Survey of Indiana Cyber Laws

Title or Description	Standard Type	Reference	Synopsis	Penalty	Statute of Limitations	Enforcement	2019 Update
Definition of Personal Information	State	IC §24-4.9-2-10	"Personal information" means: (1) a Social Security number that is not encrypted or redacted; or (2) an individual's first and last names, or first initial and last name, and one (1) or more of the following data elements that are not encrypted or redacted: (A) A driver's license number. (B) A state identification card number. (C) A credit card number. (D) A financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account. The term does not include information that is lawfully obtained from publicly available information or from federal, state, or local government records lawfully made available to the general public.	NA	NA	NA	
House Enrolled Act No. 1294 - INSPECT Program	State	H.E.A. 1294 (2019) P.L. 51-2019 (Adds Chapter 24 "Central Repository for Controlled Substances Data" Under Indiana Code Title 25, Article 26).	The bill requires prescribers to have access to and utilize INSPECT, a state-sponsored website database that allows practitioners to check a patient's controlled substance prescription history. *See* IC § 25-26-24-19(k).	"A person who knowingly or intentionally releases confidential information in an unauthorized manner violates this chapter and commits a Class A misdemeanor" IC § 25-26-24-25.	Undefined by statute.	Undefined by statute.	Removed the information regarding Senate Bill 211 (2018) and replaced with information regarding H.E.A. 1294 (2019) which repealed and replaced the legislation created by SB 211 (2019)
Telephone Solicitation of Consumers ("Do Not Call Law")	State	Ind. Code art. 24-4.7 (See Ind. Code § 24-4.7-4, et seq.)	"A telephone solicitor may not make or cause to be made a telephone sales call to a telephone number if that telephone number appears in the most current quarterly listing published by the division." Ind. Code § 24-4.7-4-1.	An injunction to enjoin future violations; $10,000 for the first call; $25,000 for subsequent calls; all money the defendant obtained through their violation of this law; the attorney general's reasonable costs in investigation of the deceptive act and maintaining the action; reasonable attorney's fees; costs of the action. Ind. Code § 24-4.7-5-2(a).	2 years after the call is made. Ind. Code § 24-4.7-5-4.	Attorney General. Ind. Code § 24-4.7-5-1.	

Survey of Indiana Cyber Laws

Title or Description	Standard Type	Reference	Synopsis	Penalty	Statute of Limitations	Enforcement	2019 Update
Do Not Text Law	State	Ind. Code art. 24-4.7	"A telephone solicitor may not make or cause to be made a telephone sales call to a telephone number if that telephone number appears in the most current quarterly listing published by the division." Ind. Code § 24-4.7-4-1. A Telephone sales call can be defined as the "transmission of: a text message . . ." Ind. Code § 24-4.7-2-9(b)	An injunction to enjoin future violations; $10,000 for the first call; $25,000 for subsequent calls; all money the defendant obtained through their violation of this law; the attorney general's reasonable costs in investigation of the deceptive act and maintaining the action; reasonable attorney's fees; costs of the action. Ind. Code § 24-4.7-5-2(a).	2 years after the text is made. Ind. Code § 24-4.7-5-4.	Attorney General. Ind. Code § 24-4.7-5-1.	
Prohibited Spyware	State	Ind. Code art. 24-4.8	"A person who is not the owner or operator of the computer may not knowingly or intentionally: (1) transmit computer software to the computer; and (2) by means of the computer software transmitted under subdivision (1), do any of the following: (A) use intentionally deceptive means to modify computer settings...(B)Use intentionally deceptive means to collect personally identifying information...(C) Extract the hard drive of an owner or operator's computer...(D) Use intentionally deceptive means to prevent reasonable efforts by an owner or operator to block or disable the installation or execution of computer software...(E) Knowingly or intentionally misrepresent that computer software will be uninstalled or disabled...(F) Use intentionally deceptive means to remove, disable, or otherwise make inoperative security, antispyware, or antivirus computer software installed on the computer...(G) Take control of another person's computer with the intent to cause damage to the computer or cause the owner to incur a financial charge for a service that the owner or operator has not authorized...(I) Prevent reasonable efforts by an owner or operator to block or disable the installation or execution of computer software..." Ind. Code § 24-4.8-2-2.	Enjoin further violations; to recover the greater of either damages or $100,000. Ind. Code § 24-4.8-3-1.	Undefined by statute.	Private right of action. Ind. Code § 24-4.8-3-1.	Increased the synopsis to include the specific deceptive actions which can be committed.
Disclosure of Security Breach Act	State	Ind. Code art. 24-4.9	After a data security breach involving "personal information," a "data base owner" may need to alert (1) affected Indiana residents, (2) the attorney general, (3) consumer reporting agencies (if over 1,000 consumers effected), and (4) the data base owner (if the breached party is not the data base owner). Must notify without unreasonable delay (likely within 30 days of the breach discovery). Ind. Code § 24-4.9-3-1; Ind. Code § 24-4.9.-3-2; Ind. Code § 24-4.9-3-3.	An injunction to enjoin future violations; $150,000 per deceptive act; the attorney general's reasonable costs Ind. Code § 24-4.9.-4-2.	Likely 2 years from notification of Attorney General. Undefined by the statute.	Attorney General. Ind. Code § 24-4.9-4-2	
Protection of Personal Information	State	Ind. Code § 24-4.9-3-3.5c	"A data base owner shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect and safeguard from unlawful use or disclosure any personal information of Indiana residents collected or maintained by the data base owner... A person that knowingly or intentionally fails to comply with any provision of this section commits a deceptive act . . ." Ind. Code § 24-4.9-3-3.5(c), (e).	An injunction to enjoin further violations; $5,000 per deceptive act; and the attorney general's reasonable costs. Ind. Code § 24-4.9-3-3.5(f).	Likely 2 years from notification of Attorney General. Undefined by the statute.	Attorney General. Ind. Code § 24-4.9-3-3.5(f)	

