Requirements for Personal Information Protection Part 2: U.S. State Laws

Virginia A Jones, CRM, FAI

November 2009

Revised April 2017

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

www.armaedfoundation.org

TABLE OF CONTENTS

Preface

Requirements for Personal Information Protection Part 2: U.S. State Laws was first published in 2008 by the ARMA International Educational Foundation. Funds for the study were provided under the auspices of ARMA International Educational Foundation. The paper is the result of research by the author to compile known U.S. State Privacy Laws as a reference for records and information management practitioners.

Although most U.S. federal law pertains only to U.S. federal agencies, a number of the laws also either directly relate to or indirectly impact state and local governments. The paper is not a definitive compilation of all state privacy law. The choice of the 26 privacy issues covered in this document is based on high profile privacy issues from the National Conference of State Legislatures, the National Association of Chief Information Officers, and various news sources. The document does not cover identity theft laws or data security laws unless they are included with privacy of personal information requirements. Some Freedom of Information laws having privacy or confidentiality requirements were also included in this document.

This paper is the second of a two-part research project, funded by the ARMA International Educational Foundation, to identify privacy laws that impact records management programs. Part one, *Requirements for Personal Information Protection: U.S. Federal Law*, Revised *2017*, covers protection of personal privacy information in federal law. Both papers are available for download on the AIEF website (http://www.armaedfoundation.org/).

Disclaimer: This research report has not been reviewed by any legal expert and should not be considered legal advice.

Introduction

As with Federal privacy law, organizations must understand complicated and at times conflicting state laws and regulations to protect the data and records of customers and citizens. The proliferation of accessible personally identifiable information (PII) and increasingly easy access to the information has resulted in misuse of personal information by the unscrupulous through identity theft, phishing, spamming, stalking, or preying. There are personal information protection laws in every state but compliance with these laws is often difficult due to their complexity that affect or relate to these issues.

With increased collection of data and easier methods of collection, protecting personal information has become a significant 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 business meetings, government interactions, personal and business banking and other financial transactions, data vaulting, shopping, socializing, and even attending classes. According to the Identity Theft Resource Center there were 36,601,939 records containing sensitive personal information involved in 1,093 security breaches in the U.S. in 2016[1].

As stated in *Requirements for Personal Information Protection Part 1: U.S. Federal Law*, (ARMA International Educational Foundation) there is a generational trust of and reliance on computerized data by younger Americans whose desire for quick access to information or activities leads many to submit personal information online, thus increasing the vulnerability of their personal information. In addition, many more users with limited technical or internet knowledge are now using online services and social networks.

To increase efficiency, data is frequently shared by those who collect it. Increased sharing of data between states law enforcement agencies and states drug monitoring databases, as well as data collected as part of the Affordable Care Act, poses many concerns regarding the protection of personal information. Exposure to privacy information breaches is compounded by the ease of access to personal information.

As breaches and misuse of PII become more prevalent, more laws are necessary to prevent misuse, to prevent unauthorized sharing, and to ensure protection of individual personal information. While there are a number of federal laws for protection of personal information, there are still gaps in protection that have been filled to some degree by individual state laws.

Privacy and Records Management

In 1974, Congress found that "*the right to privacy is a personal and fundamental right protected by the Constitution of the United States*."[2] The need for information privacy

---

[1] Identity Theft Resource Center, ITRC Breach Statistics Report 2015, http://www.idtheftcenter.org/images/breach/2016/ITRCBreachStatsKnownvsUnknownRecordsSummary2016.pdf last accessed 7/29/2017

[2] Public Law 93-579 §2

encompasses all segments of the population. Citizens are affected by government data collection and dissemination. Employees are affected by employer data collection and dissemination and the use made of the data by employers. Customers/consumers are affected by financial 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. A number of privacy laws were enacted by the states to directly address these issues.

The definition of "*personally identifiable information*" or "*personal information*" varies slightly from state to state, and, in fact, individual states can have multiple definitions, spread out over several laws. Most are based, on the Federal Trade Commission (FTC) definition:

> *"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."* [3]

Other definitions can include references to medical information, financial information, educational records, political affiliation, and religious affiliation. For example, in its definition of personal information, Alaska also includes passport number, state identification number, and a combination of individual's name with medical information, insurance policy number, employment information, or employment history.

Privacy can be categorized into four classes.[4]

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

Although the state privacy laws covered in this document includes protection for all four of the privacy classes, information privacy directly relates to records and information management

---

[3] *Online Profiling: A Report to Congress*, Federal Trade Commission, June 2000, page 4, note 14.
[4] *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

(RIM). The impacts of the laws and regulations discussed in this paper are considered with the records management life cycle concept in mind –from creation or receipt of the records and information to final disposition. Privacy law can impact records creation, file management for active and inactive records, records protection, records access, and records retention and disposition.

Almost every privacy law sets requirements for access to personal information, such as who may or may not receive or access the data, and the right of a citizen to inspect and correct records about themselves. For example, those state laws modeled on the federal Privacy Act of 1974 require state agencies to allow a citizen to access their records or any information pertaining to them, permit them to review the records, and permit them to request amendments in the event of errors or omissions.

Since information privacy is integral to records and information management, the records and information manager (or person whose function includes records and information management) should advise and/or assist in establishing processes, procedures and monitoring of personal information activities for compliance with applicable laws and regulations. The records and information manager should be aware of laws pertinent to their organization and the requirements of those laws including rules or regulations generated under the authority of the laws. All RIM policies and procedures should include provisions for protecting personally identifiable information.

Federal Law Relevance

Federal laws relating to the privacy of personally identifiable information cover factors such as 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. Some federal laws pertain only to government, some to certain levels or sectors of government, and some to certain sectors of business such as finance, banking, medical, and telecommunications. Some federal laws also impact state law. In addition, many states have adopted laws similar to federal laws requiring compliance by state and local government.

Federal privacy laws of relevance to states include the Children's Online Privacy Protection Act (COPPA), the Computer Fraud and Abuse Act, the Computer Matching and Privacy Protection Act, the Driver's Privacy Protection Act, the Electronic Communications Privacy Act, the Fair Credit Reporting Act, the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), the Privacy Act of 1974, and the Financial Services Modernization Act (aka Gramm-Leach-Bliley Act). These laws are described in detail in *Requirements for Personal Information Protection Part 1: U.S. Federal Law, Revised 2017 (*ARMA International Educational Foundation).

The Children's Online Privacy Protection Act (COPPA)[5] governs personal information collected online that can serve to identify an individual child. The primary intent is to place parents in

[5] 15 USC §§6501-6506

control of what information is collected from their children online. The Act allows a state attorney general to bring a civil action if a commercial website operator violates COPPA and there is reason to believe that an interest of the state has been or is currently being threatened or adversely affected.

The Computer Fraud and Abuse Act[6] governs access to a computer to obtain information considered to be protected data. The act was intended to only address federal and interstate computer crimes and does not appear to infringe on states' rights and/or computer laws. It specifically does not restrict state or local law enforcement from conducting investigative, protective or intelligence activities. The extortion provision of the Act also covers those who extort "governmental entities," which includes state governments.

The Computer Matching and Privacy Protection Act[7] sets requirements for federal agencies in matching information about individuals held by other federal, state, or local agencies. To participate in a computer matching program, state agencies must enter into a written agreement with a federal agency, and the federal agency's data integrity board must monitor the state agency's compliance. State agencies involved in computer matching programs must not deny, suspend, or terminate assistance under a federal program based upon information obtained through the computer matching program until the Act's notice requirements are met and the information is verified.

The Driver's Privacy Protection Act[8] applies directly to the states. It governs disclosure or availability of personal information obtained in connection with a motor vehicle record. Non-compliance with the Act may result in fines as well as civil actions by individuals whose information has been disclosed. States, at their discretion, can enact their own versions of privacy protections to fill any gaps. (For example, the State of Utah has legislation that provides additional protections for personal information contained in motor vehicle title and registration records.)

The Electronic Communications Privacy Act[9] is relevant for governmental entities attempting to access the contents or records of wire or electronic communications. States must follow the Act's requirements and adhere to its restrictions. The portion of the Act dealing with restrictions on videotape rental and sales records pre-empts state and local laws dealing with the same subject only if the state and local laws require disclosures prohibited by the Act. Some states have laws that prohibit the intentional interception of electronic communications, including e-mail.

The Fair Credit Reporting Act (FCRA)[10] addresses the use and disclosure of an individual's credit report information, including the use of credit report information by employers in employment

[6] 18 USC §§1030 and 1037
[7] 1988, Amended 1990
[8] 18 USC §§2721-2725
[9] 18 USC §§2510-2522, 2701-2711, & 3121-3127
[10] 15USC §§1681 *et seq.*

decisions. Through the Fair and Accurate Credit Transactions Act amendment, Congress preempted the states on credit and debit card truncation and set a national standard. This does not affect consistent state laws dealing with the collection, distribution, or use of consumer information, but the Act takes precedence over inconsistent state laws. The Act prevents states from regulating certain areas covered by FCRA, except where state laws enacted after January 1, 2004 explicitly state the intent to supplement FCRA and provide greater consumer protection.

The Family Educational Rights and Privacy Act (FERPA)[11] governs the privacy of student's education records. It applies to educational agencies and institutions that receive funds under an applicable program of the Department of Education, including state educational agencies or institutions. The Act applies specifically to state educational agencies or institutions regarding the right of a parent to inspect his or her child's education records.

