 2015, the European Court of Justice (ECJ) deemed invalid the Safe Harbor agreement which has been in place since 2000. The court concluded that the agreement did not provide adequate protection for personal data. In addition, the Court confirmed that national data protection authorities have the authority to examine whether transfers of personal data to a third country meet the requirements of the EU data protection legislation.

The U.S.is currently in a grace period while negotiations with the EU continues to arrive at a compliant alternative to Safe Harbor. While this work continues, four other transfer options have been made available for other countries and the US to use to continue transfer of personal data.

Federal laws relating to the privacy of personally identifiable information cover a number of factors including how the data is collected, what data is collected,

sharing or disclosing data, how the data is used, and how well the data is protected. The laws apply to particular private or government sectors, and most of the laws include penalties for non-compliance. Some laws pertain only to government, some only to certain levels or sectors of government, and some only pertain to certain sectors of business such as finance, banking, medical, and telecommunications. Each organization must determine which laws apply to them. Many states have adopted laws similar to Federal laws for compliance by state and local government. These state laws are the subject of a Part II research paper.

Federal privacy laws cover one or more of the following elements:

- What can or cannot be collected
- How it can or cannot be used
- How and where it can be disseminated
- Rights of data subjects including the right to see what information has been collected and/or maintained about them, the right to correct incorrect information maintained about themselves, and/or the right to "opt out" of certain collection practices
- Penalties for noncompliance or if privacy is breached

These elements are set by the Privacy Act of 1974 and most privacy laws include some or all of these requirements. The Privacy Act of 1974 provides that data collected for one purpose cannot be used for other purposes without notifying the data subject in some manner.[24] However, the Privacy Act and many other federal privacy laws include exceptions to these requirements, and many include the caveat "*unless exempted by other law*." Most of the "exemptions" are established for law enforcement purposes, to protect national security, to prevent or respond to terrorist acts and so on. Many of the exceptions are found in the Electronic Communications Privacy Act, the Foreign Intelligence Surveillance Act and the USA Patriot Act.

Some privacy laws were developed after deliberate misuse of data. The Driver's Privacy Protection Act was enacted after it was found that many state Motor Vehicle Departments either disclosed or sold driver and car owner data to various sources such as insurance companies. The Fair Credit Reporting Act (FACR) was enacted to address the use and disclosure of an individual's credit report information, including the right of the individual to know what is in their credit report and to correct inaccuracies. The amendment to FACR, the Fair and Accurate Credit Transactions Act (FACTA), was enacted to include the right of a data subject to "opt out" of disclosure or sharing of personal data by creditors.

[24] 5USC §552a (a)(7) and 5USC §552a (b)

Several privacy laws were enacted as reaction to data breaches with severe consequences. For example, the Children's Online Privacy Protection Act (COPPA), was established to protect children from exploitive advertising and predators. The Act requires parental permission for children under 13 to take part in online activities that require the submission of personal information. The Veteran Affairs Information Security Enhancement Act was enacted after the loss of Veteran's Administration laptops and other electronic media containing patient personal and medical information.

At least 28 federal laws set privacy and data protection requirements. This paper discusses 32 federal personal information protection laws and their records management impact. Four of the laws covered were enacted for other purposes, but have noteworthy personal information privacy elements. The paper is not a definitive compilation of all Privacy law, but includes many high-profile privacy laws and regulations. It does not cover identity theft laws or data security laws unless the law included a significant privacy of personal information element.

The complete research report continues with summaries of 31 Federal laws and seven high profile regulations. A summary of the U.S./E.U. Safe Harbor Data Privacy Framework is also included. Each summary includes the year the Act was passed, the citation (either U.S. Code or Public Law), a summary of provisions, definitions of personally identifiable information and records related terms where applicable, and any implied or explicit RIM impact. The summary of provisions includes overviews of the major provisions of each law. Organizations must access the laws to understand all the provisions and requirements for each one.

In some cases, the laws include summaries of high profile rules established under the authority of that law. Where a law was enacted to amend another law, it is summarized under the law it amends. A ready reference table of the laws is also included in Appendix A.

Americans With Disabilities Act

The Americans with Disabilities Act is not a privacy law, but has a personal information privacy component.

Year Passed:

1990

Citation:

42 USC §§12101-12101, §§12111-12117

Applies to:

Employers of 15 or more employees for each working day during each of 20 or more calendar workweeks in the current or preceding calendar year. Does not include the United States (as an entity owned by the government), an Indian Tribe, or a private membership club (other than labor organizations) exempt from taxation under 501(c).

Scope and Purpose:

Prevents discrimination against employees and applicants who are disabled but can perform the essential duties of the job they hold or are seeking.

Summary of Provisions:

- Employers shall not discriminate against a qualified individual with a disability because of the disability of such individual in regard to job application procedures, the hiring, advancement, or discharge of employees, employee compensation, job training, and other terms, conditions, and privileges of employment.
- Employers may not conduct a medical examination or make inquiries of a job applicant as to whether they have a disability or as to the nature or severity of the disability.
- Employers may make pre-employment inquiries into the ability of an applicant to perform job-related functions.
- Employers may require a medical examination after an offer of employment has been made to a job applicant and prior to the commencement of the employment duties of such applicant, and may condition an offer of employment on the results of such examination. If the applicant is rejected based on the medical examination, the employer must show that the rejection is based on job-related results and consistent with business necessity. If the rejection is based on "safety reasons," the employer must show that the applicant poses a significant risk of substantial harm to

himself or others, and the risk cannot be mitigated through reasonable accommodation.

- Information obtained regarding the medical condition or history of the applicant is collected and maintained on separate forms and in separate medical files and is treated as a confidential medical record with limited access.
- Employers may not require a medical examination and shall not make inquiries of an existing employee as to whether such employee is an individual with a disability or as to the nature or severity of the disability, unless such examination or inquiry is shown to be job-related and consistent with business necessity.
- Employers may conduct voluntary medical examinations, including voluntary medical histories, which are part of an employee health program available to employees at that work site. Information obtained regarding the medical condition or history of the employee must be collected and maintained on separate forms and in separate medical files and treated as a confidential medical record with limited access.
- An employer may make inquiries into the ability of an employee to perform job-related functions.

Records Management Impact

Information obtained regarding the medical condition or history of an employee or an applicant for a job must be collected and maintained on separate forms and in separate medical files and treated as a confidential medical record.[25]

[25] 42USC §12112(d)(3)(B) & (4)(C)

Anti-cybersquatting Consumer Protection Act

(amends the Lanham Act (trademarks))

The Anti-cybersquatting Consumer Protection Act is not a privacy law, but has a personal information privacy component.

Year Passed:

1999

Citation:

15 USC §1125(d)

Applies to:

Anyone registering a domain name.

Scope and Purpose:

Prohibits bad-faith registration, trafficking, or use of domain names that incorporate a third party's trademark or the name of a living person.

Summary of Provisions:

- Imposes liability on whoever registers a domain name that consists of the name of a living person or a name substantially and confusingly similar to the name of a living person, without that person's consent.
- The court determining bad faith intent may consider the rights of the registrant, commonly used names, prior use, fair use, diversion of consumer, offers to sell, false contact information, multiple domain names, and distinctiveness of the domain name or trademark.
- Allows civil action, in the judicial district in which the domain name registrar, registry, or other authority is located, against a bad faith domain by any person who believes that he or she is likely to be damaged by such act.

Cable Communications Policy Act

Year Passed:
1984

Citation:
47 USC §551

Applies to:
Cable television operators.

Scope and Purpose:

Governs cable television subscriber information.

Summary of Provisions:

- Requires cable television operators to provide notice to their subscribers, at the time of service initiation and annually, of the personal data collected, the use and disclosure of that data, and subscriber rights under the Act.
- Prohibits cable television operators from collecting personally identifiable information (PII) about the subscriber over the cable system without their prior written consent, except as disclosed by the notice.
- Generally prohibits disclosure of the information without prior written or electronic consent of the subscriber concerned, except for lists of subscriber names and addresses that do not include subscriber viewing habits or transactions over the cable system, and except as required by court order or other law.
- Requires cable operators to take such actions as are necessary to prevent unauthorized access to PII by a person other than the subscriber or cable operator.
- Requires cable operators to allow subscribers access to their PII and the right to correct any errors.
- Requires the cable operator to destroy PII when no longer necessary for the purpose for which it was collected.
- May disclose PII to an authorized government entity, except the disclosure shall not include records revealing cable subscriber selection of video programming from a cable operator.

Definitions

The term "personally identifiable information" does not include any record of aggregate data which does not identify particular persons.

Records Management Impact

A cable operator shall destroy personally identifiable information if the information is no longer necessary for the purpose for which it was collected and there are no pending legal requests or orders for access to such information.[26]

[26] 47USC §551(e)

Children's Online Privacy Protection Act (COPPA)

Year Passed

1998

Citation:

15 USC §§6501-6506

Applies to:

Operators of web sites and online services that collect personal information online from children younger than age 13 (including operators of general user sites with actual knowledge they are collecting information from children under the age of 13 and persons that have an interest in the online collection of children's personal information).

Scope and Purpose:

Governs personal information collected online that can serve to identify an individual child. The primary intent is to place parents in control of what information is collected from their children online.

Congress established COPPA as a regulatory framework for the collection and use of personal information from and about children via the Internet with the following goals:[27]

- enhancing parental involvement in a child's online activities in order to protect the privacy of children in the online environment
- helping to protect the safety of children in online situations
- maintaining the security of children's personal information collected online
- limiting the collection of personal information from children without parental consent

Summary of Provisions:

- It is unlawful for an operator of a website or online service directed to children or any operator that has actual knowledge that it is a collection of personal information from a child, to collect personal information from a child in a manner that violates the regulations set by the Federal Trade Commission. A "child" is defined as "any person under the age of thirteen."
- Neither an operator of such a website or online service nor the operator's agent shall be held to be liable under any Federal or State law for any

[27] *Internet and Online Privacy, A Legal and Business Guide*, Andrew Frackmen, Esq., Rebecca C. Martin, Esq., and Claudia Ray, Esq, ALM Publishing, New York, 2002, page 46.

disclosure made in good faith and following reasonable procedures in responding to a request for disclosure of personal information to the parent of a child.

- The law directs the Federal Trade Commission to publish regulations to meet the requirements of the law, including allowing satisfaction of the requirements of the regulations by following self-regulatory guidelines issued by representatives of the marketing or online industries approved by the FTC.

Definitions

Defines "personal information" as individually identifiable information about an individual collected online including a first and last name, a home or other physical address including street name and name of city or town, an e-mail address, a telephone number, a Social Security number, any other identifier that permits the physical or online contacting of a specific individual, or information concerning the child or parents that the website collects online from the child and combines with another identifier under this definition (such as hobbies, interests, or information collected through cookies).[28]

Children's Online Privacy Protection Rule
16CFR Part 312
Effective 4/21/2000

- The rule requires operators of a commercial website or online service that collects personal information from children under the age of 13 to:
  - provide a clear and prominent notice on the website or online service of what information it collects from children, how it uses such information, and its disclosure practices for such information
  - obtain verifiable parental consent prior to any collection, use, and/or disclosure of personal information from children
  - provide a reasonable means for a parent to review the personal information collected form a child and to refuse to permit its further use or maintenance
  - not condition a child's participation in a gym, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity
  - establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children[29]

[28] 15 USC §6501(8)
[29] 16CFR Part 312.3

- These requirements must be met even if the operator only the uses the information internally and does not disclose it to third parties.
- All required notices must be clearly and understandably written, be complete, and must contain no unrelated, confusing, or contradictory materials.[30]
    - The link to the notice must be clearly labeled and placed in a prominent place and manner on the website or home page of the online service.
    - The notice must include all required information required by the regulation.
    - The operator must make reasonable efforts to ensure that a parent receives notice of a child's personal information collection, use, and/or disclosure practices including notice of any material changes to those practices since the parent's previous consent.
- The operator must receive verifiable parental consent before collection, use, and/or disclosure of a child's personal information.
- The operator must provide a parent the right to review the child's collected personal information and allow the parent the opportunity to refuse further use of or future online collection of their child's personal information.
- An operator is prohibited from making it a condition for a child to participate in an online activity, such as a game or the offering of a prize, on the child disclosing more personal information than is reasonably necessary to participate in such activity.
- The Rule includes allowing Federal Trade Commission approved safe harbors if the operator meets self-regulatory guidelines issued by approved marketing or online industries.
- The operator must establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.[31]

Records Management Impact

The requirements of the rule that the operator must provide a verifiable method of parental consent imply that the consent must be kept on file.