Survey of Indiana Cyber Laws

Title or Description	Standard Type	Reference	Synopsis	Penalty	Statute of Limitations	Enforcement	2019 Update
Disposal of Personal Information	State	Ind. Code § 24-4.9-3-3.5(d)	"A data base owner shall not dispose of or abandon records or documents containing unencrypted and unredacted personal information of Indiana residents without shredding, incinerating, mutilating, erasing, or otherwise rendering the personal information illegible or unusable ... A person that knowingly or intentionally fails to comply with any provision of this section commits a deceptive act . . ." Ind. Code § 24-4.9-3-3.5(d)-(e).	An injunction to enjoin further violations; $5,000 per deceptive act; and the attorney general's reasonable costs. Ind. Code § 24-4.9-3-3.5(f).	Likely 2 years from notification of Attorney General. Undefined by the statute.	Attorney General. Ind. Code § 24-4.9-3-3.5(f)	
Disposal of Personal Information	State	Ind. Code § 24-4-14-8	"A person who disposes of the unencrypted, unredacted personal information of a customer without shredding, incinerating, mutilating, erasing, or otherwise rendering the information illegible or unusable commits a Class C infraction. However, the offense is a Class A infraction if: (1) the person violates this section by disposing of unencrypted, unredacted personal information of more than one hundred customers; or (2) the person has prior unrelated judgement for a violation of this section." Ind. Code § 24-4-14-8	Class C or Class A infraction. Ind. Code § 24-4-14-8.	2 years. Ind. Code § 34-28-5-1(c)(2)	Prosecuting Attorney. Ind. Code § 34-28-5-1	Added additional information to the synopsis.
Disposal of Electronic Waste	State	Ind. Code § 13-20.5-10-1	Covered entities cannot dispose of covered electronic devices in a landfill or through incineration. Ind. Code § 13-20.5-10-1	None. Ind. Code § 13-20.5-10-2	N/A	N/A	
Deceptive Consumer Sales Act	State	Ind. Code § 24-5-0.5	"A supplier may not commit an unfair, abusive, or deceptive act, omission, or practice in connection with a consumer transaction. Such an act, omission, or practice by a supplier is a violation of this chapter whether it occurs before, during, or after the transaction. An act, omission, or practice prohibited by this section includes both implicit and explicit misrepresentations." Ind. Code § 24-5-0.5-3(a).	$5,000 per knowingly deceptive act. IC § 24-5-0.5-4(g). The court may also (1) issue an injunction; (2) order the supplier to make payment of the money unlawfully received from the aggrieved consumers to be held in escrow for distribution to aggrieved consumers...(4)order the supplier to pay to the state the reasonable costs of the attorney general's investigation and prosecution related to the action. Ind. Code 24-5-0.5-4(c).	2 years after the occurrence of the deceptive act. Ind. Code § 24-5-0.5-5(b).	Private Right of action and Attorney General. Ind. Code § 24-5-0.5-4(a),(c).	