The Health Insurance Portability and Accountability Act (HIPAA)[12] governs the disclosure of protected health information. It was enacted to standardize the electronic exchange of health information and to improve the privacy and security of health information. HIPAA preempts state law with some exceptions.

The HIPAA Privacy Rule covers medical records and other individually identifiable health information used or disclosed by an entity covered by HIPAA. The information can be in paper form, electronic form, or transmitted orally. The HIPAA Privacy Rule does not preempt state law in four instances:

1. Where the Secretary of U.S. Health and Human Services

    a) determines that the state law provision is necessary to prevent fraud and abuse, to ensure appropriate state regulation of insurance and health plans, to support state reporting on health care delivery or costs, or to serve a compelling need related to public health, safety or welfare; and/or

    b) determines that a contrary provision of state law has as its principal purpose the regulation of the manufacture, registration, distribution or dispensing, or other control of any controlled substance.

2. The state law is more stringent than the HIPAA Privacy Rule in that it is more protective of an individual's privacy or it provides the individual with greater rights.

3. The state law provides for the reporting of diseases or injury, child abuse, birth, death, or for the conduct of public health surveillance, investigation or intervention.

4. The state law requires a health plan to report, or provide access to, information for the purpose of management audits, financial audits, program monitoring and evaluation, or the licensure or certification of facilities or individuals.

---

[11] 29 USC §§2601-2654
[12] Public Law 104-191

As part of HIPAA, HHS issued regulations requiring health care providers, health plans, and other entities covered by the HIPAA to notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been accessed, acquired, used, or disclosed as a result of a breach. These "breach notification" regulations under HIPAA were implemented the HITECH Act.

The Privacy Act of 1974[13] applies to U.S. Federal Executive Branch. It establishes certain controls over what personal information is collected by the federal government and how it is used. Section 7 of this Act applies to federal, state, and local agencies. It prohibits, with some exceptions, agencies from denying an individual any right, benefit, or privilege because of his or her refusal to disclose a Social Security Number (SSN).

The Financial Services Modernization Act (aka Gramm-Leach-Bliley Act)[14] applies to financial institutions (as defined in the Act) and governs the privacy and security of personal financial information. Title V of the Act 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. The Act does not supersede, alter, or affect state laws or regulations unless they are inconsistent. For those entities regulated by the Federal Trade Commission (FTC), states also can provide greater legal protections as long as the FTC deems them not inconsistent with the Act. For example, the California Financial Information Privacy Act sets requirements for California financial institutions that are more stringent than the Gramm-Leach-Bliley Act.

State Law

State laws generally cover the same requirements found in federal law:

- What can be collected;
- How it can be used;
- How and where it can be disseminated;
- Rights of citizens, including the right to see what information has been collected and/or maintained about them; and/or
- The right of citizens to correct incorrect information maintained about themselves.

Some state laws also set penalties if compliance or privacy is breached. Depending on the state, the penalties may be either criminal or civil.

Many states have adopted laws similar to Federal laws for compliance by state and local government – such as limiting the use of social security numbers and collecting financial or health information. Some states have enacted additional privacy laws not covered by federal

[13] 5 USC §552a
[14] 15USC §§6801-6809 & 6821

law – such as genetic testing laws and data breach notification laws. This research paper describes three major areas of privacy protection set by state law – privacy in state Constitutions, privacy torts, and state privacy laws.

Privacy in State Constitutions

Not all state constitutions specifically address privacy. Constitutions in ten states *expressly* recognize a right to privacy. Some other states address constitutional rights of privacy through court decisions. The term "right of privacy" is often used interchangeably when referring to the constitutional right of privacy or to the common law right to privacy under state tort law. Constitutional right is distinctly different from tort law. Constitutional privacy right is not extended to invasions of privacy covered by state tort law.

Privacy Tort

A *tort* is a wrongful act, other than a breach of contract, that results in injury to another's person, property, reputation, or the like, and for which the injured party is entitled to compensation.[15] It is a civil wrong arising from an act or failure to act, independently of any contract, for which an action for personal injury or property damages may be brought.[16]

The common law concepts of privacy exist in 47 states. Two states recognize a civil right of action for invasion of privacy. New York does not have a common law right of privacy, but it does have a tort for appropriation of a person's name or picture without written consent that is also a misdemeanor.

The common laws of privacy generally recognize four types of privacy tort:[17]

1. Intrusion can include information stored on a person's computer, and can also involve online information.
    - Intrusion upon seclusion - unwelcome or unauthorized invasion upon the solitude of another or upon his or her private space or affairs;
    - An intrusion that is offensive or objectionable to a reasonable person;
    - An intrusion upon a private matter; and/or
    - An intrusion that causes anguish and suffering.
2. Public disclosure is the disclosure of truthful, though negative, information regarding an individual that is not a matter of legitimate public concern.

---

[15] Dictionary.com Unabridged, based on the Random House Dictionary, © Random House, Inc. 2016, (http://dictionary.reference.com/browse/tort) last accessed March, 2016.
[16] Collins English Dictionary - Complete & Unabridged 2012 Digital Edition © William Collins Sons & Co. Ltd., 1986, © HarperCollins Publishers, 2012, (http://dictionary.reference.com/browse/tort) last accessed March, 2016.
[17] *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, §604.8

3. False light is the dissemination of untrue information regarding an individual, which is offensive to a reasonable person.
4. Misappropriation is the unauthorized adoption and use by one person of the name or likeness of another.

The common law privacy torts are often referenced in cases regarding character defamation, paparazzi stalking, and identity theft.

State Privacy Laws

The majority of privacy protection is derived from state statutes and codes. This paper covers twenty-six privacy issues regulated by laws in all 50 states and the District of Columbia. Every state does not have laws covering every issue. The range and statutory requirements differ from state to state. The twenty-six issues include:

General Privacy

- Personally Identifiable Information (PII) /Personal Information Definition;
- Personal Information Privacy;
- Library Patron Records and e-reader privacy;
- Privacy in State Constitution;
- Data (Security) Breach;
- Disposal of Records Containing Social Security Numbers (SSN) or PII;
- SSN Restricted Use;
- Radio Frequency Identification (RFID) and Privacy;
- Student Information;

Financial Information Privacy

- Consumer Protection;
- Credit Card Number on Receipts;
- Security Freeze;
- Financial Information Privacy;
- Insurance Information Privacy;

Health Information Privacy

- Genetic Privacy;
- Health Information Privacy;
- Prescription Drug Database and/or Prescription Drug Monitoring;

Online and Data Privacy

- Electronic Surveillance;
- Data Sharing;
- Privacy of Personal Information: Internet;
- Employee E-mail Communications and Internet Access;
- Privacy Policies on Web Sites;
- Privacy Policies: Government Web Sites;
- Interception of Electronic Communications;
- Spyware; and
- Phishing;

State laws continue to evolve, and, as personal privacy and identity theft continues to be a growing issue, states will continue to enact laws for privacy protection. While this paper includes citations for each state that are current through the end of 2016, records managers should diligently monitor pertinent state legislation for new issues and laws.

General Privacy

PII /Personal Information Definition

Only three states and the District of Columbia do not have laws containing definitions of "personally identifiable information" or "personal information" ranging from a simple definition in one state law to many definitions in multiple laws for the same state. Generally, all definitions specify the data subject's name and social security and other identifying numbers as private. Arizona and Michigan, for example, each define PII in 5 separate laws. Each definition is slightly different and pertains to the circumstances covered by that particular law.

Personal Information Privacy

Nine states have enacted personal privacy laws based on the Federal Privacy Act that pertain to state agency and local government collection and use of personal information. As with the federal Act, the laws emphasize that information collected for one purpose may not be used for other purposes without notifying the citizen. The laws allow citizens to see what PII is maintained about themselves and they have the right to correct incorrect information. Some states give citizens the right to request a list of who has had access to their PII.

Library Patron Records and e-reader Privacy

Forty-five states and the District of Columbia have enacted laws to protect the confidentiality of personal information about a library patron. The states without such laws include Hawaii, Kentucky, North Dakota, Oklahoma, and Oregon. Some of the states also require confidentiality for records regarding library materials accessed or checked out by a patron. As this requirement may conflict with the USA FREEDOM Act, many states allow release of the information for "law enforcement" purposes. Some states require digital book services and online book sellers to protect the personal information of users purchasing e-readers or related services.

Privacy in State Constitution

Some states cover privacy in State constitutions. Constitutions in 10 states—Alaska, Arizona, California, Florida, Hawaii, Illinois, Louisiana, Montana, South Carolina and Washington—have explicit provisions around the right to privacy. Some of the privacy protections mirror the Fourth Amendment of the U.S. Constitution relating to search and seizure or government surveillance, with more specific references to privacy. [18]

Data (Security) Breach

Forty-seven states and the District of Columbia require notification of security breaches involving personal information; only Alabama, New Mexico, and South Dakota do not. In some states, the law outlines the information that must be included in the notification. Some states have state laws that require breaches to be reported to a centralized data base, including Maine, Maryland, New York, New Hampshire, North Carolina, Vermont and Virginia (Virginia's notification law only applies to electronic breaches affecting more than 1,000 customers).

However, a number of other states have some level of notification that is made publicly available, usually through response to Freedom of Information requests. These states include California, Colorado, Florida, Illinois, Massachusetts, Michigan, Nebraska, Hawaii and Wisconsin. Those states with no security breach law are Alabama, New Mexico, and South Dakota. There is currently no inclusive federal security breach law. The federal HITECH Act requires notification of breach of personal information by certain health care entities defined in HIPAA.