Operators who self-regulate under safe harbors must keep, for a period of not less than 3 years:[32]

Consumer complaints alleging violations of the guidelines

Records of disciplinary actions taken against the operators

[30] 16CFR Part 312.4
[31] 16CFR Part 312.8
[32] 16CFR Part 312.10(d)

Results of independent assessments of operator's compliance with the self-regulated guidelines

Computer Fraud and Abuse Act

Year Passed:
1986, Amended 1990

Citation:
18 USC §§1030 and 1037

Applies to:
Anyone accessing a computer to obtain information or to transmit email.

Scope and Purpose:

Governs unauthorized access to a protected computer to obtain information or to transmit electronic mail through another's computer.

Summary of Provisions:

- It is illegal to knowingly access a computer without authorization and obtain information determined by the U.S. Government to be protected for reasons of national defense or foreign relations, or obtain any restricted data, willfully communicate, deliver or disclose the information to any person not entitled to receive it, or willfully fail to deliver the information to any federal officer or employee entitled to receive it.
- It is illegal to intentionally access a computer without authorization, or to exceed authorized access to obtain financial records of a financial institution or card issuer to obtain a consumer's credit information, to obtain information from any U.S. government agency or department, or to obtain information from any protected computer involving interstate or foreign communication.
- It is illegal to knowingly and with intent to defraud, access a protected computer and obtain anything of value.
- It is illegal to knowingly transmit a program, information, code, or command that knowingly causes damage to a protected computer, or intentionally access a protected computer without authorization and cause damage.
- It is illegal to intentionally traffic in computer passwords with the intent to defraud where the trafficking affects interstate commerce, foreign relations, or computers that may be accessed by a U.S. government computer.
- It is illegal to extort something of value by sending a threat to damage a protected computer through interstate communications or foreign commerce.

- It is illegal to access a protected computer without authorization, and intentionally initiate the transmission of multiple commercial electronic mail messages from or through such computer
- It is illegal to use a protected computer to relay or retransmit multiple commercial electronic mail messages with the intent to deceive or mislead recipients or any Internet access service as to the origin of such messages
- It is illegal to materially falsify header information in multiple commercial electronic mail messages and intentionally initiate the transmission of such messages.
- It is illegal to register, using information that materially falsifies the identity of the actual registrant, for five or more electronic mail accounts or online user accounts or two or more domain names, and intentionally initiate the transmission of multiple commercial electronic mail messages from any combination of such accounts or domain names.
- It is illegal to falsely represent oneself to be the registrant or the legitimate successor in interest to the registrant of 5 or more Internet Protocol addresses, and intentionally initiate the transmission of multiple commercial electronic mail messages from such addresses.
- It provides for penalties and punishment for violation of the Act.

Definitions

The term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution.[33]

[33] 18USC §1030(e)(5)

Department of Veteran Affairs Information Security Enhancement Act

(part of Veterans Benefits, Health Care, and Information Technology Act of 2006)

Year Passed:

2006

Citation:

38 USC §§5722-5728

Applies to:

U.S. Department of Veteran Affairs

Scope and Purpose:

Governs the development and maintenance of cost-effective security controls needed to protect Veteran Affairs (VA) information, in any media or format, and VA information systems.

Summary of Provisions:

- Requires the establishment and maintenance of an agency-wide information security program (program), that provides development and maintenance of cost-effective security controls needed to protect VA information, in any media or format, and VA information systems.
- Outlines program elements and requirements, including compliance with information security requirements promulgated by the National Institute of Standards and Technology (NIST), and the Office of Management and Budget (OMB). Outlines program responsibilities of certain agency officials.
- Requires the program to ensure that information security protections are commensurate with the risk and potential harm from unauthorized access, use, disclosure, disruption, modification, or destruction; and includes a plan and milestones of actions being taken to correct any security compliance failure or policy violation.
- Requires the VA's Office of Inspector General or a non-VA entity to conduct an independent risk analysis of potential misuse of sensitive personal information (SPI) involved in any data breach with respect to SPI maintained by the VA. If a potential misuse is determined, requires the agency to provide to affected individuals, credit protection services, fraud alerts, and credit monitoring through credit reporting agencies, and requires immediate notification to veterans' committees in the event of a significant SPI data breach.
- Provides confidentiality requirements for VA contractors who perform any function that requires access to SPI.

- Authorizes a scholarship program to provide financial assistance to a person pursuing a doctoral degree in computer science or electrical or computer engineering; and who enters into an agreement to be employed by the VA in such field for a period of obligated service as determined by the VA. Also authorizes education debt reduction payments to a qualified individual who has completed such education and is a VA employee who serves in a position related to information security.

Definitions

The term "confidentiality" means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

The term "data breach" means the loss, theft, or other unauthorized access, other than those incidental to the scope of employment, to data containing sensitive personal information in electronic or printed form, that results in the potential compromise of the confidentiality or integrity of the data.

The term "information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, whether automated or manual.

The term "sensitive personal information", with respect to an individual, means any information about the individual maintained by an agency, including:

- Education, financial transactions, medical history, and criminal or employment history.
- Information that can be used to distinguish or trace the individual's identity including name, social security number, date and place of birth, mother's maiden name, or biometric records.

The term "VA sensitive data" means all Department data on any storage media or in any form or format which requires protection due to the risk of harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information, and includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, and records about individuals requiring protection under applicable confidentiality provisions.

Records Management Impact

Requires a report be provided to the veterans' committees after each SPI data breach.

Requires quarterly reports to the veterans' committees on any SPI data breaches.

Digital Millennium Copyright Act – Title II

Online Copyright Infringement Liability Limitation Act

The Digital Millennium Copyright Act is not a privacy law, but has a personal information privacy component.

Year Passed:

1998

Citation:

Public Law 105-304 §§201-203 (17USC §512)

Applies to:

Copyright owner or its agent and ISPs.

Scope and Purpose:

Title II governs notification to ISPs when subscribers are discovered sharing unauthorized materials and establishes limited liability for ISPs for online copyright infringement of subscribers.

Summary of Provisions:

- Establishes limited liability for online copyright infringement for entities offering the transmission, routing, or providing of connections for digital online communications between points specified by a user of material of the user's choosing, without modification of the material; and providers of online services or network access.
- Describes specific circumstances that provide for limited liability. Specifies conditions under which limitation on liability of nonprofit educational institutions shall apply.
- Describes the elements required for a notification of claimed infringement of copyright.
- Makes liable for damages persons who knowingly misrepresent that material or activity which is infringing on a copyright or that was removed or disabled by mistake or misidentification.
- Copyright owner may obtain and serve a subpoena on an ISP seeking identity of a customer alleged to be infringing on the owner's copyright.
- The court can grant injunctive relief restraining a service provider from providing access to infringing material or activity residing on the provider's system or network, and from granting access by terminating the accounts of a subscriber or account holder who is engaging in infringing activity as identified in the order.

- Copyright owner can send cease and desist notices to an ISP when subscribers are caught sharing unauthorized material.

Driver's Privacy Protection Act

Year Passed:
1994

Citation:
18 USC §§2721-2725

Applies to:
State departments of motor vehicles

Scope and Purpose:

Governs disclosure or availability of personal information obtained in connection with a motor vehicle record.

Summary of Provisions:

- Prohibits the disclosure of "personal information" except as provided within the Act.
- Prohibits the disclosure of "highly restricted personal information" without the express consent of the person to whom the information applies except for a government agency to carry out its functions, for legal proceedings, for insurance underwriting or investigations, and to verify information regarding the holder of a commercial driver's license by employers or insurers.
- Allows the resale or redisclosure of "personal information" for certain uses without permission of the data subject. Allows the resale or redisclosure of "personal information" for any purpose with permission of the data subject.
- Prohibits and makes unlawful for any person to knowingly obtain or disclose personal information from a motor vehicle record for any use not permitted by the Act, and for any person to make false representation to obtain personal information from an individual's motor vehicle record.
- Sets penalties for violation of the Act.

Definitions

The term "motor vehicle record" means any record that pertains to a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles.

The term "personal information" means information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not

include information on vehicular accidents, driving violations, and driver's status.

The term "highly restricted personal information" means an individual's photograph or image, social security number, medical or disability information.

The term "express consent" means consent in writing, including consent conveyed electronically that bears an electronic signature as defined in section 106(5) of Public Law 106–229.

Records Management Impact

Any authorized recipient that resells or rediscloses personal information covered by the Act must keep, for a period of 5 years, records identifying each recipient of the information and the permitted purpose for which the information will be used, and must make such records available to the Motor Vehicle Department upon request.[34]

Implies that "express consent," which must be in writing or conveyed electronically so that it bears an electronic signature, must be maintained to support the disclosure of highly restricted personal information.

[34] 18USC §2721(c)

E-Government Act of 2002

Year Passed:
2002

Citation:
Public Law 107-347

Applies to:
Federal agencies

Scope and Purpose:

To enhance the management and promotion of electronic Government services and processes by establishing a Federal Chief Information Officer within the Office of Management and Budget, and by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to Government information and services.

Summary of Provisions:

- Establishes the Office of Electronic Government in the Office of Management and Budget (OMB) as responsible for setting strategic direction for implementing electronic Government under relevant statutes, including the Privacy Act, the Government Paperwork Elimination Act, and the Federal Information Security Management Act of 2002.
- Defines "electronic Government" (E-Government) as the use by Government of web-based Internet applications and other information technologies, combined with processes that implement these technologies, to enhance the access to and delivery of Government information and services; or to bring about improvements in Government operations.
- Makes the head of each agency responsible for:
  - complying with the requirements of this Act, the related information resource management policies and guidance established by the Director of OMB, and the related IT standards promulgated by the Secretary of Commerce;
  - communicating such policies, guidance, and related IT standards to all relevant agency officials; and
  - supporting the efforts of the GSA to develop, maintain, and promote an integrated Internet-based system of delivering Government information and services to the public.

- Requires each court to make any document that is filed electronically publicly available online, with exceptions (such as sealed documents). Directs the Supreme Court to prescribe rules to protect privacy and security concerns relating to electronic filing of documents and their public availability, providing for uniform treatment of privacy and security issues throughout the Federal courts, taking into consideration best practices in Federal and State courts, and meeting requirements regarding the filing of an unredacted document under seal.
- Sets forth provisions regarding the issuance by Judicial Conference of the United States of interim and final rules on privacy and security. Directs the Judicial Conference to explore the feasibility of technology to post online dockets with links allowing all filings, decisions, and rulings in each case to be obtained from the docket sheet of that case.
- Requires the Committee to submit recommendations to the Director of OMB and the Archivist of the United States on, and directs the Archivist to require, the adoption by agencies of policies and procedures to ensure that specified Federal statutes are applied effectively and comprehensively to Government information on the Internet and to other electronic records.
- Requires the Director of OMB to promulgate guidance for agency websites that includes:
    - requirements that websites include direct links to descriptions of the mission and statutory authority of the agency, information made available under the Freedom of Information Act, information about the organizational structure of the agency, and the strategic plan of the agency
    - minimum agency goals to assist public users to navigate agency websites, including goals pertaining to the speed of retrieval of search results, the relevance of the results, tools to aggregate and dis-aggregate data, and security protocols to protect information.
- Requires each agency to conduct a privacy impact assessment, ensure the review of that assessment by the Chief Information Officer or equivalent official, and make such assessment publicly available, before:
    - developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form,
    - or initiating a new collection of information that will be collected, maintained, or disseminated using information technology.
- Requires the Director of OMB to issue guidance to agencies specifying the required contents of a privacy impact assessment.
- Requires the Director of OMB to develop guidance for privacy notices on agency websites used by the public.