Survey of Indiana Cyber Laws

Title or Description	Standard Type	Reference	Synopsis	Penalty	Statute of Limitations	Enforcement	2019 Update
Regulation of Automatic Dialing Machines	State	Ind. Code § 24-5-14	Indiana's Auto Dialer law prohibits most prerecorded calls, commonly known as "robo-calls," made via an automatic dialing-announcing device ("ADAD") regardless of the subject matter of the message. Ind. Code § 24-5-14-5(b).	$10,000 for the first violation, $25,000 for each violation after the first violation. IC §24-5-14-13. The court may also (1) issue an injunction; (2) order the supplier to make payment of the money unlawfully received from the aggrieved consumers to be held in escrow for distribution to aggrieved consumers...(4)order the supplier to pay to the state the reasonable costs of the attorney general's investigation and prosecution related to the action. Ind. Code 24-5-0.5-4(c)."	2 years after the occurrence of the deceptive act. Ind. Code § 24-5-0.5-5.	Attorney General. Ind. Code § 24-5-14-13.	
Do Not Fax Law	State	Ind. Code § 24-5-0.5-3(b)(19).	Prohibition on sending unsolicited facsimile ("fax") advertisements . The law applies to advertisements sent to residential and business fax numbers. Unlike the Do Not Call law, the Do Not Fax law does not require people to register their fax numbers.	$5,000 per knowingly deceptive act. Ind. Code § 24-5-0.5-4(g)	2 years after the occurrence of the deceptive act. Ind. Code § 24-5-0.5-5.	Attorney General. Ind. Code § 24-5-14-13.	
Deceptive Commercial Electronic Mail	State	Ind. Code § 24-5-22	Prohibition on sending unsolicited commercial electronic mail, when failing to comply with statutory sending standards. Ind. Code § 24-5-22-8.	Damages or $500 per email. Ind. Code § 24-5-22-10(d)(2).	Undefined by statute.	Private right of action. Ind. Code § 24-5-22-10(a).	
Health Records and Identifying Information Protection	State	Ind. Code § 4-6-14	Provision relates to the Indiana Attorney General's responsibility related to abandoned health records and other records that contain personal information.	NA	NA	NA	
Notice of Security Breach Act for State Agencies	State	Ind. Code Ch. 4-1-11	"Any state agency that owns or licenses computerized data that includes personal information shall disclose a breach of the security of the system following discovery or notification of the breach to any state resident whose unencrypted personal information was or is reasonably believed to have been acquired by an unauthorized person." Ind. Code § 4-1-11-5.	NA	NA	NA	
Release of Social Security Numbers by State Agencies	State	Ind. Code § 4-1-10, et seq.	Details the scope of permissible disclosures of Social Security numbers as well as the consequences for violations of the statute.	Level 6 felony. Ind. Code § 4-1-10-8. Class A infraction. Ind. Code § 4-1-10-10.	Undefined by statute.	Attorney General. Ind. Code §§ 4-1-10-11; 4-1-10-12.	
Release of Social Security Numbers by State Agencies, Notice to Attorney General: Rules	Rule	10 Ind. Admin. Code § 5-4-1	"When a state agency becomes aware of a release of Social Security numbers or other personal identifying information, the state agency or employee shall, within two (2) business days of the disclosure, notify the office of attorney general for the state in writing . . ."	NA	NA	NA	