Disposal of records containing SSN or PII

Thirty-three states have laws that either specify how records containing SSN or PII may be disposed (shredding, pulping, drilling a hard disk) or require the records to be disposed of "responsibly." Some states law pertains only to government entities, other states law pertains to anyone doing business in the state.

SSN Restricted Use

All fifty states and the District of Columbia have enacted laws protecting social security numbers. The laws vary from state to state and include a range of coverage:

- Places restrictions on the collection and use of Social Security numbers;
- Prohibits the release of an employee's Social Security number;
- Requires a business that collects Social Security numbers to create a privacy protection policy that must ensure confidentiality of Social Security numbers;
- Restricts access to Social Security numbers (SSNs) on birth, death, and marriage certificates;

[18] National Conference of State Legislatures, Provisions Related To The Right To Privacy, http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx, last accessed 03/30/2016.

- Eliminates the use of voters' Social Security numbers on certain election-related documents;
- Prohibits the inclusion of Social Security numbers on motor vehicle registration renewal notices;
- Provides that no government agency shall require an individual to furnish or disclose his Social Security number; and

Radio Frequency Identification (RFID) and Privacy

Nineteen states have enacted laws regarding the use of RFID tags. The laws vary and include prohibiting requiring the implantation of a RFID microchip, prohibiting unauthorized "skimming" of RFID in ID cards, and the use of RFID in driver licenses or vehicles.

RFID is a technology that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency portion of the electromagnetic spectrum to uniquely identify an object, animal, or person.[19] A simple RFID tag, when stimulated by a remote reader, sends back information via radio waves. The use of RFID has raised privacy concerns in some states, particularly with regard to the potential linking of personal information with RFID tags.

Student Information

Six states have enacted laws requiring the protection of student PII. Most specifically prohibit education technology service providers, such as operators of Internet websites, online or cloud computing services, and mobile services from selling student data, using student data to engage in targeted advertising to students or their families, amassing a profile on students to be used for non-educational purposes, or disclosing student data except as permitted by law. Some also require educational technology providers to have reasonable procedures and practices for ensuring the security of student data they collect or maintain, protecting that student data from unauthorized access, destruction, use, modification, or disclosure, and deleting the student data within a specified time frame or under specific conditions.

FINANCIAL INFORMATION PRIVACY

Consumer Protection

Seventeen states have consumer protection laws that resemble the FTC law in restricting certain business practices that contravene a state's interests in protecting its consumers. Typically, the laws prohibit businesses from engaging in false, misleading, or deceptive practices, and are used to intervene in business transactions involving the transfer of personal information in violation of the state consumer protection law.

Credit Card Number on Receipts

Thirty-six states have laws that prohibit all but the last 4 or last 5 numbers of a payment or credit card to be printed on a receipt. Through the Fair and Accurate Credit Transactions Act, Congress preempted the states on credit and debit card truncation to set a national standard.

---

[19] Whatis.com, (http://internetofthingsagenda.techtarget.com/definition/RFID-radio-frequency-identification), last accessed March, 2016

Under Title I, §113 of the Act, only the last five digits of the card account number can be printed on electronically printed receipts provided to the customer. The new truncation requirement does not apply to handwritten receipts or receipts imprinted with a copy of the credit card.

Security Freeze

Forty-nine states and the District of Columbia have enacted laws allowing consumers to place "security freeze" on their credit reports. Michigan is the only state without a "security freeze" law. A consumer report security freeze limits a consumer reporting agency from releasing a credit report or any information from the report without authorization from the consumer. If a person suspects that he or she has been victimized by identity theft, a consumer report security freeze can help the person track whether an identity thief is using the person's information to set up bogus accounts.

Financial Information Privacy

Nineteen states have enacted laws similar to the requirements of the Graham-Leach-Bliley Act. The laws usually reinforce the privacy requirements of the Act, although some are more stringent. Generally, the laws pertain to financial institutions, although a few states also include government handling of financial information (such as personal income tax information).

Insurance Information Privacy

Seventeen states have laws protecting the privacy of medical information and financial information collected for insurance policy purposes. California's Insurance Information and Privacy Protection Act, for example, sets privacy requirements on state licensed insurance entities similar to those required of financial institutions by the Graham-Leach-Bliley Act.

HEALTH INFORMATION PRIVACY

Genetic Privacy

Thirty-seven states have enacted laws to safeguard genetic information beyond the protections provided for other types of health information. This approach provides special legal protections for genetic information as a result of its predictive, personal and familial nature, and other unique characteristics. With respect to privacy, Washington is the only state that treats genetic information the same as other health information by including genetic information in the definition of health care information under the state health privacy law.

State genetic privacy laws typically restrict parties (such as insurers or employers) from carrying out a particular action without consent. Some states require informed consent for a third party either to perform or require a genetic test or to obtain genetic information, and some states require consent to disclose genetic information. Five states explicitly define genetic information as personal property. Nineteen states have established specific penalties - civil, criminal or both - for violating genetic privacy laws.

The states with genetic privacy laws also may have laws concerning other, related genetics policy issues, such as the use of genetic information in insurance and employment. All laws prohibit discrimination based on the results of genetic tests. Most states also restrict employer access to genetic information.

Health Information Privacy
Sixteen states have enacted laws similar to HIPAA that, in some cases, are more stringent that the federal law or that cover more types of medical or health records than the federal law. For example, Alabama has specific statutes protecting privacy of certain health information such as HIV/AIDS test results and mental health records and Texas law prohibits employers from providing personal health information without first obtaining the employee's consent.

HIPAA requires covered entities, including state governments, to have privacy officers. All 50 states and the District of Columbia have HIPAA privacy officers.

Prescription Drug Database and/or Prescription Drug Monitoring
Twenty-eight states have a centralized prescription drug database that is considered confidential. Prescription Drug Monitoring Programs (PDMPs) allow physicians and pharmacists to log each filled prescription into a state database to help medical professionals prevent abusers from obtaining prescriptions from multiple doctors.

ONLINE AND DATA PRIVACY
Electronic Surveillance
Forty-nine states and the District of Columbia have laws regarding electronic surveillance. Vermont is the only state without an electronic surveillance law.

Electronic surveillance involves the traditional laws on wiretapping--any interception of a telephone transmission by accessing the telephone signal itself--and eavesdropping--listening in on conversations without the consent of the parties. Some states have extended these laws to cover data communications as well as telephone surveillance. Some state electronic surveillance laws include prohibiting the intentional interception of electronic communications, including e-mail. Some states have also included photo or video surveillance and cell phones in their electronic surveillance laws.

Data Sharing
Four states have laws regarding the sharing of citizen or customer/client data. For example, California and Utah have laws that require all nonfinancial businesses, including on-line businesses, to disclose to customers, in writing or by electronic mail, the types of personal information the business shares with or sells to a third party for direct marketing purposes or for compensation. Under the California law, businesses may post a privacy statement that gives customers the opportunity to choose not to share information at no cost.

Privacy of Personal Information - Internet
Seven states have laws regarding the online privacy of personal information. Some states require Internet Service Providers (ISPs) to keep certain customer personal information private, unless the customer gives permission to disclose the information, and also prohibit disclosure of personally identifying information.

Some states require all nonfinancial businesses to disclose to customers, in writing or by

electronic mail, the types of personal information the business shares with or sells to a third party. Missouri law prohibits the posting of certain personal information on the Internet with the intention of causing or threatening great bodily harm or death.

Employee E-mail Communications and Internet Access

Four states require employers to give notice to employees prior to monitoring e-mail communications, Internet access, or to provide policy regarding the monitoring of email communications or internet access by employees.

Privacy Policies on Web Sites

Five states have enacted laws regarding the privacy policies posted on web sites. Some require entities that collect personally identifiable information from online users to conspicuously post its privacy policy on its Web site or online service, and to comply with that policy. Some states have laws that prohibit knowingly making a false or misleading statement in a privacy policy published on the Internet, or otherwise distributed or published.

Privacy Policies: Government Web Sites

Seventeen states require by statute, government Web sites, or state portals, to establish privacy policies and procedures, or to incorporate machine-readable privacy policies into their Web sites.

Interception of Electronic Communication

Nineteen states have laws regulating the interception of wire, oral, and electronic communications to protect the privacy of innocent persons and accessing stored electronic communications. Some states also include the use of pen registers and trap and trap devices.

Spyware

Fifteen states have passed some form of anti-spyware laws. Spyware is malicious software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user. It can track or collect the online activities or personal information of Web users, change settings on users' computers, or cause advertising messages to pop up on users' computer screens.

Phishing

Eleven states have laws that specifically address phishing. Phishing is a scam where fraudsters send spam or popup messages to lure personal or financial information from unsuspecting victims.

To aid in understanding the particular laws for each state pertaining to the issues covered by this paper, a table for each state is included showing the citations per privacy issue. Only enacted laws are included for each state, however, not all states have laws pertaining to all issues. Each table also includes the URL for that state's statutes or codes. Specific URLs directing the user to a LexisNexis site are free access. All resources used for research for this paper are listed in Appendix A – Resources. In addition, a full matrix of all states, all 26 issues,

and the pertinent citations for each issue for each state is included in Appendix B.