- Sets forth provisions regarding modifying or waiving requirements of this section for security reasons, or to protect classified, sensitive, or private information.
- Requires the Director of OMB to oversee agency information security policies and practices through the Federal Information Security Management Act of 2002.
- Requires the Director of Office of Personnel Management (OPM) to:
  - analyze, on an ongoing basis, the personnel needs of the Government related to IT and information resource management,
  - identify where current IT and information resource management training do not satisfy such needs,
  - oversee the development of curricula, training methods, and training priorities that correspond to the projected needs, and
  - assess the training of Federal employees in IT disciplines to ensure that information resource management needs of the Government are addressed.

Records Management Impact:

Each agency shall conduct a privacy impact assessment before developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or initiating a new collection of information that will be collected, maintained, or disseminated using information technology.[35]

The E-Government Act amends the Paperwork Reduction Act by adding requirements for an inventory of major information systems that shall, among other requirements, be used to support information resources management including preparation of information system inventories required for records management under chapters 21, 29, 31, and 33 of the Paperwork Reduction Act.[36]

Confidential Information Protection and Statistical Efficiency Act
Title V of E-Government Act of 2002

Year Passed:
2002

Citation:
Public Law 107-347, §§501-526

[35] Public Law 107-347 §208(b)(1)(B)
[36] Public Law 107-347 §305(2)(c)(3)(C)(v)

Applies to:

Federal agencies

Scope and Purpose:

Governs confidential or personally identifiable information supplied to an agency for statistical purposes and authorizes the sharing of data for statistical purposes among certain federal agencies.

Summary of Provisions:

- Directs that data or information acquired by an agency under a pledge of confidentiality and for exclusively statistical purposes be used exclusively for statistical purposes.
- Bars the use of data or information acquired by an agency under a pledge of confidentiality for exclusively statistical purposes from being disclosed by an agency in identifiable form for use other than an exclusively statistical purpose, except with the respondent's informed consent.
- Requires a statistical agency or unit to clearly distinguish data or information it collects for non-statistical purposes (as authorized by law), and provide notice to the public, before it is collected, that it could be used for non-statistical purposes.
- Requires the head of each of the Designated Statistical Agencies (DSA) to:
  - identify opportunities to eliminate duplication and reduce reporting burden and cost in providing information for statistical purposes;
  - enter into joint statistical projects to improve the quality and reduce the cost of statistical programs; and
  - protect the confidentiality of individually identifiable information acquired for statistical purposes by adhering to safeguard principles.
- Requires:
  - business data provided by a DSA pursuant to this subtitle to be used exclusively for statistical purposes; and
  - publication of data acquired by a DSA in a manner whereby the data furnished by any particular respondent are not in identifiable form.

M03-22 OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002

September 2003 (updated by M-10-22 OMB in June 2010)

- Provides information to agencies on implementing the privacy provisions of the E-Government Act of 2002.

- Includes guidance to agencies specifying the required contents of a privacy impact assessment (PIA), how to conduct a PIA, when to conduct a PIA, and guidance for privacy notices on agency websites used by the public.
- Directs agencies to conduct reviews of how information about individuals is handled within their agency when they use IT to collect new information, or when agencies develop or buy new IT systems to handle collections of personally identifiable information.
- Directs agencies to describe how the government handles information that individuals provide electronically, so that the public has assurances that personal information is protected.
- Revision June 2010 establishes new procedures and provides updated guidance and requirements for agency use of web measurement and customization technologies with the central goal to respect and safeguard the privacy of the American public while also increasing the Federal Government's ability to serve the public by improving and modernizing its activities online.

Definitions

The term "information in identifiable form" means information in an IT system or online collection that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).

The term "Privacy Impact Assessment (PIA)" means an analysis of how information is handled to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Records Management Impact

Agencies may choose to conduct a PIA when developing the System of Records (SOR) notice required by the Privacy Act of 1974, in that the PIA and SOR overlap in content (e.g., the categories of records in the system, the uses of the records, the policies and practices for handling, etc.).[37]

[37] OMB M-03-22, Attachment A (II)(E)(1)

When agencies collect information subject to the Privacy Act of 1974, agencies are directed to explain what portion of the information is maintained and retrieved by name or personal identifier in a Privacy Act system of records and provide a Privacy Act Statement either at the point of collection, or via link to the agency's general Privacy Policy.[38]

Agencies are required to submit an annual report on compliance with this guidance to OMB as part of their annual E-Government Act status report.[39]

M05-04 OMB Policies for Federal Agency Public Websites
December 2004

Sets policies for the establishment and management of federal agency public websites.

Records Management Impact

Requires federal agencies to meet records management requirements by implementing OMB Privacy Act Guidance (OMB Circular A-130) and by implementing guidance form the National Archives and Records Administration.[40]

[38] OMB M-03-22, Attachment A (III)(D)(2)(a)(i)
[39] OMB M-03-22, Attachment A (VII)
[40] OMB M-05-04, Section 10

Electronic Communications Privacy Act

(amended Omnibus Crime Control & Safe Streets Act of 1968)

Passed in 1986, the Act consists of three titles

Title I - Wire And Electronic Communications Interception And Interception Of Oral Communications (Federal Wiretap Statute)

Year Passed

1968

Citation:

18 USC §§2510-2522

Applies to:

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.

Scope and Purpose:

Regulates the interception of wire, oral, and electronic communications to protect the privacy of innocent persons.

Summary of Provisions:

- Prohibits the intentional interception, use or disclosure of wire, oral and electronic communications unless a statutory exception applies. Wire communications include transfers of the human voice by means of a wire, cable or other connection between the sender and receiver. Electronic communications include electronic transfers of communications not carried by sound waves, such as e-mail, video conferences and other data transfers, and both wire and wireless transfers.
- Prohibits the manufacture, distribution, possession, and advertising of wire, oral, or electronic communication intercepting devices.
- Enables the confiscation of wire, oral, or electronic communication intercepting devices by the U.S. government.
- Prohibits the use as evidence of intercepted wire or oral communications if disclosure of the information is in violation of the Act.
- The Attorney General or those acting for the Attorney General, the principal prosecuting attorney of any State or political subdivision, and any attorney for U.S. Government may authorize or apply for a court order for interception of wire, oral, or electronic communications.

- Authorizes the disclosure and use of intercepted wire, oral, or electronic communications for law enforcement or investigative purposes necessary for the performance of their duties.
- Specifies the procedure for interception of wire, oral, or electronic communications.
- Specifies reports concerning intercepted wire, oral, or electronic communications.
- Specifies penalties and authorizes recovery of civil damages.

Records Management Impact:

Whenever an order authorizing interception is entered, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. Such reports shall be made at such intervals as the judge may require.[41]

The contents of any wire, oral, or electronic communication intercepted by any means authorized shall, if possible, be recorded on tape or wire or other comparable device, and immediately upon the expiration of the period of the order, or extensions thereof, such recordings shall be made available to the judge issuing such order and sealed under his directions. Custody of the recordings shall be wherever the judge orders. They shall not be destroyed except upon an order of the issuing or denying judge and in any event, shall be kept for ten years.[42]

Applications made and orders granted under this chapter shall be sealed by the judge. Custody of the applications and orders shall be wherever the judge directs. Such applications and orders shall be disclosed only upon a showing of good cause before a judge of competent jurisdiction and shall not be destroyed except on order of the issuing or denying judge, and in any event shall be kept for ten years.[43]

Title II - Stored Wire and Electronic Communications and Transactional Records Access

Year Passed
1986

Citation:
18 USC §§2701-2711

[41] 18USC §2518 (6)
[42] 18USC §2518 (8)(a)
[43] 18USC §2518 (8)(b)

Applies to:

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

Scope and Purpose:

Regulates the accessing of stored electronic communications

Summary of Provisions:

- Protects wire, oral and electronic communications while in transit and while in electronic storage (e-mail and voice mail).
- Prohibits the access to and disclosure of electronic communications and stored communications and customer records except as authorized by statute.
- Requires disclosure of customer communications or records in electronic storage under service of a warrant, court order, or an administrative subpoena without notifying the customer of such action.
- A court order or subpoena issued under this Act may require the service provider to create a backup copy of the content of the communications sought without notifying the subscriber or customer of the subpoena or court order.
- Imposes disclosure restrictions on ISPs and other online service providers (providers to the public of electronic communication service and providers of remote computing service) by prohibiting them from knowingly disclosing the contents of such stored communications, or the record or other information pertaining to a customer of such service, except as expressly permitted by statute. Government may obtain the records or other information about a customer without notice to the customer under certain court orders or warrants, upon receipt of formal written request relevant to investigation concerning telemarketing fraud, or by consent of the customer.
- Grants the Director of the Federal Bureau of Investigation (FBI) access to telephone or electronic communication service information and records relevant to any investigation to protect against international terrorism or clandestine intelligence activities. Prohibits the service provider from disclosing that the FBI has south or obtained such access.

Records Management Impact:

A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all

necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process, and shall retain such records for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity. [44]

A governmental entity may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought to preserve those communications. The service provider shall not destroy such backup copy until the later of the delivery of the information or the resolution of any proceedings (including appeals of any proceeding) concerning the government's subpoena or court order. [45]

Video Privacy Protection Act
[Amendment to the Stored Electronic Communication Privacy Act]

Year Passed:
1988

Citation:
18USC §2710

Applies to:
Video tape service providers

Scope and Purpose:

Governs the disclosure of customer personal information.

Summary of Provisions:

- Prohibits the disclosure of personally identifiable information concerning any customer of such provider.
- Provides certain exceptions for disclosure of personally identifiable information.

Definitions

The term "personally identifiable information" includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider.

Records Management Impact

[44] 18USC §2703(f)
[45] 18USC §2704(1) & (3)

A person subject to this section shall destroy personally identifiable information as soon as practicable, but no later than one year from the date 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 under the Act.[46]

Title III – Pen Register and Trap & Trace Devices

Year Passed

1988

Citation:

18USC §§3121-3127

Applies to:

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.

Scope and Purpose:

Governs use of pen registers and trap and trap devices.

Summary of Provisions:

- Prohibits the unauthorized use of a pen register or trap and trace device, except as permitted by statute. (A *pen register* captures outgoing address information such as a phone number or e-mail header) (A trap/trace device captures incoming address information such as caller ID information or e-mail header)
- Specifies procedures and circumstances for the application for and issuance of a court order for a pen register or a trap and trace device.
- Requires the assistance and cooperation of the provider of wire or electronic communication service in the installation and use of a pen register or a trap and trace device upon request of an attorney for the Government or an officer of a law enforcement agency.
- Provides for the emergency installation of a pen register or a trap and trace device.

Records Management Impact:

Where a law enforcement agency, through court order, installs and uses its own pen register or trap and trace device on a packet-switched data network

[46] 18USC §2710(e)

of a provider of electronic communication service to the public, the agency shall ensure that a record will be maintained which will identify any officer or officers who installed the device and any officer or officers who accessed the device to obtain information from the network; the date and time the device was installed, the date and time the device was uninstalled, and the date, time, and duration of each time the device is accessed to obtain information; the configuration of the device at the time of its installation and any subsequent modification thereof; and any information which has been collected by the device.[47]

The Attorney General shall annually report to Congress on the number of pen register orders and orders for trap and trace devices applied for by law enforcement agencies of the Department of Justice, which report shall include specified information.[48]

[47] 18USC §3123(3)(A)
[48] 18USC §3126

Employee Polygraph Protection Act

Year Passed:
1988

Citation:
29 USC §§2001-2009

Applies to:
Employers in the private sector.

Scope and Purpose:

Governs the administration of a lie-detector test either for pre-employment screening or during the course of employment.