Survey of Indiana Cyber Laws

Title or Description	Standard Type	Reference	Synopsis	Penalty	Statute of Limitations	Enforcement	2019 Update
Driver's Privacy Protection Act ("DPPA")	State	Ind. Code § 9-14-13-2	Prohibits the disclosure of personal information associated with motor vehicle records by the Indiana Bureau of Motor Vehicles.	Class C misdemeanor. Ind. Code § 9-14-13-11	2 years. Ind. Code § 34-28-5-1(c)(2)	Prosecuting Attorney. Ind. Code § 33-39-1-5	
Criminal Law - Wiretap Statute	State	Ind. Code § 35-33.5	Provision outlines the requirements for the state to obtain a warrant to intercept the telephonic or telegraphic communications of an individual.	Suppression of Evidence. Ind. Code § 35-33.5-4-4.	NA	NA	
Rights of Victims of Identity Deception: Civil	State	Ind. Code § 24-5-26-2	Provision outlines the duties of those that conduct trade or commerce concerning the protections for victims of identity theft.	Recover damages actually suffered as a consumer as a result of the deceptive act or $500, whichever is greater. Ind. Code § 24-5-26-3	2 years from the mistreatment date. Ind. Code § 24-5-26-3	Attorney General. Ind. Code § 24-5-26-3	
Rights of Victims of Identity Deception: Criminal	State	Ind. Code § 35-40-14	Provision outlines the duty of law enforcement agencies concerning identity theft and the protections for victims of identity theft.	NA	NA	NA	
Criminal Law - Offense Against Intellectual Property	State	Ind. Code § 35-43-1-7	A person who knowingly or intentionally and who without authorization: (1) modifies data, a computer program, or supporting documentation; (2) destroys data, a computer program, or supporting documentation; or (3) discloses or takes data, a computer program, or supporting documentation that is: (A) a trade secret (as defined in IC 24-2-3-2); or (B) otherwise confidential as provided by law; and that resides or exists internally or externally on a computer, computer system, or computer network, commits an offense against intellectual property, a Level 6 felony.	Level 6 Felony. Ind. Code § 35-50-2-7	5 years. Ind. Code § 35-41-4-2(a)(1)	Prosecuting Attorney. Ind. Code § 33-39-1-5	
Criminal Law - Offense Against Computer Users	State	Ind. Code § 35-43-1-8	(a) A person who knowingly or intentionally and who without authorization: (1) disrupts, denies, or causes the disruption or denial of computer system services to an authorized user of the computer system services that are: (A) owned by; (B) under contract to; or (C) operated for, on behalf of, or in conjunction with; another person in whole or part; (2) destroys, takes, or damages equipment or supplies used or intended to be used in a computer, computer system, or computer network; (3) destroys or damages a computer, computer system, or computer network; or (4) introduces a computer contaminant into a computer, computer system, or computer network; commits an offense against computer users, a Level 6 felony. (b) However, the offense is: (1) a Level 5 felony if: (A) the pecuniary loss caused by the offense is at least seven hundred fifty dollars ($750) but less than fifty thousand dollars ($50,000); (B) the offense was committed for the purpose of devising or executing any scheme or artifice to defraud or obtain property; or (C) the offense interrupts or impairs: (i) a governmental operation; or (ii) the public communication, transportation, or supply of water, gas, or another public service; and (2) a Level 4 felony if: (A) the pecuniary loss caused by the offense is at least fifty thousand dollars ($50,000); or (B) the offense endangers human life.	Level 6 Felony. Ind. Code § 35-50-2-7	5 years. Ind. Code § 35-41-4-2(a)(1)	Prosecuting Attorney. Ind. Code § 33-39-1-5	