Laws – State by State

The following tables show the citations per privacy issue for each state. Only enacted laws are included for each state. As shown, not all states have laws pertaining to all issues.

Alabama

State Code: Code of Alabama
http://alisondb.legislature.state.al.us/alison/codeofalabama/1975/coatoc.htm

PII /Personal Information Definition	§13A-8-191
Library Patron Records & e-reader Privacy	§§41-8-9 & 10
Data (Security) Breach	none
Security Freeze	§13A-8-200
Health Information Privacy	§22-56-4b(6) & (7) §§22-11A-2, 14, 22, 38, 54 & 69 §22-11C-7 §22-13-33
Prescription Drug Database and/or Prescription Drug Monitoring	§§20-2-210 *et seq*
SSN Restricted Use	§41-13-6 §17-4-38
Radio Frequency Identification (RFID) and Privacy	§13A-8-111 & 113
Electronic Surveillance	§13A-11-30 *et seq*

Alaska

State Code: Alaska Statutes
http://www.legis.state.ak.us/basis/statutes.asp#01

PII /Personal Information Definition	§45.48.590 §45.48.090
Library Patron Records & e-reader Privacy	§40.25.140
Privacy in State Constitution	Article I, §22
Data (Security) Breach	§§45.48.010 *et seq*
Disposal of records containing SSN or PII	§§45.48.500 *et seq*
Credit Card Number on Receipts	§§45.48.750 *et seq*
Security Freeze	§§45.48.100 *et seq*
Financial Information Privacy (Banking and Financial Institutions – Depositor and Customer Records)	§06.01.028
Genetic Privacy	§18.13.010-100
Prescription Drug Database and/or Prescription Drug Monitoring	§17.30.200
SSN Restricted Use	§45.48-400 §23.30.107(b)
Electronic Surveillance	§42.20.310
Spyware	§45.45.792

Arizona

State Code: Arizona Revised Statutes
http://www.azleg.gov/arstitle/

PII /Personal Information Definition:	§28-440 §13-2001 §44-7301 §44-7201 §44-7501
Library Patron Records & e-reader Privacy	§41-1354 §41-151.22
Privacy in State Constitution	Article II, §8
Data (Security) Breach	§44-7501
Disposal of records containing SSN or PII	§44-7601
Credit Card Number on Receipts	§44-1367
Security Freeze	§44-1698
Genetic Privacy	§20-448.02
Prescription Drug Database and/or Prescription Drug Monitoring	§36-2608
SSN Restricted Use	§15-1823 §§44-1373 – 44-1373.03 §16-168F §11-461 §25-501 §25-806
Electronic Surveillance	§13-3005
Privacy Policies: Government Web Sites	§§41-4151 & 41-4152
Spyware	§44-7302

Arkansas

State Code: Arkansas Code
http://www.lexisnexis.com/hottopics/arcode/Default.asp

PII /Personal Information Definition	§4-110-103 §§ 4-110-101 – 108
Library Patron Records & e-reader Privacy	§§13-2-701 – 13-2-706
Data (Security) Breach	§§4-110-101 – 4-110-108
Disposal of records containing SSN or PII	§4-110-103 & 104
Security Freeze	§§4-112-101 *et seq*
Genetic Privacy	§20-35-101 – 103
SSN Restricted Use	§4-86-107 §6-18-208
Radio Frequency Identification (RFID) and Privacy	§27-16-1206
Electronic Surveillance:	§5-60-120 §5-16-101
Privacy Policies: Government Web Sites	§25-1-114
Spyware	§4-111-103
Phishing	§§4-111-102 – 103

California

State Code: California Statutes - 29 Codes
http://leginfo.legislature.ca.gov/faces/codes.xhtml

PII /Personal Information Definition	Civil Code §1798.80; §1798.92
Library Patron Records & e-reader Privacy	Government Code §6254(j); §6267; §6276.28
Personal Information Privacy	Government Code §§11549 – 11549.6; §11019.9; §1798.82 Civil Code §1798.83 to 84
Privacy in State Constitution	Article I, §1
Data (Security) Breach	Civil Code - §1798.29 §§1798.82 through 1798 -– 84
Disposal of records containing SSN or PII	Civil Code §§1798.80 – 1798.84
Consumer Protection	Civil Code §§1798.80 -– 1798.84
Student Information	Business and Professions Code §§22.2 -22584 & 22585
Credit Card Number on Receipts	Civil Code §1747.9
Security Freeze	§§1785.11.2 *et seq*
Financial Information Privacy	Financial Code §§4050 -– 4060; §4161; §§1785.1 *et seq*
Insurance Information Privacy	Code of Regulations §§2689.1 – 2689.24 Insurance Code §§791 -– 791.28
Genetic Privacy	Insurance Code §10149.1
Health Information Privacy	Civil Code §56 – 56.07; §56.10 §§56.16 & 56.17; §§56.20 – 56.265; §§56.27-56.31; §§56.35-56.37

SSN Restricted Use	Civil Code §1798.85 – .86; §1798.89 Elections Code §2138.5; Code of Civil Procedure §674; Revenue and Taxation
	Code §2191.3; Commercial Code §9526.5; Government Code §§6254.27 – 6254.29; §15705 §27300 *et seq*; Welfare and Institutions Code §14045; Labor Code § 226
RFID & Privacy	Civil Code §52.7; §§1798.79 & 1798.795; Finance Code §13082
Electronic Surveillance	Penal Code §§631 – 632
Data Sharing	Civil Code §§1798.83 – .84
Privacy of Personal Information: Internet	Business and Professions Code §§22575 – 22582
Privacy Policies on Web Sites	Business & Professions Code §§22575 – 22578 Education Code §99122
Privacy Policies: Government Web Sites	Government Code §11019.9
Spyware	Business & Professions Code §22947
Phishing	Business & Professions Code §§22948 – 22948.3

Colorado

State Code: Colorado Revised Statutes
http://www.lexisnexis.com/hottopics/Colorado/

PII /Personal Information Definition	§6-1-713
Library Patron Records & e-reader Privacy	§24-90-119
Data (Security) Breach	§6-1-716
Disposal of records containing SSN or PII	§6-1-713
Consumer Protection	§6-1-105
Credit Card Number on Receipts	§6-1-711
Security Freeze	§§12-14.3-106.6 & 106.7
Genetic Privacy	§10-3-1104.7
Prescription Drug Database and/or Prescription Drug Monitoring	§12-22-704
SSN Restricted Use	§6-1-715 §23-5-127 §24-72.3-102 §14-10-115 §14-14-113 (1) (b) §26-13-127
Electronic Surveillance	§18-9-303
Employee E-mail Communications and Internet Access	§24-72-204.5
Privacy Policies: Government Web Sites	§§24-72-501 & 502

Connecticut

State Code: Connecticut General Statutes
https://www.cga.ct.gov/current/pub/titles.htm

PII /Personal Information Definition	§14-10; §38a-976; §42-471
Library Patron Records & e-reader Privacy	§11-25
Data (Security) Breach	§36A-701(b)
Disposal of records containing SSN or PII	§42-471
Security Freeze	§§36a-701*et seq*
Financial Information Privacy	§§ 36a-41 – 36a-45
Insurance Information Privacy	§38a-975
Prescription Drug Database and/or Prescription Drug Monitoring	§21a-254
SSN Restricted Use	§42-470; §42-471; §§7-51 & 7-51a; §14-10
Electronic Surveillance	§52-570d
Employee E-mail Communications and Internet Access	§31-48d
Privacy Policies on Web Sites	§42-471

Delaware

State Code: Delaware Code
http://delcode.delaware.gov/

PII /Personal Information Definition	Title 11 §854
Library Patron Records & e-reader Privacy	Title 29 §10002(g) (12) Title 6 §1206C
Data (Security) Breach	Title 6 §§12B-101 – 12B-104
Disposal of records containing SSN or PII	Title 6 §5001C to 5004C Title 19 §736
Consumer Protection	Title 6 §2533
Student Information	Title 14 §8101A to 8106A (effective 08/2017)
Credit Card Number on Receipts	Title 5 §915A
Security Freeze	Title 6 §2203
Genetic Privacy	Title 16 §§1220 – 1227
SSN Restricted Use	Title 11 §914
Electronic Surveillance	Title 11 §2402 – 2403
Privacy of Personal Information: Internet	Title 6 §1204C
Employee E-mail Communications and Internet Access	Title 19 §705
Privacy Policies on Web Sites	Title 6 §205C
Privacy Policies: Government Web Sites	Title 29 §9017C *et seq.*

District of Columbia

State Code: District of Columbia Code
http://dccode.elaws.us/

Data (Security) Breach	§28- 3851 *et seq*
Library Patron Records & e-reader Privacy	§39-108
Security Freeze	§§28-3861 – 3864
SSN Restricted Use	§§47-3151 – 3154
Electronic Surveillance	§23-542

Florida

State Code: Florida Statutes
http://www.leg.state.fl.us/Statutes/index.cfm?Mode=View%20Statutes&Submenu=1&Tab=statutes&CFID=72725658&CFTOKEN=42781737

Library Patron Records & e-reader Privacy	§257.261
Privacy in State Constitution	Article I §§12 & 23
Data (Security) Breach	§817.5681 §501.171.2(3 to 7)
Disposal of records containing SSN or PII	§501-171(8)
Consumer Protection	§817.02
Credit Card Number on Receipts	§501.0118
Security Freeze	§501.005
Financial Information Privacy	§655.059
Genetic Privacy	§760.40
Prescription Drug Database and/or Prescription Drug Monitoring	§893.055
SSN Restricted Use	§97.0585; §119.0714; §741.465
Electronic Surveillance	§934.03