Summary of Provisions:

- Prohibits the administration of a lie-detector test either for pre-employment screening or during the course of employment by employers in the private sector with certain exceptions. An employee or applicant may not be disciplined, discharged, or denied employment for refusing to take a lie detector test or for filing a complaint against an employer who administers one.
- Employers shall post copies of the notice of protection issued by the Department of Labor in a conspicuous place on its premises.
- Directs the Department of Labor to issue such rules and regulations as may be necessary to carry out the requirements of the Act.
- Provides for enforcement of the Act
- Specifies exemptions to the requirements of the Act – governmental employers, for purposes of national defense and security, FBI contractors, security services, drug security, drug theft, or drug diversion investigations, and ongoing investigations.

Records Management Impact

The Department of Labor shall make investigations and inspections, and require the keeping of records necessary or appropriate for the administration of this chapter.[49]

[49] 29USC §2004(a)(3)

Fair Credit Reporting Act (FCRA)

Year Passed:
1970

Citation:
15USC §§1681 *et seq.*

Applies to:
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 subsection (d) of section 1681m.

Scope and Purpose:

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. Requires that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information in accordance with the requirements of the Act.

Summary of Provisions:

- Details the information that consumer credit reports may contain and how and by whom a consumer's credit information can be used.
- Addresses the use and disclosure of an individual's credit report information.
- Generally prohibits the disclosure of consumer report information except as expressly authorized by the statute.
- Regulates the information contained in a consumer report as defined.
- Identifies permissible purposes of consumer reports and permits the disclosure of a consumer report in certain situations.
- Permits an entity to share consumer report information with its affiliates if the consumer does not opt out of such sharing.
- Defines consumer opt-out rights and describes opt out methods.
- Provides requirements that the user of the information must fulfill for certain uses such for employment purposes.
- Places certain responsibilities on the users of consumer reports when they take adverse action against a consumer based in whole or in part on

information contained in a report, including providing the consumer with a copy of the report and a description in writing of the consumer rights.

- Places time limitations on certain types of information in consumer reports.
- Defines consumer rights for access to the information contained in their credit report and for correcting inaccurate information.
- Consumer reporting agencies must have in place reasonable procedures to ensure compliance with the Act's requirements regarding information that must be included or excluded in a report, the identity and purpose of consumer report users, and measures to protect consumers as well as users of reports.
- Requires furnishers of consumer information to consumer reporting agencies to provide accurate information to reporting agencies.

Definitions

The term "file", when used in connection with information on any consumer, means all of the information on that consumer recorded and retained by a consumer reporting agency regardless of how the information is stored.

The term "medical information" means information or data, whether oral or recorded, in any form or medium, created by or derived from a health care provider or the consumer, that relates to the past, present, or future physical, mental, or behavioral health or condition of an individual; the provision of health care to an individual; or the payment for the provision of health care to an individual. It does not include the age or gender of a consumer, demographic information about the consumer including a consumer's residence address or e-mail address, or any other information about a consumer that does not relate to the physical, mental, or behavioral health or condition of a consumer, including the existence or value of any insurance policy.

Records Management Impact:

A consumer reporting agency shall not furnish for employment purposes, or in connection with a credit or insurance transaction, a consumer report that contains medical information about a consumer, unless it is furnished for purposes specified in the law.[50]

Implies retention of data and inclusion of information by excluding certain information from consumer reports based on age of the information with specified exceptions. No consumer reporting agency may make any consumer report containing any of the following items of information:

[50] 15USC §1681b(g)(1)

- Cases under Title 11 or under the Bankruptcy Act that, from the date of entry of the order for relief or the date of adjudication, as the case may be, antedate the report by more than 10 years.
- Civil suits, civil judgments, and records of arrest that, from date of entry, antedate the report by more than seven years or until the governing statute of limitations has expired, whichever is the longer period.
- Paid tax liens which, from date of payment, antedate the report by more than seven years.
- Accounts placed for collection or charged to profit and loss which antedate the report by more than seven years after the expiration of the required 180 day period beginning of the date of delinquency immediately preceding the collection activity or charge to profit and loss.
- Any other adverse item of information, other than records of convictions of crimes which antedates the report by more than seven years.
- The name, address, and telephone number of any medical information furnisher that has notified the agency of its status, with some exceptions.[51]

Implies retention of data and inclusion of information by requiring a fraud alert be placed in the file of a consumer reporting identity theft and:

- To provide that alert along with any credit score generated in using that file, during the 7-year period beginning on the date of such request, unless the consumer or such representative requests that such fraud alert be removed before the end of such period and the agency has received appropriate proof of the identity of the requester for such purpose;
- during the 5-year period beginning on the date of such request, exclude the consumer from any list of consumers prepared by the consumer reporting agency and provided to any third party to offer credit or insurance to the consumer as part of a transaction that was not initiated by the consumer, unless the consumer or such representative requests that such exclusion be rescinded before the end of such period.[52]

Implies retention of data and inclusion of information by requiring an active duty alert be placed in the file of a military consumer on active duty and:

- To provide that alert along with any credit score generated in using that file, during a period of not less than 12 months, or such longer period as the shall be determined by regulation, beginning on the date of the request, unless the active duty military consumer or such representative

[51] 15USC §1681c(a)
[52] 15USC §1681c-1(b)(1)

requests that such fraud alert be removed before the end of such period, and the agency has received appropriate proof of the identity of the requester for such purpose;

- during the 2-year period beginning on the date of such request, exclude the active duty military consumer from any list of consumers prepared by the consumer reporting agency and provided to any third party to offer credit or insurance to the consumer as part of a transaction that was not initiated by the consumer, unless the consumer requests that such exclusion be rescinded before the end of such period.[53]

Implies creation of records, which can be disclosed to the consumer upon request, showing:

- identification of each person (including each end-user identified in section 1681e of this title), with some exceptions, that procured a consumer report for employment purposes during the 2-year period preceding the date on which the request is made; or for any other purpose during the 1-year period preceding the date on which the request is made;
- the dates, original payees, and amounts of any checks upon which is based any adverse characterization of the consumer included in the file at the time of the disclosure.
- a record of all inquiries received by the agency during the 1-year period preceding the request that identified the consumer in connection with a credit or insurance transaction that was not initiated by the consumer. [54]

Requires a business entity that has provided credit to, provided for consideration products, goods, or services to, accepted payment from, or otherwise entered into a commercial transaction for consideration with, a person who has allegedly made unauthorized use of the means of identification of the victim, to provide a copy of application and business transaction records in the control of the business entity, evidencing any transaction alleged to be a result of identity theft to the victim upon written request; any law enforcement agency or officer specified by the victim in such a request; or any law enforcement agency investigating the identity theft and authorized by the victim to take receipt of records provided under this subsection.[55]

Nothing in subsection 1681g(e) creates an obligation on the part of a business entity to obtain, retain, or maintain information or records that are not

[53] 15USC §1681c-1(c)
[54] 15USC §1681g(a)(3) – (5)
[55] 15USC §1681g(e)(1)

otherwise required to be obtained, retained, or maintained in the ordinary course of its business or under other applicable law.[56]

Following any deletion of information which is found to be inaccurate or whose accuracy can no longer be verified or any notation as to disputed information, the consumer reporting agency shall, at the request of the consumer, furnish notification that the item has been deleted or that the information is in dispute to any person specifically designated by the consumer who has within two years prior thereto received a consumer report for employment purposes, or within six months prior thereto received a consumer report for any other purpose, which contained the deleted or disputed information.[57] [Implies retention of records maintained under 1681g(a)(3) – (5)]

Each consumer reporting agency that receives a complaint transmitted by the Federal Trade Commission pursuant to a file of a consumer maintained by that consumer reporting agency which contains incomplete or inaccurate information, with respect to which, the consumer appears to have disputed the completeness or accuracy and otherwise followed all required procedures, shall file regular reports to the Commission regarding determinations of and actions taken by the agency in connection with its review of such complaints. The reporting agency shall maintain, for a reasonable time period, records regarding the disposition of each such complaint that is sufficient to demonstrate compliance with this subsection.[58]

A person who makes an offer of credit or insurance to a consumer under a credit or insurance transaction not initiated by the consumer shall maintain on file the criteria used to select the consumer to receive the offer, all criteria bearing on credit worthiness or insurability, as applicable, that are the basis for determining whether or not to extend credit or insurance pursuant to the offer, and any requirement for the furnishing of collateral as a condition of the extension of credit or insurance until the expiration of the 3-year period beginning on the date on which the offer is made to the consumer.[59]

An action to enforce any liability created under this subchapter may be brought in any appropriate United States district court, without regard to the amount in controversy, or in any other court of competent jurisdiction, not later than the earlier of 2 years after the date of discovery by the plaintiff of the violation that is the basis for such liability; or 5 years after the date on which the violation that is the basis for such liability occurs.[60]

[56] 15USC §1681g(e)(8)
[57] 15USC §1681i(d)
[58] 15USC §1681i(e)(3)
[59] 15USC §1681m(d)(3)
[60] 15USC §1681p

Each consumer reporting agency shall submit an annual summary report to the Federal Trade Commission on consumer complaints received by the agency on identity theft or fraud alerts.[61]

The election of a consumer to prohibit the making of solicitations [opt out] shall be effective for at least 5 years, beginning on the date on which the person receives the election of the consumer, unless the consumer requests that such election be revoked. The consumer may extend the opt-out for another period of at least 5 years, pursuant to specified procedures.[62] [Implies retention of the information.]

Requires certain agencies to issue final regulations [12 CFR 717.83) requiring any person that maintains or otherwise possesses consumer information, or any compilation of consumer information, derived from consumer reports for a business purpose to properly dispose of any such information or compilation.[63]

Fair and Accurate Credit Transactions Act (FACTA)
(Amended the Fair Credit Report Act)

Year Passed:
2003

Citation:
Public Law 108-159
Amended 21 (of 29 total) sections of 15USC §1681 *et seq.*

Summary of Provisions:

- Amended FCRA regarding information contained in consumer reports, disclosure of consumer report information, disclosures to law enforcement.
- Changes the definition of consumer report to exclude communications relating to employee investigations under certain circumstances.
- Enhances the ability of consumers to combat identity theft, including a requirement for certain federal agencies to establish guidelines for Identity Theft Prevention Programs ("Red Flag Rules")[64].
- Increases the accuracy of credit reports.
- Restricts the use of medical information to credit eligibility determinations.

[61] 15USC §1681s(f)(3)
[62] 15USC §1681s-3(a)(3)
[63] 15USC §1681w(a)(1)
[64] 15USC §1681m(e)(1)

- Allows consumers to exercise greater control regarding the type and number of solicitations they receive (opt out), and extends the marketing opt out from 2 years to 5 years.
- Requires certain agencies to issue final regulations for the proper disposal of consumer information.
- Establishes the Financial Literacy and Education Improvement Commission.

Family & Medical Leave Act (FMLA)

The Family & Medical Leave Act is not a privacy law, but has a personal information privacy component.

Year Passed:

1993

Citation:

29 USC §§2601-2654

Applies to:

Employers of 50 or more employees for each working day during each of 20 or more calendar workweeks in the current or preceding calendar year.

Scope and Purpose:

Governs the process of requesting and granting unpaid leave for medical reasons.

Summary of Provisions:

- Provides a process for employees meeting eligibility criteria to take up to 12 weeks of leave for medical purposes.
- Limits the types of inquiries that may be made to establish FMLA eligibility.
- Establishes investigative authority and enforcement of provisions the Act.

Records Management Impact

Any employer shall make, keep, and preserve records pertaining to compliance with this subchapter in accordance with the law and in accordance with regulations issued by the Secretary of Labor.[65]

29CFR Part 825.500 sets the requirements for what records must be kept to comply with the FMLA and how they must be stored or maintained.

[65] 29USC §2616(b)

Family Educational Rights & Privacy Act (FERPA)

Year Passed:
1974

Citation:
20 USC §1232g

Applies to:
Applies to educational agencies or institutions.

Scope and Purpose:

Governs privacy of student's education records.