Survey of Indiana Cyber Laws

Title or Description	Standard Type	Reference	Synopsis	Penalty	Statute of Limitations	Enforcement	2019 Update
Criminal Law - Identity Deception	State	Ind. Code § 35-43-5-3.5	(a) Except as provided in subsection (c), a person who knowingly or intentionally obtains, possesses, transfers, or uses the identifying information of another person, including the identifying information of a person who is deceased: (1) without the other person's consent; and (2) with intent to: (A) harm or defraud another person; (B) assume another person's identity; or (C) profess to be another person; commits identity deception, a Level 6 felony.	Level 6 Felony. Ind. Code § 35-50-2-7	5 years. Ind. Code § 35-41-4-2(a)(1)	Prosecuting Attorney. Ind. Code § 33-39-1-5	
Criminal Law - Synthetic Identity Deception	State	Ind. Code § 35-43-5-3.8	(a) A person who knowingly or intentionally obtains, possesses, transfers, or uses the synthetic identifying information: (1) with intent to harm or defraud another person; (2) with intent to assume another person's identity; or (3) with intent to profess to be another person; commits synthetic identity deception, a Level 6 felony.	Level 6 Felony. Ind. Code § 35-50-2-7	5 years. Ind. Code § 35-41-4-2(a)(1)	Prosecuting Attorney. Ind. Code § 33-39-1-5	
Criminal Law - Fraud	State	Ind. Code § 35-43-5-4	Encompasses different types of fraud including obtaining property by use of another's credit card unlawfully.	NA	5 years. IC § 35-41-4-2(a)(1)	Prosecuting Attorney. Ind. Code § 33-39-1-5	
Criminal Law - Unlawful Possession of a Card Skimming Device	State	Ind. Code § 35-43-5-4.3	A person who possesses a card skimming device with intent to commit: (1) identity deception (IC 35-43-5-3.5); (2) synthetic identity deception (IC 35-43-5-3.8); (3) fraud (IC 35-43-5-4); or commits unlawful possession of a card skimming device. Unlawful possession of a card skimming device under subdivision (1), (2), or (3) is a Level 6 felony. Unlawful possession of a card skimming device under subdivision (4) is a Level 5 felony.	Level 5 Felony. Ind. Code § 35-50-2-6	5 years. Ind. Code § 35-41-4-2(a)(1)	Prosecuting Attorney. Ind. Code § 33-39-1-5	
Unlawful Recording	State	Ind. Code § 35-46-8-4	"A person who knowingly or intentionally uses an audiovisual recording device in a motion picture exhibition facility with the intent to transmit or record a motion picture commits unlawful recording, a Class B misdemeanor."	Class B misdemeanor. Ind. Code § 35-50-3-3	2 years. Ind. Code § 35-41-4-2(a)(2)	Prosecuting Attorney. Ind. Code § 33-39-1-5	
Unlawful Photography and Surveillance of Private Property	State	Ind. Code § 35-46-8.5-1	"A person who knowingly or intentionally places a camera or electronic surveillance equipment that records images or data of any kind while unattended on the private property of another person without the consent of the owner or tenant of the private property commits a Class A misdemeanor." Note: Multiple exceptions are enumerated within the statute.	Class A misdemeanor. Ind. Code § 35-50-3-2	2 years. Ind. Code § 35-41-4-2(a)(2)	Prosecuting Attorney. Ind. Code § 33-39-1-5	
State Insurance Commissioners Navigators and Application Organizations	State	760 Ind. Admin. Code § 4-5-2	"Navigators and application organizations shall comply with the following safeguards to maintain and protect the confidentiality of personal information."	Not less than $50 and up to $10,000 per violation. 760 Ind. Admin. Code § 4-7-1(d)	NA	If a navigator or application organization does not comply with the requirements of this rule, the commissioner may initiate an enforcement action against the navigator or application organization under 760 Ind. Admin. Code 4-7.	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Alabama Breach Notification Law	Ala. Code § 8-38-5	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 1000 people • Notify Credit Reporting Agencies: Yes, if over 1000 people • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: over 10,000 residents or $500,000 • Credit Monitoring: No	$500,000 and $5,000 per day. Ala. Code § 8-38-9	Attorney General. Ala. Code § 8-38-9	N/A
Alabama Personal Information Protection Act	Ala. Code § 8-38-3	"Each covered entity and third-party agent shall implement and maintain reasonable security measures to protect sensitive personally identifying information against a breach of security."	Most likely, this would be considered a deceptive practice under Ala. Code § 8-19-5.	None	
Alabama Unfair, Deceptive, or Abusive Acts and Practices	Ala. Code § 8-19-5	"The following deceptive acts or practices in the conduct of any trade or commerce are hereby declared to be unlawful: . . . (27) Engaging in any other unconscionable, false, misleading, or deceptive act or practice in the conduct of trade or commerce."	Up to $2,000 per violation: Ala. Code § 8-19-11	Attorney General. Ala. Code § 8-19-4	
Definition of Personal Information	Ala. Code § 8-38-2	(6) SENSITVE PERSONALLY IDENTIFYING INFORMATION. a. Except as provided in paragraph b., an Alabama resident's first name or first initial and last name in combination with one or more of the following with respect to the same Alabama resident: 1. A non-truncated Social Security number or tax identification number. 2. A non-truncated driver's license number, state-issued identification card number, passport number, military identification number, or other unique identification number issued on a government document used to verify the identity of a specific individual. 3. A financial account number, including a bank account number, credit card number, or debit card number, in combination with any security code, access code, password, expiration date, or PIN, that is necessary to access the financial account or to conduct a transaction that will credit or debit the financial account. 4. Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional. 5. An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual. 6. A user name or email address, in combination with a password or security question and answer that would permit access to an online account affiliated with the covered entity that is reasonably likely to contain or is used to obtain sensitive personally identifying information. b. The term does not include either of the following: 1. Information about an individual which has been lawfully made public by a federal, state, or local government record or a widely distributed media. 2. Information that is truncated, encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable, including encryption of the data, document, or device containing the sensitive personally identifying information, unless the covered entity knows or has reason to know that the encryption key or security credential that could render the personally identifying information readable or useable has been breached together with the information.	NA	NA	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Alabama Insurance Data Security Law	Act 2021–173. S.B. No. 54 (Adding Ch. 26 to Tit. 27; Amending Ala. Code § 10A-20-6.16)	Requires insurers to develop and implement an information security program, report certain cybersecurity events to the Commissioner of Insurance and provides for civil penalties under certain conditions. Two Important changes include: (1) a new definition of personal information ("PI"). "Nonpublic information" refers to any electronic information that is not publicly available concerning a consumer which, because of the name, number or other identifier, can be used to identify the consumer in combination with any of the following elements: social security number; driver's license number or Alabama identification card, financial account number, credit care, or debit car number; security code, access code, or password that would permit access to a consumer's financial account; biometric records; any information or data, except age or gender, derived form a health care provider that can be used to identify a particular consumer that relates to: past, present or future physical mental, or behavioral health of a consumer or member of the consumer's family, provision of health care to any consumer, or payment for the provision of health care to any consumer. (2) Notification of the Commissioner of Insurance within three business days if it is determined that a cybersecurity even involving nonpublic information that is in the possession of the licensee has occurred.	Revocation of license; up to $10,000 per violation Ala. Code § 27-62-10.	The Commissioner of Insurance. Ala. Code § 27-62-10.	New Law
Alaska Breach Notification Law	Alaska Stat. § 45.48.010	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if not disclosing to residents • Notify Credit Reporting Agencies: Yes, if over 1000 people • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: over 300,000 residents or $150,000 • Credit Monitoring: No	Up to $50,000: Alaska Stat. § 45.48.080(b)(1)	Attorney General: Alaska Stat. § 44.23.020(b)(4)	Changed "If not data owner, notify data owner: Unclear" to "Yes." See § 45.48.070.
Alaska Personal Information Protection Act	Alaska Stat. § 45.48.430	"A person doing business, including the business of government, may not disclose an individual's social security number to a third party."	Up to $3,000: Alaska Stat. § 45.48.480	Attorney General: Alaska Stat. § 44.23.020(b)(4)	
Alaska Unfair, Deceptive, or Abusive Acts and Practices	Alaska Stat. § 45.50.471	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of trade or commerce are declared to be unlawful."	Between $1,000 and $25,000 per violation: Alaska Stat. § 45.50.551	Attorney General: Alaska Stat. § 45.50.501	
Definition of Personal Information	Alaska Stat. § 45.48.090(7)	“personal information” means information in any form on an individual that is not encrypted or redacted, or is encrypted and the encryption key has been accessed or acquired, and that consists of a combination of (A) an individual's name; in this subparagraph, “individual's name” means a combination of an individual's (i) first name or first initial; and (ii) last name; and (B) one or more of the following information elements: (i) the individual's social security number; (ii) the individual's driver's license number or state identification card number; (iii) except as provided in (iv) of this subparagraph, the individual's account number, credit card number, or debit card number; (iv) if an account can only be accessed with a personal code, the number in (iii) of this subparagraph and the personal code; in this sub-subparagraph, “personal code” means a security code, an access code, a personal identification number, or a password; (v) passwords, personal identification numbers, or other access codes for financial accounts.	NA	NA	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Arizona Breach Notification Law	Ariz. Rev. Stat. § 18-552	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 1000 people • Notify Credit Reporting Agencies: Yes, if over 1000 people • If not data owner, notify data owner: Yes • How many days to Notify: Within 45 days • Substitute Notice: Yes, if: over 100,000 people or $50,000 • Credit Monitoring: No	Up to $500,000: Ariz. Rev. Stat. § 18-552(L)	Attorney General: Ariz. Rev. Stat. § 18-552(L)	Statute is now cited as Ariz. Rev. Stat. § 18-552 instead of § 18-545. Changed notification from "without unreasonable delay" to "45 days": Beginning Aug. 1, 2018, notification to affected individuals must be made within 45 days after the determination that there has been a security system breach. Changed penalty from $10,000 to $500,000 and cited updated statute. Updated statute cited in enforcement section.
Arizona Unfair, Deceptive, or Abusive Acts and Practices	Ariz. Rev. Stat. § 44-1522	"The act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise whether or not any person has in fact been misled, deceived or damaged thereby, is declared to be an unlawful practice."	Up to $10,000 per violation: Ariz. Rev. Stat. § 44-1531	Attorney General: Ariz. Rev. Stat. § 44-1524	
Definition of Personal Information	Ariz. Rev. Stat. § 18-551(7)	"Personal Information": (a) Means any of the following: (i) An individual's first name or first initial and last name in combination with one or more specified data elements. (ii) An individual's user name or e-mail address, in combination with a password or security question and answer, that allows access to an online account. (b) Does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.	NA	NA	
Arkansas Breach Notification Law	Ark. Code § 4-110-105	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 1000 people • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay; 45 days if over 1000 people • Substitute Notice: Yes, if: 500,000 residents or $250,000 • Credit Monitoring: No	Up to $10,000 per violation: Ark. Code §§ 4-110-108; 4-88-113	Attorney General: Ark. Code Ark. Code §§ 4-110-108;§ 4-88-104	Amended by HB 1943. Changed attorney general notice requirement to yes if over 1000 people and days to notify to 45 if over 1000 people affected.