Georgia

State Code: Code of Georgia Annotated
http://www.lexisnexis.com/hottopics/gacode/Default.asp

PII /Personal Information Definition	§10-15-1
Library Patron Records & e-reader Privacy	§24-9-46
Data (Security) Breach	§§10-1-910 – 10-1-912
Disposal of records containing SSN or PII	§10-15-2
Consumer Protection	§10-1-373
Credit Card Number on Receipts	§10-15-3
Security Freeze	§§10-1-913 – 10-1-915
Genetic Privacy	§§33-54-1 to 8
SSN Restricted Use	§10-1-393.8; §40-5-28.1; §50-18-72
Electronic Surveillance	§16-11-62
Spyware	§16-9-152
Phishing	§16-9-109.1

Hawaii

State Code: Hawaii Revised Statutes
http://www.capitol.hawaii.gov/docs/HRS.htm

Privacy in State Constitution	Article I, §§6 & 7
Data (Security) Breach	§§487N-1 – N-4
Disposal of records containing SSN or PII	§487R-1 – 4
Consumer Protection	§481A-4
Security Freeze	§§489P-1 – 6
Genetic Privacy	§431:10A-118
Prescription Drug Database and/or Prescription Drug Monitoring	§329-101 *et seq*
SSN Restricted Use	§§487J-1 – 487J-4; §487R-2; §501-151; §502-33; §504-1; §636-3; §803-6; §92F-12
Electronic Surveillance	§803-42

Idaho

State Code: Idaho Statutes
https://legislature.idaho.gov/statutesrules/idstat/

PII /Personal Information Definition	§28-51-104; §28-52-102
Library Patron Records & e-reader Privacy	§9-340E(3)
Data (Security) Breach	§§28-51-104 – 28-51-107
Credit Card Number on Receipts	§28-51-103
Security Freeze	§§28-52-103 – 107
Genetic Privacy	§39-8301 – 8304; §41-1313
Prescription Drug Database and/or Prescription Drug Monitoring	§37-2726
SSN Restricted Use	§18-3122; §18-3126
Electronic Surveillance	§18-6702

Illinois

State Code: Illinois Compiled Statutes
http://www.ilga.gov/legislation/ilcs/ilcs.asp

PII /Personal Information Definition	815 ILCS §530/5
Library Patron Records & e-reader Privacy	5 ILCS §140/7(l)
Privacy in State Constitution	Article I, §§6
Data (Security) Breach	815 ILCS §530/1 – 530/30
Disposal of records containing SSN or PII	815 ILCS §530/30 & 530/40 20 ILCS § 450/20
RFID & Privacy	5 ILCS §179/30 720 ILCS §§5/16-0.1 & 30
Consumer Protection	815 ILCS §510/3
Credit Card Number on Receipts	815 ILCS §505/2MM
Security Freeze	815 ILCS §505/2MM
Financial Information Privacy	205 ILCS §105/3-8 & §5/48.1 *et seq.*
Genetic Privacy	410 ILCS §513/15
Prescription Drug Database and/or Prescription Drug Monitoring	720 ILCS §570/317
SSN Restricted Use	110 ILCS §§305/30, §520/16, §660/5-125, §665/10-125, §670/15-125, §675/20-130, §680/25-125, §685/30-135, §690/35-130, §805/3-60; 805 ILCS §505/2RR
Electronic Surveillance	720 ILCS §5/14-1
Privacy Policies: Government Web Sites	5 ILCS §177/15
Phishing	740 ILCS §§7/1 - 7/15

Indiana

State Code: Indiana Code
http://www.in.gov/legislative/ic/code/

PII /Personal Information Definition	§4-1-6-1
Personal Privacy	§4-1-6 *et seq*
Library Patron Records & e-reader Privacy	§5-14-3-4 (a)(16)
Data (Security) Breach	§§24-4.9-1-1 – 24-4.9-1-5; §§4-1-11-1 to 4-1-11-10
Disposal of records containing SSN or PII	§24-4-14-8 §24-4-9-3.5 to 5(c)
Credit Card Number on Receipts	§24-5-24
Security Freeze	§§ 24-5-24-1 – 24-5-24-17
SSN Restricted Use	§§4-1-10-1 *et seq*; §36-2-11-15
Electronic Surveillance	§35-33.5-1-5
Spyware	§24-4.8-2-3

Iowa

State Code: Iowa Code
https://www.legis.iowa.gov/law/statutory

PII /Personal Information Definition	§715C; §61-2.1; §321.11
Library Patron Records & e-reader Privacy	§22.7-13
Data (Security) Breach	§715C
Security Freeze	§§714G.1 – G.11
SSN Restricted Use	§22.3B; §22.7-32
Electronic Surveillance	§727.8
Privacy Policies: Government Web Sites	§22.11
Spyware	§715.4

Kansas

State Code: Kansas Statutes
http://www.kslegislature.org/li/b2017_18/statute/

PII /Personal Information Definition	§50-7a01(g)
Library Patron Records & e-reader Privacy	§45-221(a)(23)
Data (Security) Breach	§§50-7a01 & 50-7a02
Disposal of records containing SSN or PII	§50-7a01 & 03
Consumer Protection	§50-7a01
Credit Card Number on Receipts	§50-669b
Security Freeze	§50-723
Prescription Drug Database and/or Prescription Drug Monitoring	§65-1681 *et seq*
SSN Restricted Use	§75-3520; §40-2425; §76-768; §17-12a607
Electronic Surveillance	§21-4001

Kentucky

State Code: Kentucky Revised Statutes
http://www.lrc.ky.gov/statutes/

PII /Personal Information Definition	§365.720(4)
Data (Security) Breach	§365.732 §61.931 to 934
Disposal of records containing SSN or PII	§365.725
Credit Card Number on Receipts	§§434.550 – 434.730
Security Freeze	§367.365
SSN Restricted Use	§15.400(3); §15.540(2); §216.2927(4)
Electronic Surveillance	§526.010
Phishing	§434.697

Louisiana

State Code: Codified Laws of Louisiana
https://www.legis.la.gov/legis/lawsearch.aspx

PII /Personal Information Definition	§37:1782; §51:2007; §14:67.16
Library Patron Records & e-reader Privacy	§44:13
Privacy in State Constitution	Article I, §5
Data (Security) Breach	§§51:3071 through 51:3077
Credit Card Number on Receipts	§9:3518.3
Security Freeze	§9:3571.1
Genetic Privacy	§22:213.7; §40:1299.6
Prescription Drug Database and/or Prescription Drug Monitoring	§40:1004 *et seq*
SSN Restricted Use	Code of Civil Procedure Article 1922;
Electronic Surveillance	§15:1303
Spyware	§51:2008
Phishing	§§51:2021 – 2025; §§51:2031 – 2034; §§51:2073 – 2074

Maine

State Code: Maine Statutes
http://www.mainelegislature.org/legis/statutes/search.htm

PII /Personal Information Definition	Title 10 §1347, §9551, §1312, Title 33 §651-B
Library Patron Records & e-reader Privacy	Title 27 §121
Data (Security) Breach	Title 10 §§1346 – 1349
Student Information	Title 20A §951 & 953
Credit Card Number on Receipts	Title 10, §1149
Security Freeze	Title 10 §1313-C
Financial Information Privacy	Title 9-B §§161– 164
Insurance Information Privacy	Title 24-A §2204
Health Information Privacy	Title 22 §1711-C
Prescription Drug Database and/or Prescription Drug Monitoring	Title 22 §7248
SSN Restricted Use	Title 10 §§1271 – 1284; Title 32 §16607(2)(E)
Electronic Surveillance	Title 15, §709
Privacy Policies: Government Web Sites	Title 1 §14-A; §§541–542

Maryland

State Code: Maryland Code
http://www.lexisnexis.com/hottopics/mdcode/

PII /Personal Information Definition	§14–3501; §10-624
Personal Privacy	§10-624
Library Patron Records & e-reader Privacy	§23-107
Data (Security) Breach	§§14-3501 – 14-3508
Disposal of records containing SSN or PII	§14-3502(b) §10-1301 to 1303
Credit Card Number on Receipts	§14-1318
Security Freeze	§14-1212.1
Financial Information Privacy	§§1-301 – 306
Genetic Privacy	§27-909, §49B-15 & 16
SSN Restricted Use	§§14-3401 *et seq*; §1-109; §6-114, §7-113, §15-110; §1-202
Electronic Surveillance	§10-402
Privacy Policies: Government Web Sites	§10-624 (4)

Massachusetts

State Code: Massachusetts General Laws
http://www.mass.gov/legis/laws/mgl/index.htm

PII /Personal Information Definition	Chapter 93: §105; Chapter 66A: §1
Personal Privacy	Chapter 66A: §§1 *et seq*
Library Patron Records & e-reader Privacy	Chapter 78: §7
Data (Security) Breach	Chapter 93H §§1-6
Disposal of records containing SSN or PII	Chapter 93I, §§1-3
Security Freeze	Chapter 93 §50, §56 & §62A
Insurance Information Privacy	Chapter 175I
Genetic Privacy	Chapter 111 §70G
SSN Restricted Use	Chapter 93H §2
Electronic Surveillance	Chapter 272 §99