Summary of Provisions:

- Prohibits schools receiving public finds from disclosing personally identifiable information in a student's education records, other than directory information (as defined), without the consent of a student or the parent of a minor student.
- Sets some exceptions to disclosure prohibition.
- Transfers the rights of the parents to the student when the student turns 18, or when the student attends a postsecondary educational institution.
- Grants the student or the parents of a minor student the right to inspect and review their education records, are provided an opportunity to challenge the content of the records if inaccurate, misleading or otherwise in violation of the student's privacy, and are provided an opportunity for the correction or deletion of any such inaccurate, misleading or otherwise inappropriate data.

Definitions

The term "education records" means, with some exceptions, those records, files, documents, and other materials which contain information directly related to a student, and are maintained by an educational agency or institution or by a person acting for such agency or institution. The term "education records" does not include:

- records of instructional, supervisory, and administrative personnel which are in the sole possession of such personnel and which are not accessible or revealed to any other person except a substitute;
- records maintained by a law enforcement unit of the educational agency or institution that were created by that law enforcement unit for the purpose of law enforcement;

- in the case of persons who are employed by an educational agency or institution but who are not in attendance at such agency or institution, records made and maintained in the normal course of business which relate exclusively to such person in that person's capacity as an employee and are not available for use for any other purpose; or
- records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in his professional or paraprofessional capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student's choice.

Records Management Impact

Organizations conducting studies for, or on behalf of, educational agencies or institutions for the purpose of developing, validating, or administering predictive tests, administering student aid programs, and improving instruction, if such studies are conducted in such a manner as to not disclose the personal identification of students and their parents to persons other than representatives of such organizations, and if such information is destroyed when no longer needed for the purpose for which it is conducted.[66]

Each educational agency or institution shall maintain a record, kept with the education records of each student, indicating all individuals (other than those specified exceptions), agencies, or organizations which have requested or obtained access to a student's education records maintained by such educational agency or institution, and which will indicate specifically the legitimate interest that each such person, agency, or organization has in obtaining this information. Such record of access shall be available only to the student or the parents of a minor student, to the school official and his assistants who are responsible for the custody of such records, and to persons or organizations authorized to audit the operation of the system. Personal information shall only be transferred to a third party on the condition that such party will not permit any other party to have access to such information without the written consent of the student or the parents of a minor student. If a third party outside the educational agency or institution permits access to information or fails to destroy information in violation of this section, the educational agency or institution shall be prohibited from

[66] 20USC §1232g(b)(1)(F)

permitting access to information from education records to that third party for a period of not less than five years. [67]

[67] 20USC §1232g(b)(4)(A)

Financial Services Modernization Act (Gramm-Leach-Bliley Act)
Subchapter I—Disclosure Of Nonpublic Personal Information

Year Passed:
1999

Citation:
15USC §§6801-6809

Applies to:
Financial institutions

Scope and Purpose:

Enacted as a means of removing legal barriers preventing mergers between banks, insurance companies, brokerage firms and other financial entities. Has seven titles that mainly deal with modernizing the financial services industry. Title V provides additional protection to individuals' personal information that is collected, used, and disclosed by financial services entities. Title V also assesses criminal penalties against those who fraudulently attempt to gain access to individuals' financial information.

Summary of Provisions:

- Requires financial institutions, as defined, to respect the privacy of its customers and protect the security and confidentiality of customers' nonpublic personal information.
- Prohibits, with some exceptions, financial institutions to disclose directly or through an affiliate, nonpublic personal information to a nonaffiliated third party unless it provides a privacy policy and provides opt-out choices to the data subject.
- Prohibits a nonaffiliated third party that receives nonpublic personal information from a financial institution to disclose or share the information with any other nonaffiliated third party.
- When establishing a customer relationship with a consumer, requires a financial institution to provide a clear and conspicuous disclosure to the consumer, in a form permitted under the statute, the financial institution's policies and procedures with respect to disclosure of a consumer's nonpublic personal information and for protecting the information.
- Instructs federal agencies that enforce the Act to establish standards for financial institutions within their jurisdiction
    - to ensure that customer information is secure and confidential,

- to protect against threats to the security and integrity of customer information, and
- to protect against unauthorized access or use of such records that might result in substantial harm or inconvenience to the customer.

Definitions

The term "nonpublic personal information" means personally identifiable financial information provided by a consumer to a financial institution; resulting from any transaction with the consumer or any service performed for the consumer; or otherwise obtained by the financial institution. It does not include publicly available information, as such term is defined by the regulations prescribed under this title. Such term shall include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any nonpublic personal information other than publicly available information; but shall not include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any nonpublic personal information.

Records Management Impact

The disclosure required to be provided to a consumer shall include specified information regarding the policies and procedures of the financial institution.[68]

Privacy rules were promulgated by the Federal Trade Commission and those federal agencies that regulate traditional banking institutions. The banking regulators issued separate, but similar to the FTC rule, rules under the Joint Banking Privacy Rule (12 CFR, Parts 216, 332, 40, and 573 respectively.) The requirements of each of these rules are similar in scope, purpose, and provisions.

Privacy Of Consumer Financial Information
16 CFR Part 313
Federal Trade Commission

Governs the treatment of nonpublic personal information about consumers by the financial institutions defined in this section.

- Requires a financial institution in specified circumstances to provide notice to customers about its privacy policies and practices.
- Specifies the information required to be included in the privacy notice and the procedure for delivery and when it is to be issued.

[68] 15USC §6803(b)

- Describes the conditions under which a financial institution may disclose nonpublic personal information about consumers to nonaffiliated third parties.
- Provides a method for consumers to prevent a financial institution from disclosing that information to most nonaffiliated third parties by "opting out" of that disclosure, subject to certain exceptions.

The rule applies only to nonpublic personal information about individuals who obtain financial products or services primarily for personal, family, or household purposes from the defined financial institutions. It applies to those defined "financial institutions" and "other persons" over which the Federal Trade Commission has enforcement authority pursuant to the Gramm-Leach-Bliley Act.

Definitions:

The term "nonpublic personal information" means personally identifiable financial information; and any list, description, or other grouping of consumers (and publicly available information pertaining to them), that is derived using any personally identifiable financial information that is not publicly available. It does not include publicly available information, except as included on a list described in this section; or any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any personally identifiable financial information that is not publicly available.

The term "personally identifiable financial information" means any information provided by a consumer to obtain a financial product or service; about a consumer resulting from any transaction involving a financial product or service between the financial institution and a consumer; or otherwise obtained about a consumer in connection with providing a financial product or service to that consumer.

The term "publicly available information" means any information that a financial institution has a reasonable basis to believe is lawfully made available to the general public from Federal, State, or local government records; widely distributed media; or disclosures to the general public that are required to be made by Federal, State, or local law. A financial institution has a reasonable basis to believe that information is lawfully made available to the general public if it has taken steps to determine that the information is of the type that is available to the general public; and whether an individual can direct that the information not be made available to the general public and, if so, that the consumer has not done so.

Subchapter II-Fraudulent Access To Financial Information

Year Passed:

1999

Citation:

15USC §6821

Applies to:

Financial institutions and persons using personal information collected by financial institutions.

Scope and Purpose:

Enacted as a means of removing legal barriers preventing mergers between banks, insurance companies, brokerage firms and other financial entities. Has seven titles that mainly deal with modernizing the financial services industry. Title V provides additional protection to individuals' personal information that is collected, used and disclosed by financial services entities. Title V also assesses criminal penalties against those who fraudulently attempt to gain access to individuals' financial information.

Summary of Provisions:

- Prohibits any person to obtain customer information by false pretenses.
- Prohibits solicitation of a person to obtain customer information from financial institution under false pretenses.
- There are some provisions for no applicability to law enforcement, financial institutions, insurance institutions, and child support judgments.

Definitions

The term "nonpublic personal information" means personally identifiable financial information provided by a consumer to a financial institution; resulting from any transaction with the consumer or any service performed for the consumer; or otherwise obtained by the financial institution. It does not include publicly available information, as such term is defined by the regulations prescribed under this title. Such term shall include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any nonpublic personal information other than publicly available information; but shall not include any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived without using any nonpublic personal information.

Records Management Impact

Implies recordkeeping to monitor all requests to obtain customer information.

Foreign Intelligence Surveillance Act

Year Passed:
1978, Amended 2008

Citation:
50USC §§1801-1811

Applies to:
U.S. Government

Scope and Purpose:

Governs the government's authority to conduct electronic surveillance to acquire foreign intelligence information from a foreign power, agent of a foreign power, and, under certain circumstances, a United States person.

Summary of Provisions:

- Limits intelligence gathering to surveillance of a foreign power, and agent of a foreign power and a U.S. person.
- Authorizes, under certain circumstances, electronic surveillance without a court order.
- Permits the government to, pursuant to a court order, require the production of certain tangible things (including books, records, papers, documents) for an investigation to obtain foreign intelligence information not concerning a U.S. person or to protect against international terrorism or clandestine intelligence activities.
- Prohibits disclosure to anyone else that the FBI has sought or obtained tangible things under this Act.
- Establishes a special court to hear applications for and grant orders approving electronic surveillance.
- Allows for a private cause of action

Definitions:

The term "foreign intelligence information" means information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; sabotage or international terrorism by a foreign power or an agent of a foreign power; or clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or information with respect to a foreign power or foreign territory that relates to, and if concerning a

United States person is necessary to the national defense or the security of the United States; or the conduct of the foreign affairs of the United States.

Records Management Impact

The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution. [69]

[69] 50USC §1861(a)

Health Insurance Portability & Accountability Act (HIPAA)

Year Passed:

1996

Citation:

Public Law 104-191

Applies to:

Health plans, health care clearinghouses, and health care providers who transmit health information electronically.

Scope and Purpose:

Governs the disclosure of protected health information. To amend the Internal Revenue Code of 1986 to improve portability and continuity of health insurance coverage in the group and individual markets, to combat waste, fraud, and abuse in health insurance and health care delivery, to promote the use of medical savings accounts, to improve access to long-term care services and coverage, to simplify the administration of health insurance, and for other purposes.

Enacted in 1996 to standardize the electronic exchange of health information and to improve the privacy and security of health information.

Summary of Provisions:

- Amends the Employee Retirement Income Security Act of 1974 to add group health plan portability, access, and renewability requirements.
- Amends title XI of the Social Security Act to require the Secretary of Health and Human Services to establish a program to coordinate law enforcement programs to control health care fraud and abuse, to conduct investigations, audits, and inspections relating to the delivery of and payment for health care, to facilitate enforcement of certain provisions of title XI applicable to health care fraud and abuse, to provide for the modifications and establishment of safe harbors and to issue advisory opinions and special fraud alerts, and to provide for the reporting and disclosure of certain final adverse actions against health care providers, suppliers, or practitioners pursuant to the Act.
- Directs the HHS Secretary to establish a national health care fraud and abuse data collection program for reporting final adverse actions against health care providers, suppliers or practitioners and to maintain a database of such information.

- Directs the HHS Secretary to submit detailed recommendations on standards with respect to the privacy of individually identifiable health information
- Amends title XI of the Social Security Act by adding a new part for the development of an electronic system for processing health care information consistent with the goal of improving the operation of the overall health care system, and reducing related administrative costs through the adoption of certain standards for information transactions and data elements for such transactions as well as standards relating to security and performance of specified tasks.
- Amends the Internal Revenue Code to allow a deduction for limited amounts paid to a medical saving account.
- Amends the Internal Revenue Code by adding group health plan portability, access, and renewability requirements.
- Revises provisions prohibiting a deduction for interest on loans with respect to company-owned life insurance.
- Establishes penalties for the wrongful disclosure of individually identifiable health information.

Definitions:

The term "health information" means any information, whether oral or recorded in any form or medium, that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

The term "individually identifiable health information" means any information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and identifies the individual; or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

The term "standard", when used with reference to a data element of health information or a transaction referred to in section 1173(a)(1), means any such data element or transaction that meets each of the standards and implementation specifications adopted or established by the Secretary with

respect to the data element or transaction under sections 1172 through 1174 of this Act.