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Arkansas Personal Information Protection Act	Ark. Code § 4-110-104(b)	"A person or business that acquires, owns, or licenses personal information about an Arkansas resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure"	Up to $10,000 per violation: Ark. Code §§ 4-110-108; 4-88-113	Attorney General: Ark. Code Ark. Code §§ 4-110-108;§ 4-88-104	
Concealment, surppression, or omission of material facts	Ark. Code § 4-88-108	following is unlawful: (1) The act, use, or employment by a person of any deception, fraud, or false pretense; (2) The concealment, suppression, or omission of any material fact with intent that others rely upon the concealment, suppression, or omission; (3) Displaying or causing to be displayed a fictitious or misleading name or telephone number on an Arkansas resident's caller identification service; or (4) Using a third party to display or cause to be displayed a fictitious or misleading name or telephone number on an Arkansas resident's caller identification service. (b) Subdivision (a)(3) of this section does not apply to the transmission of a caller identification service by a telecommunications provider that complies with § 23-17-122."	Up to $10,000 per violation: Ark. Code § 4-88-113	Attorney General: Ark. Code § 4-88-104	
Definition of Personal Information	Ark. Code § 4-110-103(7)	(7) “Personal information” means an individual's first name or first initial and his or her last name in combination with any one (1) or more of the following data elements when either the name or the data element is not encrypted or redacted: (A) Social Security number; (B) Driver's license number or Arkansas identification card number; (C) Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; and (D) Medical information; and (E)(i) Biometric data.(ii) as used in this subdivision (7)(E), "biometric data" means data generated by automatic measurements of an individual's biological characteristics, including without limitation: (a) Fingerprints; (b) Faceprint; (c) A retinal or iris scan; (d) Hand geometry; (e) Voiceprint analysis; (f) Deoxyribonucleic acid (DNA); or (g) Any other unique biological characteristics of an individual if the characteristics are used by the owner or licensee to uniquely authenticate the individual's identity when the individual accesses a system or account.	NA	NA	Amended by H.B. 1943. Added subsection (E).
California Breach Notification Law: Person or business who owns or licenses computerized data including personal information; breach of security of the system; disclosure requirments.	Cal. Civ. Code § 1798.82	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, if over 1000 people • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. • Credit Monitoring: No	Up to $3,000 per transaction: Cal. Civ. Code § 1798.84	Private right of action: Cal. Civ. Code § 1798.84	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
California Personal Information Protection Act: Security procedures and practices with respect to personal information about California residents	Cal. Civ. Code § 1798.81.5	"A business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."	Up to $3,000 per transaction: Cal. Civ. Code § 1798.84	Private right of action: Cal. Civ. Code § 1798.84	
California Unfair, Deceptive, or Abusive Acts and Practices	Cal. Bus. & Prof. Code § 17200	"As used in this chapter, unfair competition shall mean and include any unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising and any act prohibited by Chapter 1 (commencing with Section 17500) of Part 3 of Division 7 of the Business and Professions Code."	$2,500 per violation: Cal. Bus. & Prof. Code § 17206	Attorney General: Cal. Bus. & Prof. Code § 17206	
California Equipment of Connected devises with security features; requirements	Cal. Civ. Code § 1798.91.04	A manufacturer of a connected device (such as an Amazon Alexa or the like) shall equip the device with a reasonable security feature or features that are all of the following: (1) Appropriate to the nature and function of the device. (2) Appropriate to the information it may collect, contain, or transmit. (3) Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure. (b) Subject to all of the requirements of subdivision (a), if a connected device is equipped with a means for authentication outside a local area network, it shall be deemed a reasonable security feature under subdivision (a) if either of the following requirements are met: (1) The preprogrammed password is unique to each device manufactured. (2) The device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time.	Not stated in statute	Attorney General. Cal. Civ. Code § 1798.91.06(e)	New law (as of Jan. 1, 2019)