Michigan

State Code: Michigan Compiled Laws
http://www.legislature.mi.gov/(S(xmsyvhxkwyagttiudwhypyaw))/mileg.aspx?page=ChapterIndex

PII /Personal Information Definition	§445.63; §37.251; §205.827; §257.40b; §500.503
Library Patron Records & e-reader Privacy	§397.603
Data (Security) Breach	§445.61; §445.63; §445.72
Disposal of records containing SSN or PII	§445.72a
Credit Card Number on Receipts	§445.903 - 3(hh)
Insurance Information Privacy	§§500.501 *et seq*
Genetic Privacy	§333.17020; §333.17520
Health Information Privacy	§550.1406
SSN Restricted Use	§§445.81 *et seq*; §565.491; §565.452; §565.581; §37.252
RFID & Privacy	§28.304
Electronic Surveillance	§750.539c
Privacy Policies: Government Web Sites	Public Act 161-572(7)

Minnesota

State Code: Minnesota Statutes
https://www.revisor.mn.gov/statutes/

PII /Personal Information Definition	§60A.98; §72A.491
Library Patron Records & e-reader Privacy	§13.40 subdivision 2
Data (Security) Breach	§325E.61; §609.891
Consumer Protection	§325D.45
Security Freeze	§§13C.016 – 019
Insurance Information Privacy	§§72A.491 – 505
Genetic Privacy	§13.386
Prescription Drug Database and/or Prescription Drug Monitoring	§152.126
SSN Restricted Use	§325E.59; §201.091, subdivision 9; §203B.17, subdivision 2; §203B.19; §203B.20; §203B.24 Subdivision 1; §47.69
RFID & Privacy	§171.07
Electronic Surveillance	§626A.02
On-line Privacy of Personal Information	§§325M.01 – .09; §47.69
Privacy Policies: Government Web Sites	§13.15

Mississippi

State Code: Mississippi Code
http://www.lexisnexis.com/hottopics/mscode/

Library Patron Records & e-reader Privacy	§ 39-3-365
Data (Security) Breach	§75-24-29
Disposal of records containing SSN or PII	§41-9-75
Security Freeze	§§75-24-201 – 215
Financial Information Privacy	§35-7-49
Health Information Privacy	§41-91-11; §41-9-67
Prescription Drug Database and/or Prescription Drug Monitoring	§73-21-127
SSN Restricted Use	§75-71-607(b)(5)
Electronic Surveillance	§§41-29-501 – 537

Missouri

State Code: Missouri Revised Statutes
http://revisor.mo.gov/main/Home.aspx

PII /Personal Information Definition	§59.331; §32.091.1(3); §407.1500.1(9)
Library Patron Records & e-reader Privacy	§182.817 §182.815
Data (Security) Breach	§407.1500
Credit Card Number on Receipts	§407.433.1
Security Freeze	§§407.1380 –1385
Financial Information Privacy	§§408.675-700; §362.422.1
Genetic Privacy	§375.1309
SSN Restricted Use	§407.1355; §610.035; §566.226.1
RFID & Privacy	§167.168
Electronic Surveillance	§542.402
On-line Privacy of Personal Information	§578.45

Montana

State Code: Montana Code Annotated
http://leg.mt.gov/bills/mca/index.html

PII /Personal Information Definition	§33-19-104(21); §61-11-503(6); §30-14-1702(7); §2-6-501(4); §2-17-551(6)
Library Patron Records & e-reader Privacy	§22-1-1103
Privacy in State Constitution	Article II, §10
Data (Security) Breach	§§30-14-1701 – 1705
Disposal of records containing SSN or PII	§30-14-1703
Credit Card Number on Receipts	§2-6-501(5)
Security Freeze	§§30-14-1726 –1735
Insurance Information Privacy	§33-19-202 *et seq*
SSN Restricted Use	§2-6-502; §32-6-306; §40-5-923
Electronic Surveillance	§45-8-213
Privacy Policies: Government Web Sites	§§2-17-550 – 553
Phishing	§30-14-1712; §33-19-410

Nebraska

State Code: Nebraska Revised Statutes
http://nebraskalegislature.gov/laws/laws.php

PII /Personal Information Definition	§44-903(22); §28-636(2)
Library Patron Records & e-reader Privacy	§84-712.05(11)
Data (Security) Breach	§§87-801 – 87-807
Consumer Protection	§87-303
Credit Card Number on Receipts	§28-633
Security Freeze	§8-2601 *et seq*
Insurance Information Privacy	§44-901 *et seq*
Genetic Privacy	§71-551
SSN Restricted Use	§48-237; §84-712.05(17)
Electronic Surveillance	§86-290
Privacy Policies on Web Sites	§87-302(14)

Nevada

State Code: Nevada Revised Statutes
http://leg.state.nv.us/law1.cfm

PII /Personal Information Definition	§603A.040; §205.4617
Library Patron Records & e-reader Privacy	§239.013
Data (Security) Breach	§603A.010 *et seq*
Disposal of records containing SSN or PII	§603A.200
Credit Card Number on Receipts	§597.945
Security Freeze	§598C.105; §§598C.300 – 598C.390
Genetic Privacy	§629.101 – §629.201
Prescription Drug Database and/or Prescription Drug Monitoring	§453.1545
SSN Restricted Use	§239B.030; §239B.050
RFID & Privacy	§§205.461 – 205.4675 §205.46515
Electronic Surveillance	§200.620
Privacy of Personal Information - Internet	§205.498
Spyware	§205.4765

New Hampshire

State Code: New Hampshire Revised Statutes
http://www.gencourt.state.nh.us/rsa/html/indexes/default.html

PII /Personal Information Definition	§638:25; §260:14(c); §359-I:1(II); §359-C:19 (IV); §7-A:1(IV)
Library Patron Records & e-reader Privacy	§201-D:11
Data (Security) Breach	§359-C:19 – 21
Student Information	§189-65 to 68
Security Freeze	§§359-B:22 – B:26
Financial Information Privacy	§§359-C:1 – 359-C:21
Genetic Privacy	§141-H:2
SSN Restricted Use	§287-D:2-c II; §382-A:9-528, §400-A:15-b
RFID & Privacy	§236-30 §189-68
Electronic Surveillance	§570-A:2
Spyware	§359-H:2

New Jersey

State Code: New Jersey Permanent Statutes
http://njlaw.rutgers.edu/collections/njstats/

PII /Personal Information Definition	§2C:20-1v; §2C:20-23l
Library Patron Records & e-reader Privacy	§18A:73-43.2
Data (Security) Breach	§56:8-161 – 163
Disposal of records containing SSN or PII	§56.8-161 & 162
Consumer Protection	§30:4G-16.1
Credit Card Number on Receipts	§56:11-42
Security Freeze	§56:11-30, §§56:11-44 – 11-50
Genetic Privacy	§§10:5-43 – 10:5-49
Health Information Privacy	§26:2H-12.8g
Prescription Drug Database and/or Prescription Drug Monitoring	§45:1-45
SSN Restricted Use	§56:8-164; §47:1-16; §18A:3-28
Electronic Surveillance	§2A:156A-1 *et seq*

\

New Mexico

State Code: New Mexico Statutes Annotated
http://public.nmcompcomm.us/nmnxtadmin/NMPublic.aspx

PII /Personal Information Definition	§30-16-24.1(2)
Library Patron Records & e-reader Privacy	§18-9-1 *et seq*
Consumer Protection	§57-12-10
Credit Card Number on Receipts	§56-4-3.1
Security Freeze	§§56-3A-1 – 56-3A-6
Insurance Information Privacy	§§59A-17A-1 *et seq*
Genetic Privacy	§40-11A-511
Health Information Privacy	§§24-14B-1 *et seq*
SSN Restricted Use	§1-4-5; §1-12-7.1; §57-12B-3 & 4; §13-7-6
Electronic Surveillance	§30-12-1

New York

State Code: Laws of New York
http://codes.findlaw.com/ny/

PII /Personal Information Definition	Penal Law §190.77; General Business Law §399-H-d; General Business Law §899-AAA; Public Officers Law §92; State Technology Law §202;
Personal Privacy	Public Officers Law §§91 – 99
Library Patron Records & e-reader Privacy	Civil Practice Law and Rules §4509
Data (Security) Breach	Tech Law §208; General Business Law §899-aa
Disposal of records containing SSN or PII	Banking Law §9-j; General Business Law §399-H
Consumer Protection	Business Corporation Law §349
Credit Card Number on Receipts	General Business Law §520-A (4-a.a)
Security Freeze	General Business Law 380-t
Genetic Privacy	Public Health Law §2733; Civil Rights Law §79-L
SSN Restricted Use	General Business Law §399-dd; Public Officers Law §96-a; Labor Law §203-d; Education Law §2-B
Electronic Surveillance	Penal Law §§250.00 – 250.05
Privacy Policies: Government Web Sites	Technical Law §§201 – 207
Phishing	Business Law §390-b

North Carolina

State Code: North Carolina General Statutes
http://www.ncleg.net/gascripts/Statutes/StatutesTOC.pl