National Standards to Protect the Privacy of Personal Health Information
(HIPAA Privacy Rule)
45CFR Parts 160, 162, & 164
August, 2002

Establishes a set of national standards for the protection of certain health information. The Rule addresses the use and disclosure of individuals' health information by organizations subject to the HIPAA Privacy Rule, as well as requirements for individuals' privacy rights to understand and control how their health information is used.

The Rule is intended to give patients greater control over their health information, place limitations on the use and release of medical records, establish standards for safeguarding personal health information, and provide for the disclosure of health information when a covered entity has a public responsibility to do so.

- The Rule applies to health plans, health care clearinghouses, and to any health care provider who transmits health information in electronic form in connection with transactions covered by HIPAA Privacy or Security Rules.
- The Privacy Rule protects all individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral [*protected health information*].
- A covered entity may not use or disclose protected health information unless permitted or required by the Privacy Rule permits or requires; or if authorized in writing by the data subject.
- Limits, with some exceptions, the amount of protected health information that can be used or disclosed to the minimum amount necessary to accomplish the purpose of the use or disclosure. A covered entity must establish policies and procedures to reasonably limit uses and disclosures to the minimum necessary, including limited access and uses of the information based on the specific roles of their workforce.
- Patient written authorization is required for the use or disclosure of protected health information that is not for treatment, payment, or health care operations or otherwise permitted or required by the Rule. Patient consent is optional for the disclosure and use of protected information for routine health purposes.
- Covered entities can disclose protected information to its business associates as long as there is a written agreement that the associate will appropriately safeguard protected health information.

- Covered entities must provide patients with a written copy of their privacy practices and a notice of patient privacy rights and make a good faith effort to obtain a patient's written acknowledgement of the privacy notice.
- A limited data set may be used and disclosed for research, health care operations, and public health purposes, provided the recipient enters into a data use agreement promising specified safeguards for the protected health information within the limited data set.
- Gives patients the right to access their health information, with some exceptions, and gives patients the right to request amendments to correct information. Provides parents and legal guardians access rights to their child's protected health information.
- Individuals have a right to an accounting of the disclosures of their protected health information by a covered entity or the covered entity's business associates.
- Requires entities covered by the Rule to adopt written privacy procedures establishing who can access personal health information, how a covered entity may use such information, and when disclosure is permitted.
- A covered entity must mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of protected health information by its workforce or its business associates in violation of its privacy policies and procedures or the Privacy Rule.
- A covered entity must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information in violation of the Privacy Rule and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure. A covered entity must apply appropriate sanctions against members of its workforce who fail to comply.
- Covered entities must designate a privacy officer and must train their employees regarding their privacy procedures.
- A covered entity must establish policies and procedures for individuals to complain about its compliance with the Rule.

Definitions:

The term "limited data set" means protected health information from which certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed.

The term "electronic media" means electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or

disk, optical disk, or digital memory card; or transmission media used to exchange information already in electronic storage media.

The term "electronic protected health information" means protected health information in electronic format.

The term "health information" means any information, whether oral or recorded in any form or medium, that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

The term "individually identifiable health information" is information that is a subset of health information, including demographic information collected from an individual, and is created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual; or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

The term "protected health information" means individually identifiable health information that is transmitted by electronic media; maintained in electronic media; or transmitted or maintained in any other form or medium. The term does not mean individually identifiable health information in education records covered by the Family Educational Rights and Privacy Act, as amended, 20USC §1232g; records described at 20 USC §1232g(a)(4)(B)(iv); and employment records held by a covered entity in its role as employer.

Records Management Impact:

A covered entity must document:

- all complaints received, and their disposition, if any[70]
- any sanctions that are applied[71]
- that required training has been provided[72]

A covered entity must maintain, until six years after the later of the date of their creation or last effective date, its privacy policies and procedures, its privacy practices notices, disposition of complaints, and other actions,

[70] 45CFR §164.530(d)(2)
[71] 45CFR §164.530(e)(2)
[72] 45CFR §164.530(b)(2)(C)(ii)

activities, and designations that the Privacy Rule requires to be documented.[73]

Individuals have a right to an accounting of the disclosures of their protected health information by a covered entity or the covered entity's business associates. The maximum disclosure accounting period is the six years immediately preceding the accounting request. A covered entity is not obligated to account for any disclosure made before the Privacy Rule compliance date.[74]

Security Standards for the Protection of Electronic Protected Health Information
(HIPAA Security Rule)
45CFR Parts 160 & 164
August, 2002

Standardizes the way covered entities protect the confidentiality, integrity and availability of electronic protected health information. The Rule protects such information while held by a covered entity and also while it is in transit between covered entities and from covered entities to others.

The Rule requires covered entities to take the following measures:

- Ensure the confidentially, integrity and availability of all electronic protected health information that they create, receive, maintain or transmit.
- Protect against any reasonably anticipated threats to the security or integrity of such information.
- Protect against any reasonably anticipated uses or disclosures of such information that are not otherwise permitted or required by the rule.
- Ensure compliance by its workforce.
- Provide for administrative safeguards, physical safeguards, technical safeguards, and business associate contracts.

Electronic Transactions and Code Set Standards
(The Transaction and Codes Set Rule)
45CFR Part 162
August, 2002

Provides for standardization for Electronic Data Exchange (EDI) by covered entities. Applies to health plans, health care clearinghouses, and health care

[73] 45CFR §164.530(j)
[74] 45CFR 164.522(a)

providers who transmit electronic any health information in connection with a transaction covered by the Rule.

Transactions are activities involving the transfer of health care information for specific purposes. Under HIPAA, if a health care provider engages in one of the identified transactions, they must comply with the standard for that transaction. HIPAA requires every provider who does business electronically to use the same health care transactions, code sets, and identifiers. HIPAA has identified ten standard transactions for Electronic Data Interchange (EDI) for the transmission of health care data. Code sets are the codes used to identify specific diagnosis and clinical procedures on claims and encounter forms.

Privacy Act 1974

Year Passed:
1974, Amended 2004

Citation:
5 USC §552a

Applies to:
U.S. Federal Executive Branch

Scope and Purpose:

Governs third party access to personal information maintained by the federal government.

Establishes certain controls over what personal information is collected by the federal government and how it is used. This law guarantees three primary rights:

(1) the right to see records about oneself, subject to the Privacy Act's exemptions;

(2) the right to amend a nonexempt record if it is inaccurate, irrelevant, untimely, or incomplete; and

(3) the right to sue the government for violations of the statute.

Summary of Provisions:

- Prohibits the disclosure of records, with some exceptions, contained in a system of records that identify an individual and relate to such areas as education, financial transactions, medical history and criminal or employment history without written consent of the data subject.
- Requires agencies to make detailed accountings of their disclosures under the exceptions.
- Permits an individual to determine what records pertaining to him are collected, maintained, used, or disseminated by federal agencies.
- Permits an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent.
- Permits an individual to gain access to information pertaining to him in federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records.

- Collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information.
- Permits exemptions from requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority.
- Allows Executive Branch agencies to be subject to civil suit for any damages which occur as a result of willful or intentional action which violates any individual's rights under the Act.
- Prohibits the sale or rental out of an individual's name and address unless specifically authorized by law
- Provides for certain limitations on agency information practices, including requiring that information about an individual be collected from that individual to the greatest extent practicable; requiring agencies to ensure that their records are accurate, relevant, timely, and complete; and prohibiting agencies from maintaining information describing how an individual exercises his or her First Amendment rights unless the individual consents to it, a statute permits it, or it is within the scope of an authorized law enforcement investigation.
- Requires the establishment of rules of conduct for persons involved in the design, development, operations, or maintenance of any system of records, or in maintaining any record, and train such persons in any rules and requirements of this Act.
- Provides that a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, shall require such system to meet the requirements of the Act.

Definitions

The term "record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

The term "system of records" means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

The term "statistical record" means a record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by law.

The term "routine use" means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected.

Records Management Impact

Each agency, with respect to each system of records under its control, shall, except for disclosures made as required by the Act, keep an accurate accounting of the date, nature, and purpose of each disclosure of a record to any person or to another agency made under this section; and the name and address of the person or agency to whom the disclosure is made. Each agency shall retain the accounting for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made.[75]

Each agency that maintains a system of records shall maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President.[76]

Computer Matching and Privacy Protection Act
(Amends the Privacy Act of 1974)

Year Passed:
1988, Amended 1990

Citation:
5 USC §552a (a)(8-13), (e)(12), (o), (p), (q), (r), & (u)

Applies to:
U.S. Federal Executive Branch

Scope and Purpose:

Governs requirements federal agencies must follow when matching information on individuals with information held by other federal, state, or local agencies.

[75] 5USC §552a(c)
[76] 5USC §552a(e)(1)

Summary of Provisions:

- A federal agency can only match information in its records with that of another agency if it enters into a written agreement with the other agency. Such written computer matching agreements must include specified detailed information about the computer matching activities.
- Computer matching agreements also must provide a detailed account of how the information will be handled by the agencies and how individuals will be notified that their information may be verified through a matching program.
- Computer matching agreements only remain in effect for a maximum of 18 months, and can be renewed for an additional one-year if the program will be conducted without any change and each agency certifies that it has been in compliance with the agreement.
- Requires every federal agency conducting or participating in a matching program to establish a data integrity board, with specified duties, to oversee and coordinate the implementation of a computer matching program.
- Prohibits agencies from denying, terminating, or suspending financial assistance under a federal benefits program, or taking any other action that is averse to an individual without ensuring the integrity of the program's information.

OMB Guidelines and White House Directives
The Office of Management and Budget issued Guidelines for Privacy Act Implementation and the White House issued directives that require each federal agency to create privacy regulations meeting requirements of the Act.

Federal Agency Responsibilities for Maintaining Records About Individuals
Appendix I to OMB Circular No. A-130
1996

Describes agency responsibilities for implementing the reporting and publication requirements of the Privacy Act of 1974, as amended. It applies to all agencies subject to the Act. This Appendix does not rescind other guidance OMB has issued to help agencies interpret the Privacy Act's provisions.

- Specifies specific reporting and publication requirements relating to the provisions of the Act.
- Requires the head of each agency to ensure that the following reviews are conducted as often as specified, and to be prepared to report to the

Director of OMB, the results of such reviews and the corrective action taken to resolve problems uncovered.

- Review every two years a random sample of agency contracts that provide for the maintenance of a system of records on behalf of the agency to accomplish an agency function, in order to ensure that the wording of each contract makes the provisions of the Act binding on the contractor and his or her employees.
- Review biennially agency recordkeeping and disposal policies and practices in order to assure compliance with the Act, paying particular attention to the maintenance of automated records.
- Review every four years the routine use disclosures associated with each system of records in order to ensure that the recipient's use of such records continues to be compatible with the purpose for which the disclosing agency collected the information.
- Review every four years each system of records for which the agency has promulgated exemption rules pursuant to the Act in order to determine whether such exemption is still needed.
- Review annually each ongoing matching program in which the agency has participated during the year in order to ensure that the requirements of the Act, the OMB guidance, and any agency regulations, operating instructions, or guidelines have been met.
- Review biennially agency training practices in order to ensure that all agency personnel are familiar with the requirements of the Act, with the agency's implementing regulation, and with any special requirements of their specific jobs.
- Review biennially the actions of agency personnel that have resulted either in the agency being found civilly liable under the Act, or an employee being found criminally liable under the provisions of the Act, in order to determine the extent of the problem, and to find the most effective way to prevent recurrence of the problem.
- Review biennially each system of records notice to ensure that it accurately describes the system of records. Where minor changes are needed, e.g., the name of the system manager, ensure that an amended notice is published in the Federal Register. Agencies may choose to make one annual comprehensive publication consolidating such minor changes. This requirement is distinguished from and in addition to the requirement to report to OMB and Congress significant changes to systems of records and to publish those changes in the Federal Register.

Privacy Protection Act

Year Passed:
1980

Citation:
42 USC §2000aa

Applies to:
Government officer or employee

Scope and Purpose:

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.