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
California Consumer Privacy Act of 2018	A.B. 375 (Adding Civ. Code § 1798 et seq.)	The California Consumer Privacy Act ("CCPA") will allow consumers to sue companies for unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information. You do not have to prove that you have been harmed by the data breach.	A consumer. Cal. Civ. Code § 1798.150	A civil penalty of up to $7,500 for each violation; An amount not less than $100 and not greater than $750 per consumer per incident or actual damages. Cal. Civ. Code §§ 1798.150(a)(1)(A) & 1798.155(b).	New Law (Passed on June 28, 2018. Goes into effect on January 1, 2020)
Definition of Personal Information	Cal. Civ. Code § 1798.140(o)	(o) (1) "Personal information" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following: (A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers. (B) Any categories of personal information described in subdivision (e) of Section 1798.80. (C) Characteristics of protected classifications under California or federal law. (D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies. (E) Biometric information. (F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an Internet Web site, application, or advertisement. (G) Geolocation data. (H) Audio, electronic, visual, thermal, olfactory, or similar information. (I) Professional or employment-related information. (J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. section 1232g, 34 C.F.R. Part 99). (K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, preferences, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes. (2) "Personal information" does not include publicly available information. For these purposes, "publicly available" means information that is lawfully made available from federal, state, or local government records, if any conditions associated with such information. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge. Information is not "publicly available" if that data is used for a purpose that is not compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained. "Publicly available" does not include consumer	NA	NA	As added by A.B. 375 (Effective January 1, 2020).
Colorado Breach Notification Law	Colo. Rev. Stat. § 6-1-716	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 500 people • Notify Credit Reporting Agencies: Yes, if over 1000 people • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay, no later than 30 days after occurrence • Substitute Notice: Yes, if: 250,000 residents or $250,000 or if contact information is insufficient • Credit Monitoring: No	"The attorney general may bring an action in law or equity to address violations of this section and for other relief that may be appropriate to ensure compliance with this section or to recover direct economic damages resulting from a violation, or both. The provisions of this section are not exclusive and do not relieve an individual or a commercial entity subject to this section from compliance with all other applicable provisions of law." Colo. Rev. Stat. § 6-1-716(4)	Attorney General: Colo. Rev. Stat. § 6-1-716(4)	Amended by H.B. 18-1128 (effective Sept. 1, 2018)