PII /Personal Information Definition	§75-61(10); §75-66
Personal Privacy	§75-66 (Publication of personal information); §143B-981 (criminal history records); §131E-257.2 (personnel records - public hospitals); §132-1.2 (confidential information)
Library Patron Records & e-reader Privacy	§125-19
Data (Security) Breach	§§75-60 & 65; §132-1.10
Disposal of records containing SSN or PII	§75-64
SSN Restricted Use	§75-61 & 62; §132-1.10
Identity Theft (PPI definition)	§14-113.20
Credit Card Number on Receipts	§14-113.24
Security Freeze	§75-63
Financial Information Privacy	§53B *et seq*
Insurance Information Privacy	§§58-39-1 et seq
Genetic Privacy	§130A-131.16; §15A-266.12
Health Information Privacy	§130A-12; §130A-15; §132-1.23 (Eugenics)
Prescription Drug Database and/or Prescription Drug Monitoring	§§90-113.70 et seq
Electronic Surveillance	§§15A-286 et seq; §14-155
Data Sharing	§143B-426.38A
Interception of Electronic Communications	§§14-454 et seq

North Dakota

State Code: North Dakota Century Code
http://www.legis.nd.gov/general-information/north-dakota-century-code

PII /Personal Information Definition	§44-04-18.17, §44-04-18.7(6)
Data (Security) Breach	§§51-30-01 – 51-30-07
Credit Card Number on Receipts	§51-07-27
Security Freeze	§§ 55-33-01 – 55-33-14
Financial Information Privacy	§§13-02-21-01 – 13-02-21-04; §§6-08.1-01 – 6-08.1-10
Insurance Information Privacy	§26.1-02-27
Health Information Privacy	§23-01.3-01 *et seq*
Prescription Drug Database and/or Prescription Drug Monitoring	§19-03.5-01 *et seq*
SSN Restricted Use	§44-04-28
RFID & Privacy	§12.1-15-06
Electronic Surveillance	§12.1-15-02

Ohio

State Code: Ohio Revised Code
http://codes.ohio.gov/orc/

PII /Personal Information Definition	§125.18; §149.45; §317.082; §1347.01(E)
Library Patron Records & e-reader Privacy	§149.432
Data (Security) Breach	§1347.12; §1349.19; §§1349.191 – 1349.192
Security Freeze	§§1349.52 – .53
Insurance Information Privacy	§1349.51
Prescription Drug Database and/or Prescription Drug Monitoring	§§4729.75 – 4729.84
SSN Restricted Use	§4503.102; §111.241; §149.45; §317.082
Electronic Surveillance	§2933.52
Privacy of Personal Information - Internet	§149.45

Oklahoma

State Code: Oklahoma Statutes Citationized
http://www.oscn.net/applications/oscn/index.asp?ftdb=STOKST&level=1

PII /Personal Information Definition	Title 24 §162; Title 47 §1109
Data (Security) Breach	Title 24 §§161 – 166; Title 74 §3113.1
Student Information	Title 10 §3-168
Consumer Protection	Title 78 §54
Security Freeze	Title 24 §§150 – 159
Financial Information Privacy	Title 6 §§2201 – 2208
Insurance Information Privacy	Title 36 §307.2
SSN Restricted Use	Title 40 §173.1; Title 74 §3111; Title 74 §3113
RFID & Privacy	Title 63 §1-1430
Electronic Surveillance	Title 13 §§176.2 *et seq*.
Phishing	Title 15 §§776.9 & 12

Oregon

State Code: Oregon Revised Statutes
https://www.oregonlegislature.gov/bills_laws/Pages/ORS.aspx

PII /Personal Information Definition	§746.600(32); §802.175(3); §646A.602(11)
Data (Security) Breach	§§646A.602 & .604
Disposal of records containing SSN or PII	§646A.622
RFID & Privacy	§339.890
Credit Card Number on Receipts	§646.899
Security Freeze	§646A.602; §646A.606; §646A.618
Financial Information Privacy	§§192.550 – .595
Insurance Information Privacy	§§746.600 – 690
Genetic Privacy	§§192.531 – 549
Health Information Privacy	§§192.518 – .529
Prescription Drug Database and/or Prescription Drug Monitoring	§431.96 *et seq*
SSN Restricted Use	§802.195; §§326.587 & .589; §646A.620; §107.840
Electronic Surveillance	§165.540, §165.543; §133.005

Pennsylvania

State Code: Pennsylvania Consolidated Statutes Annotated
http://www.legis.state.pa.us/cfdocs/legis/CH/Public/pcde_index.cfm

PII /Personal Information Definition	Title 73 §2302; Title 18 §4120
Library Patron Records & e-reader Privacy	Title 65 §67.708(b)(23)
Data (Security) Breach	Title 73 §§2301– 2308
Security Freeze	Title 73 §§2501– 2509
Insurance Information Privacy	Title 40 §310.77a
SSN Restricted Use	Title 74 §§201– 204; Title 71 §§2601– 2607
Electronic Surveillance	Title 18 §§5701 *et seq*
Privacy Policies on Web Sites	Title 18 §4107(a)(10)

Rhode Island

State Code: Rhode Island General Laws
http://webserver.rilin.state.ri.us/Statutes/Statutes.html

PII /Personal Information Definition	§11-49.2-5
Library Patron Records & e-reader Privacy	§11-18-32
Data (Security) Breach	§§11-49.2-1 – 11-49.2-9
Disposal of records containing SSN or PII	§6-52-2
RFID & Privacy	§42-153-1 to 4
Credit Card Number on Receipts	§6-30-6
Security Freeze	§§6-48-2 – 48-9
Genetic Privacy	§27-18-52 & 52.3; §27-19-44 & 44.1; §27-20-39 & 39.1; §27-41-53 & 53.1
SSN Restricted Use	§6-48-8; §§6-13-15 *et seq*
Electronic Surveillance	§11-35-21; §12-5.1
Spyware	§11-52.2

South Carolina

State Code: South Carolina Code Of Laws
http://www.scstatehouse.gov/code/statmast.php

PII /Personal Information Definition	§30-2-30; §16-13-510(D)
Personal Information Privacy	§§30-2-10 *et seq*
Library Patron Records & e-reader Privacy	§60-4-10
Privacy in State Constitution	Article I, §10
Data (Security) Breach	§1-11-490; §39-1-90
Disposal of records containing SSN or PII	§37-20-190; §30-2-310
Credit Card Number on Receipts	§16-13-512
Security Freeze	§37-20-160
Financial Information Privacy	§§16-13-500 *et seq*
Genetic Privacy	§§38-93-10 – 60
Prescription Drug Database and/or Prescription Drug Monitoring	§§44-53-1640 – 44-53-1680
SSN Restricted Use	§37-20-180; §16-13-512; §§30-2-310 – 340
Electronic Surveillance	§17-30-20
Privacy Policies: Government Web Sites	§§30-2-40

South Dakota

State Code: South Dakota Codified Laws
http://sdlegislature.gov/statutes/Codified_Laws/

PII /Personal Information Definition	§22-40-9; §22-30A-3.2; §32-5-143(6)
Library Patron Records & e-reader Privacy	§14-2-51
Security Freeze	§§54-15-1 – 15-16
Genetic Privacy	§34-14-22
SSN Restricted Use	§32-12-17.10; §32-12-17.13; §12-4-2; §1-27-44; §32-12A-20.1; §1-8-5; §32-5-144; §15-15A-9; §47-31B-607; §1-27-1.5
Electronic Surveillance	§23A-35A-20

Tennessee

State Code: Tennessee Code
http://www.lexisnexis.com/hottopics/tncode/

PII /Personal Information Definition	§47-18-2107(3)(A); §§10-7-504(15)(A) & (16)(A); §39-14-150(g)(2)
Library Patron Records & e-reader Privacy	§§10-8-101 – 103
Data (Security) Breach	§47-18-2107
Disposal of records containing SSN or PII	§10-7-504(b); §39-14-150(g)(1)
Consumer Protection	§§47-18-101 – 130
Credit Card Number on Receipts	§47-18-126
Security Freeze	§§47-18-2108 – 2109
Financial Information Privacy	§§45-10-101 – 118
Genetic Privacy	§§56-7-2701 & 2708
Health Information Privacy	§8-25-109; §8-25-307; §8-25-502; §8-36-510; §10-7-504
Prescription Drug Database and/or Prescription Drug Monitoring	§§53-10-304 – 310
SSN Restricted Use	§47-18-2110; §2-2-124
Electronic Surveillance	§10-7-512
Employee E-mail Communications and Internet Access	§31-48d
Phishing	§§47-18-5201 – 5205

Texas

State Code: Texas Statutes
http://texreg.sos.state.tx.us/public/readtac$ext.viewtac

PII /Personal Information Definition	Business & Commerce Code
Library Patron Records & e-reader Privacy	Government Code §552.124
Data (Security) Breach	Business & Commerce Code §48.002; §§48.101 – 103;
Disposal of records containing SSN or PII	Business & Commerce Code §521.052(b) §72.004
Credit Card Number on Receipts	Business & Commerce Code
Security Freeze	Business & Commerce Code §§20.034 –
Genetic Privacy	Insurance Code §546.001 *et seq*
Health Information Privacy	Health & Safety Code §181.152
SSN Restricted Use	Business & Commerce Code §§501.001 & .002; §§501.051 – 501.053;
RFID & Privacy	Transportation Code §521.032 (c)
Electronic Surveillance	Penal Code §16.02
Privacy Policies: Government Web Sites	Government Code §10- 2054.126
Spyware	Business & Commerce Code
Phishing	Business and Commerce Code §48.001;