Summary of Provisions:

- Prohibits a government officer or employee, with some exceptions, in connection with the investigation or prosecution of a criminal offense, from searching for or seizing, any work product or documentary (other than work product) materials possessed by a person reasonably believed to have a purpose to disseminate to the public a newspaper, book, broadcast, or other similar form of public communication.
- The Attorney General shall issue guidelines for procedures to obtain documentary materials in the private possession of a person when the person is not reasonably believed to be a suspect in such offense, and when the materials sought are not contraband. The guidelines shall incorporate, amongst other requirements, a recognition of the personal privacy interests of the person in possession of such documentary materials.

Right to Financial Privacy Act

Year Passed:
1978

Citation:
12 USC §§3401-3422

Applies to:
Any agency or department of the U.S. Government

Scope and Purpose:
Governs access to financial records of any customer of a financial institution

Summary of Provisions:

- Prohibits any U.S. agency or department from access to the financial records of any customer of a financial institution unless the release or records is authorized by the customer or the release of the records is pursuant to certain specified requirements, primarily court order or law enforcement purposes. The records may be obtained pursuant to an administrative subpoena or summons under certain conditions.
- Allows access for counterintelligence and protective functions.
- Prohibits release of any records until receipt of a written certification from the government that it has complied with provisions the Act.
- Provides for a court order to delay notification to the customer that records have been obtained or that a request for records has been made.
- Requires the financial institution to keep a record of all instances in which a customer's record is disclosed to a government authority pursuant to the Act, including the identity of the authority to which such disclosure is made. The customer has the right, unless prohibited by court order, to obtain a copy of such record.
- Customers have the right to challenge, in court, the dissemination of their records under a subpoena or summons.

Definitions

The term "financial record" means an original of, a copy of, or information known to have been derived from, any record held by a financial institution pertaining to a customer's relationship with the financial institution.

Records Management Impact

The customer has the right, unless the Government authority obtains a court order as provided in this title, to obtain a copy of the record which the financial institution shall keep of all instances in which the customer's record is disclosed to a Government authority pursuant to this section, including the identity of the Government authority to which such disclosure is made.[77]

Any memorandum, affidavit, or other paper filed in connection with a request for delay in notification shall be preserved by the court. Upon petition by the customer to whom such records pertain, the court may order disclosure of such papers to the petitioner unless the court makes the findings required in this section.[78]

Telecommunications Privacy Act

Year Passed:
1934, Amendments through 1999

Citation:
47 USC §222

Applies to:
Telecommunications carriers

Scope and Purpose:
Governs protection of proprietary information of customers, other telecommunication carriers, and equipment manufacturers.

Summary of Provisions:

- Telecommunications carriers must protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier.
- A telecommunications carrier that receives or obtains proprietary information from another carrier for purposes of providing any telecommunications service shall use such information only for such purpose, and shall not use such information for its own marketing efforts.
- Prohibits the use, disclosure, or access permission to individually identifiable customer proprietary network information, with some

[77] 12USC §3404(c)
[78] 12USC §3409(d)

exceptions, when providing the telecommunications service from which such information is derived, or when providing services necessary to, or used in, such telecommunications service, including the publishing of directories, unless required by law or with the approval of the customer.

- Allows the disclosure of customer proprietary network information, upon affirmative written request by the customer, to any person designated by the customer.
- Allows the use, disclosure, or access permission to aggregate customer information other than for the purposes described in this section. A local exchange carrier may use, disclose, or permit access to aggregate customer information other than for purposes described in this section only if it provides such aggregate information to other carriers or persons on reasonable and nondiscriminatory terms and conditions.
- Sets restrictions on the use of wireless location information.
- Sets restrictions on the use or disclosure of subscriber lists, and subscriber listed and unlisted information.

Definitions:

The term "customer proprietary network information" means information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier.

The term "aggregate customer information" means collective data that relates to a group or category of services or customers, from which individual customer identities and characteristics have been removed.

The term "subscriber list information" means any information identifying the listed names of subscribers of a carrier and such subscribers' telephone numbers, addresses, or primary advertising classifications (as such classifications are assigned at the time of the establishment of such service), or any combination of such listed names, numbers, addresses, or classifications; and that the carrier or an affiliate has published, caused to be published, or accepted for publication in any directory format.

Telephone Consumer Protection Act

Year Passed:
1991

Citation:
47 USC §227

Applies to:
Persons making commercial solicitations or telemarketers

Scope and Purpose:
Governs unsolicited telephone calls (do not call registry)

Summary of Provisions:

- Allows the Federal Communications Commission (FCC) to regulate unwanted commercial solicitation or telemarketing calls to residential telephones.
- Prohibits calls made with any automatic telephone dialing system or an artificial or prerecorded voice to any telephone number assigned to a paging service, cellular telephone service, specialized mobile radio service, or other radio common carrier service, or any service for which the called party is charged for the call.
- Prohibits, with some exceptions, calls made with any automatic telephone dialing system or an artificial or prerecorded voice to deliver a message to any residential telephone line without prior express consent of the called party.
- Prohibits, with some exceptions, the use of any telephone facsimile machine, computer, or other device to send, to a telephone facsimile machine, an unsolicited advertisement.
- Prohibits the use of an automatic telephone dialing system in such a way that two or more telephone lines of a multi-line business are engaged simultaneously.
- The FCC is directed to make regulations to implement the requirements of the Act, including protection of residential telephone subscriber's privacy rights to avoid receiving telephone solicitations avoid receiving telephone solicitations to which they object.
- The regulations may require the establishment and operation of a single national database to compile a list of telephone numbers of residential subscribers who object to receiving telephone solicitations, and to make that compiled list and parts thereof available for purchase.

- Provide for any person to bring civil rights of action for violations of the Act.
- Establishes technical and procedural standards regarding the uses of telephone facsimile machines, automatic telephone dialing systems, and computers or other electronic devises to send messages through telephone facsimile machines, initiate any communications in compliance with the Act.

Telephone Records and Privacy Protection Act

Year Passed:
2006

Citation:
18 USC §1039

Applies to:
Anyone obtaining (or selling) Customer Proprietary Network Information from a telephone company, including Voice over Internet Protocol service providers.

Scope and Purpose:

Governs access to Customer Proprietary Network Information, including Voice over Internet Protocol.

Summary of Provisions:

- Makes it unlawful to obtain, or attempt to obtain, confidential phone records information of a covered entity, by:
  - making false or fraudulent statements or representations to an employee of a covered entity
  - making such false or fraudulent statements or representations to a customer of a covered entity
  - providing a document to a covered entity knowing that such document is false or fraudulent
  - accessing customer accounts of a covered entity via the Internet, or by means of conduct that violates section this title, without prior authorization from the customer to whom such confidential phone records information relates
- Prohibits, with some exceptions, the sale or transfer of confidential phone records information without the authorization of the customer.
- Prohibits, with some exceptions, the purchase or receipt of confidential phone records information without the authorization of the customer.
- Sets penalties for violation of the Act.

Definitions

The term "confidential phone records information" means information that relates to the quantity, technical configuration, type, destination, location, or amount of use of a service offered by a covered entity, subscribed to by any customer of that

covered entity, and kept by or on behalf of that covered entity solely by virtue of the relationship between that covered entity and the customer; is made available to a covered entity by a customer solely by virtue of the relationship between that covered entity and the customer; or is contained in any bill, itemization, or account statement provided to a customer by or on behalf of a covered entity solely by virtue of the relationship between that covered entity and the customer.

Uniting & Strengthening America by Providing Appropriate Tools Required to Intercept & Obstruct Terrorism Act (a.k.a. USA Patriot Act)

Year Passed:

2001, Amended 2006

Citation:

Public Law 107-56 passed in 2001, amended with Public Law 109-177 (USA Patriot Improvement and Reauthorization Act) passed in 2005 and Public Law 109-178 (Additional Reauthorizing Amendments Act) passed in 2006.

Applies to:

Law enforcement and businesses that provide financial and communications services.

Scope and Purpose:

Governs the deterrent and punishment of terrorist acts in the United States and around the world and enhances law enforcement investigatory tools.

Summary of Provisions:

Consists of a number of amendments to existing laws to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes. It includes provisions for:

- enhancing domestic security against terrorism,
- enhanced surveillance procedures,
- international money laundering abatement and antiterrorist financing,
- immigration and border protection,
- removing obstacles to investigating terrorism,
- providing for victims of terrorism, public safety officers, and their families,
- increased information sharing for critical infrastructure protection,
- strengthening the criminal laws against terrorism,
- improved intelligence action.

The various amendments have been incorporated into the appropriate statutes. The 2006 amendment to the Act made permanent 14 of 16 provisions originally slated to expire in 2005. The remaining two provisions amend the Foreign Intelligence Surveillance Act and are slated to expire in 2009 unless extended.

The Act amends the following privacy laws:

Cable Communications Policy Act[79]

[79] 47 USC §551

Computer Fraud and Abuse Act[80]
Electronic Communications Privacy Act[81]
Wire And Electronic Communications Interception And Interception Of Oral Communications (*Federal Wiretap Statute*)[82]
Pen Register and Trap & Trace Device Statute (*Pen/Trap Statute*)[83]
Fair Credit Reporting Act (*FCRA*)[84]
Family Educational Rights & Privacy Act (*FERPA*)[85]
Foreign Intelligence Surveillance Act (*FISA*)[86]
Right to Financial Privacy Act[87]

Security and surveillance amendments are intended to give law enforcement greater authority to track, intercept and monitor telephonic, electronic (including e-mail and voice-mail), internet and cellular communications for both criminal investigations and for foreign surveillance. The Act also grants law enforcement access to certain financial and educational records for terrorist combating purposes. In certain contexts, businesses disclosing information under government order are granted immunity from third party liability.

Financial and communication services businesses are required, under a government order, to disclose data to law enforcement officials to assist in their investigations. The law also grants permission to financial institutions, after notice to the U.S. Treasury Department, to share information with each other to identify and report activities that may involve money laundering or terrorist activity to the federal government. It amends the Right to Financial Privacy Act by permitting the transfer of financial records to other agencies or departments if certification is received that the records are relevant to intelligence/counterintelligence activities relating to international terrorism.

Internet service providers have expanded obligations and immunities under the USA Patriot Act, mostly concerning law enforcement interaction and the way that ISPs assist with investigations by providing information. These impacts include:

- Permits an ISP to disclose customer records to a law enforcement agency without notifying the customer it will or has done so if the provider reasonably believes that immediate danger of death or serious body injury to any person requires disclosure or if the FBI has issued a national security letter (NSL) authorizing the obtaining of subscriber information

[80] 18 USC §§1030-1038
[81] 18 USC §§2701-2711, §3121-3127, §1367
[82] 18 USC §§2510-2522 45USC §605
[83] 18 USC §§3121-3127
[84] 15 USC §§1681 *et seq.*
[85] 20 USC §1232g
[86] 50 USC §§1801-1811
[87] 12 USC §§3401-3422

from an ISP – including name, address, length of service, and local and long-distance tolling bill records.

- Expands the government's authority to intercept, under certain conditions, a computer trespasser's wire or electronic communication transmitted to or through a protected computer.
- Allows government agencies to obtain, with an administrative subpoena, subscriber information such as name, address, phone number, service information, subscriber number, and source of payment (including credit card or bank account number).
- Amends and limits the Cable Communications Policy Act to make clear that businesses offering cable-based Internet service are subject to the requirements of the Cable Act to notify subscribers of government surveillance requests only when detailed cable-viewing information is being sought. Other government surveillance requests are subject to the Cable Act requirements.

Title IV of the Act, allows the FBI to request telephone toll and transactional records, financial records, and consumer reports in any investigation to protect against international terrorism or clandestine intelligence activities, provided the investigation is not conducted solely on the basis of activities protected by the first amendment to the Constitution.[88] Title IV also amends FISA to authorize consultation among federal law enforcement officers, in terrorism or related investigations or protective measures, regarding shared information acquired from an electronic surveillance or physical search. In addition, it amends FERPA to provide for disclosure of educational records to the Attorney General in a terrorism investigation or prosecution.

[88] Public Law 107-56, Section 505.