Utah

State Code: Utah Code
https://le.utah.gov/Documents/code_const.htm

PII /Personal Information Definition	§13-44-102(3)(a); §13-45-102(5)
Personal Information Privacy	§§30-2-10 *et seq*
Library Patron Records & e-reader Privacy	§13-37-101, 102, 201 to 203
Data (Security) Breach	§§13-44-101, 201-202, 301
Disposal of records containing SSN or PII	§13-44-201
RFID & Privacy	§77-23a-4.5
Credit Card Number on Receipts	§13-38-101
Security Freeze	§13-45-201 – 205
Financial Information Privacy	§7-1-1001 – 1007
Genetic Privacy	§§26-45-101 – 106
Prescription Drug Database and/or Prescription Drug Monitoring	§§58-37-7.5 – 58-37-7.8
SSN Restricted Use	§31A-21-110; §63D-2-103; §13-45-301(1)
Electronic Surveillance	§77-23a-4
Data Sharing	§§13-37-101 & 102, 201 – 203
Privacy Policies: Government Web Sites	§§63D-2-101 – 104
Spyware	§13-40-201

Vermont

State Code: Vermont Statutes
http://legislature.vermont.gov/statutes/

PII /Personal Information Definition	Title 9 §2430(5)(A); §2445(a)(3); Title 13 §2030(c)
Library Patron Records & e-reader Privacy	Title 22 §172
Data (Security) Breach	Title 9 §§2430, 2435, 2440, 2445
Disposal of records containing SSN or PII	Title 9 §2445(b)
Consumer Protection	Title 8 §§10201 – 10205
Security Freeze	Title 9 §§2480a – 2480j
Genetic Privacy	Title 18 §§9331 – 9335
Prescription Drug Database and/or Prescription Drug Monitoring	Title 18 §§4281 – 4287
SSN Restricted Use	Title 9 §2440, §2480m
RFID & Privacy	Title 23 §§7 & 8

Virginia

State Code: Code of Virginia
http://leg1.state.va.us/000/src.htm

PII /Personal Information Definition	§2.2-3801; §18.2-186.3, §38.2-602, §12.1-19, § 40.1-28.7:4, §46.2-208, §19.2-263.3, §46.2-2099.53, § 15.2-968.1, §55-370.01;
Personal Information Privacy	§2.2-3800 *et seq §2.2-3800 et seq, §33.2-504, §20-88.94, §12.1-19, §§59.1-442 thru 444, §32.1-283.4, § 2.2-614.2*
Library Patron Records & e-reader Privacy	§2.2-3705.7(3)
Data (Security) Breach	§18-2-186.6 §18.2-186.6 (data breach); §32.1-127.1:05; §22.1-253.13:3; §22.1-20.2.
Disposal of records containing SSN or PII	§42.1-86.1; §6.2-2008
SSN Restricted Use	§59.1-443.2; §2.2-3815; §24.2-1002.1, § 32.1-267, § 24.2-407.1, §59.1-443.2, § 17.1-227; §2.2-3705.4; §§2.2-3801,2.2-3808, & 2.2-3809;§16.1-77; §24.2-416.5
RFID & Privacy	§ 46.2-323.01
Student Information	§22.1-79.3, §22.1-289.01, §23-2.1:3, §22.1-79.3, §2.2-3705.1
Consumer Information	§59.1-196 et seq
Credit Card Number on Receipts	§6.2-429
Security Freeze	§§59.1-444.1 - .3
Financial Information Privacy	§6.2-1720, §3.2-3111, §58.1-3, §6.2-101; § 32.1-325.001; §58.1-1845, §6.2-2008
Insurance Information Privacy	§§38.2-600 et al, § 38.2-2126
Genetic Privacy	§38.2-508.4; §32.1-67.1, § 19.2-310.5
Health Information Privacy	§32.1-127.1:03, §32.1-127.1:05, §32.1-71.02

Prescription Drug Database and/or Prescription Drug Monitoring	§54.1-2519 et seq
Electronic Surveillance	§19.2-62
Data Sharing	§32.1-71
Privacy of Personal Information - Internet	§18.2-186.4:1; §18.2-152.5; §17.1-293
Privacy Policies: Government Web Sites	§2.2-3800 to 3803(B)
Interception of Electronic Communications	§19.2-61 & 62
Spyware	§18.2-152.4

Washington

State Code: Revised Code of Washington
http://apps.leg.wa.gov/rcw/

PII /Personal Information Definition	§19.215.010; §19.270.010; §19.190.010; §43.06A.070
Library Patron Records & e-reader Privacy	§42.56.310
Privacy in State Constitution	Article I, §7
Data (Security) Breach	§19.255.010
Disposal of records containing SSN or PII	§§19.215.005 – 215.030; §434-640-020
Credit Card Number on Receipts	§19.200.010; §63.14.123
Security Freeze	§§19.182.170 – 182.200
Financial Information Privacy	§284-04
Insurance Information Privacy	§48.102.051; §71.05.385; §48.43.021; §48.43.505
Genetic Privacy	§70.02.010
Health Information Privacy	§284-04
Prescription Drug Database and/or Prescription Drug Monitoring	§70.225.010 *et seq*
SSN Restricted Use	§28B.10.042; §48.43.022; §74.09.037; §65.04.045(3); §43.06A.070; §26.26.041; §26.23.150; §26.23.140
RFID & Privacy	§ 9A.58.020; §§42.56.230(5) & .330(8); §§19.300.010 & .020 §46.20.202
Electronic Surveillance	§9.73.030
Spyware	§19.270.030

West Virginia

State Code: West Virginia Code
http://www.legis.state.wv.us/WVCODE/Code.cfm

PII /Personal Information Definition	§5A-8-22; §17A-2A-3(f); §46A-2A-101(6); §11-15B-28
Library Patron Records & e-reader Privacy	§10-1-22
Data (Security) Breach	§§46A-2A-101 *et seq*
Security Freeze	§§46A-6L-103 & 104
Genetic Privacy	§15-2B-6(h)
SSN Restricted Use	§16-5-3; §16-5-22; §16-5-27; §16-5-33; §5A-8-21
Electronic Surveillance	§62-1D-3

Wisconsin

State Code: Wisconsin Statutes & Annotations
http://docs.legis.wisconsin.gov/statutes/prefaces/toc

PII /Personal Information Definition	§23.45(1)[c]; §85.103(1); §134.98(1)(b); §440.14(1)(b); §943.201(1)(b)
Library Patron Records & e-reader Privacy	§43.3
Data (Security) Breach	§895.507
Disposal of records containing SSN or PII	§134.97
Credit Card Number on Receipts	§134.74(2)
Security Freeze	§§100.54(1) – .54(13)
Genetic Privacy	§942.07
Health Information Privacy	§146.82
SSN Restricted Use	§36.32; §301.029(2)(a); §551.607(2)(e)
RFID & Privacy	§146.25
Electronic Surveillance	§968.31

Wyoming

State Code: Wyoming Statutes
http://www.lexisnexis.com/hottopics/wystatutes/

PII /Personal Information Definition	§40-12-501(a)(vii); §6-3-901(b)
Library Patron Records & e-reader Privacy	§16-4-203(d)(ix)
Data (Security) Breach	§§40-12-501 – 502
Credit Card Number on Receipts	§40-12-501(a)(viii)
Security Freeze	§§40-12-501, 503 – 509
Genetic Privacy	§§14-2-701– 710
Health Information Privacy	§§35-2-605 – 617
Prescription Drug Database and/or Prescription Drug Monitoring	§§35-7-1060 – 1062
SSN Restricted Use	§6-3-901
Electronic Surveillance	§7-3-701

APPENDIX A – Resources

Resources for State Laws and Privacy

Publications

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.

Privacy Law, Charlene Brownlee and Blaze D. Waleski, Law Journal Press, New York, 2016 (Originally published: 2006).

Information Security Law: Control of Digital Assets (Release 4 updates through 09/2009), Mark G. Milone, Law Journal Press, New York.

Federal Privacy Law Compendium, Stuart McKee and Lester Nakamura, NASCIO, April 2003. https://www.nascio.org/Publications/ArtMID/485/ArticleID/264/Federal-Privacy-Law-Compendium-Version-10

Web Sites

Requirements for Personal Information Protection – Part 1: U.S. Federal Law, Revised 2017 http://www.armaedfoundation.org/

Morrison & Foerster International Data Privacy – United States http://www.mofoprivacy.com/default.aspx

National Council of State Legislatures: Issues and Research http://www.ncsl.org/research/about-state-legislatures.aspx

Legal Information Institute – Cornell University Law School http://www.law.cornell.edu/states/listing.html

Privacy Rights Clearinghouse http://www.privacyrights.org/

Identity Theft Resource Center http://www.idtheftcenter.org/

State Government: USA.gov (Access to web sites for all 50 states and the District of Columbia.) The link to codified laws for each state can usually found on the "Government" portal or the "Legislature" portal of the web site. http://www.usa.gov/Agencies/State_and_Territories.shtml

APPENDIX B – State Law Table

Because of the size of this table, it is not possible to publish it as part of this document. However, this table is available for download in an Excel or PDF format.

To retrieve this file, view this page on a computer with active Internet access and click one of the following links to download the State Law Table PDF file to your computer hard drive.

Excel version: http://armaedfoundation.org/wp-content/uploads/2017/09/170601-US_State_Privacy_Laws_Appendix_B.xlsx

PDF version: http://armaedfoundation.org/wp-content/uploads/2017/09/170601-US_State_Privacy_Laws_Appendix_B.pdf

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