Appendix A
U.S. Federal Privacy Legislation Overview

Name	Year Passed	Citation	Applies to	Scope	Rules/Guidelines
Cable Communications Policy Act	1984	47 USC §551	Cable television operators	Governs cable television subscriber information	
Children's Online Privacy Protection Act	1998	15 USC §§6501-6506	Entities that collect personal information online (including Web sites or online services and persons who have an interest in the online collection of children's personal information)	Governs personal information collected online that can serve to identify an individual child.	*Children's Online Privacy Protection Rule, 16CFR Part 312*
Computer Fraud and Abuse Act	1986, Amended 1990	18 USC §§1030-1038	Anyone accessing a computer to obtain information	Governs unauthorized access to a protected computer to obtain information	
Department of Veteran Affairs Information Security Enhancement Act [***part of Veterans Benefits, Health Care, and Information Technology Act of 2006***]	2006	Public Law 109-461, §§901-902	Dept of Veteran Affairs	Governs the development and maintenance of cost-effective security controls needed to protect VA information, in any media or format, and VA information systems.	
Driver's Privacy Protection Act	1994	18 USC §§2721-2725	State departments of motor vehicles	Governs disclosure or availability of personal information obtained in connection with a motor vehicle record	

Name	Year Passed	Citation	Applies to	Scope	Rules/Guidelines
E-Government Act of 2002	2002	Public Law 107-347	Federal agencies	Establishes a Federal Chief Information Officer within the Office of Management and Budget, and establishes measures that require using internet-based information technology to enhance citizen access to Federal Government information and services.	*OMB M03-22 Guidance for Implementing the Privacy Provisions of the E-Government Act September 2003*
Confidential Information Protection and Statistical Efficiency Act	2002	Public Law 107-347, §§501-526	Federal agencies	Governs confidential or personally identifiable information supplied to an agency for statistical purposes and authorizes the sharing of data for statistical purposes among certain federal agencies.	
Employee Polygraph Protection Act	1988	29 USC §§2001-2009	Employers in the private sector	Governs the administration of a lie-detector test either for pre-employment screening or during the course of employment	

Name	Year Passed	Citation	Applies to	Scope	Rules/Guidelines
Electronic Communications Privacy Act (amended Omnibus Crime Control & Safe Streets Act of 1968)	1986	18 USC §§2701-2711, §3121-3127, §1367			
Title I **Wire And Electronic Communications Interception And Interception Of Oral Communications (*Federal Wiretap Statute*)**	1968	18 USC §§2510-2522 45USC §605	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	Regulates the interception of wire, oral, and electronic communications to protect the privacy of innocent persons	
Title II **Stored Electronic Communications Privacy Act**	1986	18 USC §§2701-2712	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	Regulates the accessing of stored electronic communications	
Video Privacy Protection Act [*Amendment to the Stored Electronic Communication Privacy Act*]	1988	18 USC §2710	Video tape service providers	Governs the disclosure of personal information of its customers	
Title III **Pen Register and Trap & Trace Device Statute (*Pen/Trap Statute*)**	1988	18 USC §§3121-3127	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	Governs use of pen registers and trap and trap devices	

Name	Year Passed	Citation	Applies to	Scope	Rules/Guidelines
Fair Credit Reporting Act	1970	15 USC §§1681 *et seq.*	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 subsection (d) of section 1681m	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	
Fair and Accurate Credit Transactions Act (FACTA) **[*Amends the Fair Credit Reporting Act*]**	2003	Public Law 108-159 Amended 21 (of 29 total) sections of 15USC §1681 *et seq.*	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	Governs opt-out notices, use of credit report information by employers in making employment decisions, and disposal of consumer credit information.	

Name	Year Passed	Citation	Applies to	Scope	Rules/Guidelines
Family Educational Rights & Privacy Act (FERPA)	1974	20 USC §1232g	Applies to educational agencies or institutions.	Governs privacy of student's education records	
Financial Services Modernization Act (aka Gramm-Leach-Bliley Act)	1999	15 USC §§6801-6809	Financial institutions	Governs the privacy and security of personal financial information	*Privacy Of Consumer Financial Information, 16 CFR Part 313*
Foreign Intelligence Surveillance Act	1978 Amended 2008	50 USC §§1801-1811	U.S.Government	Governs the government's authority to conduct electronic surveillance to acquire foreign intelligence information from a foreign power, agent of a foreign power, and, under certain circumstances, a United States person.	
Health Insurance Portability & Accountability Act (HIPAA)	1996	Public Law 104-191	Health plans, health care clearinghouses, and health care providers	Governs the disclosure of protected health information.	*National Standards to Protect the Privacy of Personal Health Information, 45CFR Parts 160, 162, & 164* *Security Standards for the Protection of Electronic Protected Health Information, 45CFR Parts 160 & 164* *Electronic Transactions and Code Set Standards, 45CFR Part 162*

Name	Year Passed	Citation	Applies to	Scope	Rules/Guidelines
Privacy Act of 1974	1974 2004 Amendment (Public Law108-447, div H, Title V, §522)	5 USC §552a	U.S. Federal Executive Branch	Governs third party access to personal information maintained by the federal government	*Federal Agency Responsibilities for Maintaining Records About Individuals, Appendix I to OMB Circular No. A-130 Revised 1996*
Computer Matching & Privacy Protection Act [*Amends the Privacy Act of 1974*]	1988, Amendments of 1990	5 USC §552a (a)(8-13), (e)(12), (o), (p), (q), (r), & (u)	U.S. Federal Executive Branch	Governs requirements federal agencies must follow when matching information on individuals with information held by other federal, state, or local agencies.	
Privacy Protection Act	1980	42 USC §2000aa	Government officer or employee	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.	
Right to Financial Privacy Act	1978	12 USC §§3401-3422	Any agency or department of the U.S. Government	Governs access to financial records of any customer of a financial institution	
Telecommunications Privacy Act	1934, Amendments through 1999	47 USC §222	Telecommunications carriers	Governs protection of proprietary information of customers, other telecommunication carriers, and equipment manufacturers.	

Name	Year Passed	Citation	Applies to	Scope	Rules/Guidelines
Telephone Records and Privacy Protection Act	2006	18 USC §1039	Anyone obtaining (or selling) Customer Proprietary Network Information from a telephone company, including Voice over Internet Protocol service providers	Governs access to Customer Proprietary Network Information, including Voice over Internet Protocol	
Telephone Consumer Protection Act	1991	47 USC §227	Persons making commercial solicitations or telemarketers	Governs unsolicited telephone calls (do not call registry)	
Uniting & Strengthening America by Providing Appropriate Tools Required to Intercept & Obstruct Terrorism Act (a.k.a. USA Patriot Act) [*Amends a number of statutes*]	2001, Amended 2006	Public Law 107-56, Public Law 109-177	Law enforcement, businesses that provide financial and communications services	Governs the deterrent and punishment of terrorist acts in the United States and around the world and enhances law enforcement investigatory tools.	

Related Federal Legislation (not considered "privacy legislation" but have personal information privacy components)					
Name	**Year Passed**	**Citation**	**Applies to**	**Scope**	**Rules/Guidelines**
Americans With Disabilities Act	1990	42 USC §§12101-12101, §§12111-12117	Employers of 15 or more employees for each working day during each of 20 or more calendar workweeks in the current or preceding calendar year.	Prevents discrimination against employees and applications who are disabled but can perform the essential duties of the job they hold or are seeking.	
Anti-cybersquatting Consumer Protection Act *(amends the Lanham Act (trademarks))*	1999	15 USC §1125	Anyone registering a domain name	Governs the registration, trafficking, or use of domain names that incorporate a third party's trademark or the name of a living person.	

Name	Year Passed	Citation	Applies to	Scope	Rules/Guidelines
Digital Millennium Copyright Act, Title II	1998	Public Law 105-304 (17 USC §512)	Copyright owner or its agent and ISPs	Title II governs notification to ISPs when subscribers are discovered sharing unauthorized materials and establishes limited liability for ISPs for online copyright infringement of subscribers.	
Family & Medical Leave Act (FMLA)	1993	29 USC §§2601-2654	Employers of 50 or more employees for each working day during each of 20 or more calendar workweeks in the current or preceding calendar year.	Governs the process of requesting and granting up to 12 weeks of unpaid leave for medical reasons.	

Appendix B

Resources

- Federal Requirements for Personal Information Protection – ARMA International Educational Foundation

  http://www.armaedfoundation.org/

- THOMAS – Library of Congress

  http://thomas.loc.gov/

- US Code Search

  http://uscode.house.gov/search/criteria.shtml

- Privacy Rights Clearinghouse

  http://www.privacyrights.org/

Bibliography

1. *Foundations of Information Privacy and Data Protection*, Peter P. Swire, CIPP/US and Kenesa Ahmad, CIPP/US, International Association of Privacy Professionals (IAPP), New Hampshire, 2012.
2. *Internet and Online Privacy*, *A Legal and Business Guide*, Andrew Frackmen, Esq., Rebecca C. Martin, Esq., and Claudia Ray, Esq, ALM Publishing, New York, 2002.
3. *Privacy Law*, Charlene Brownlee and Blaze D. Waleski, Law Journal Press, New York, 2016 (Originally published: 2006).
4. *Information Security Law: Control of Digital Assets,* Mark G. Milone, Law Journal Press, New York, 2006, (2007 and 2008 updates).
5. *Federal Privacy Law Compendium*, Stuart McKee and Lester Nakamura, NASCIO, April 2003.
6. *Identity Theft Resource Center*, http://www.idtheftcenter.org.

About the Author

Virginia A Jones, CRM (Certified Records Manager), FAI (Fellow of ARMA International), recently retired as the Records Manager for Newport News Waterworks Department. Her background includes hands-on operations, management, consulting, writing, teaching and training experience for 50 years in the records and information management field. Since 1983, she has also been principal of VAJonesAssociates, a records and information management consulting and training firm.

Ms. Jones has been a member of several AIIM standards committees and is a past member of the AIIM International Standards Board. She was also a member of the U.S. delegation (TAG) to ISO TC 171 the international standards development committee for document management applications. She has been a project leader for several standards/technical report revisions. She was project leader of the ARMA International task force developing and subsequently revising ANSI standard Vital Records Programs: Identifying, Managing, and Recovering Business-Critical Records.

Ms. Jones is the author of Handbook of Microfilm Technology & Procedures (QP Publishing), co-author of Emergency Management for Records and Information Programs (ARMA International), and a co-author of The Information Manager's Toolkit (ARMA International). She has contributed numerous articles on records and information management and micrographics concerns to national trade publications and journals. She is an active member of AIIM International (Old Dominion Chapter) and ARMA International (Tidewater Chapter), and has presented several papers at the national conferences for both associations. She has completed several research projects for the ARMA International Educational Foundation.

Ms. Jones is a Fellow of ARMA International and a Fellow of AIIM International. She is a member of the Institute of Certified Records Managers and a past member of the ICRM Board of Regents.

Funds for this study were provided by the

The ARMA International Educational Foundation (the Foundation) is an education and research funding resource to be used by individuals and organizations for the advancement of knowledge in the field of information management. It is a US non-profit, 501(c)3 organization.

Mission
The ARMA International Educational Foundation supports education and research initiatives that promote the advancement of both information managers and the information management profession.

Purpose
Recorded information is the lifeblood of the modern organization, but rarely is it treated as a critical asset, primarily because there is little quality research to create the comprehensive body of knowledge required to support information management as a profession. The Foundation's purpose is to answer that need by soliciting funds for this research and then providing a vehicle through which conclusions can be tested, documented and communicated to the information management community.

If you found value in this publication, please consider making a financial contribution to the Endowment Fund of the Foundation. This can be accomplished by visiting the Foundation's web site, www.armaedfoundation.org , or by contacting: coordinator@armaedfoundation.org

Additional information about the Foundation can be found at:

The National Database of Non-profit Organizations

To view the report, click:
http://www.guidestar.org/organizations/31-1556655/arma-international-educational-foundation.aspx

Comments about this publication and suggestions for further research are welcome at:
coordinator@armaedfoundation.org