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Colorado Unfair, Deceptive, or Abusive Acts and Practices	Colo. Rev. Stat. § 6-1-105	"A person engages in a deceptive trade practice when, in the course of the person's business, vocation, or occupation, the person:"	Up to $20,000 per violation: Colo. Rev. Stat. § 6-1-112	Attorney General: Colo. Rev. Stat. § 6-1-103.	
Definition of Personal Information	Colo. Rev. Stat. § 6-1-716(g)	(g)(I)(A) "Personal information" means a Colorado resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident, when the data elements are not encrypted, redacted, or secured by any other method rendering the name or the element unreadable or unusable: Social security number; student, military, or passport identification number; driver's license number or identification card number; medical information; health insurance identification number; or biometric data; (B) A Colorado resident's username or e-mail address, in combination with a password or security questions and answers, that would permit access to an online account; or (C) A Colorado resident's account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to that account. (II) "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.	NA	NA	Amended by H.B. 18-1128
Connecticut Breach Notification Law	Conn. Gen. Stat. § 36a-701b	• Notify Affected Residents: Yes [36a-701b(b)(1)] • Notify Attorney General: Yes [36a-701b(f)] • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes [36a-701b(c)] • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: 500,000 residents or $250,000 • Credit Monitoring: Yes, 24 months • Other:	Up to $25,000 per violation: Conn. Gen. Stat. §§ 36a-701b(g), 42-110o	Attorney General: Conn. Gen. Stat. §§ 36a-701b(g), 42-110b	Fixed enforcement provision citation; violation of 36a-701(b) constitutes an "unfair trade practice" for the purposes of 42-110b - ATM

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Connecticut Personal Information Protection Act	Conn. Gen. Stat. § 42-471	"Any person who collects Social Security numbers in the course of business shall create a privacy protection policy which shall be published or publicly displayed. For purposes of this subsection, "publicly displayed" includes, but is not limited to, posting on an Internet web page. Such policy shall: (1) Protect the confidentiality of Social Security numbers, (2) prohibit unlawful disclosure of Social Security numbers, and (3) limit access to Social Security numbers."	Up to $25,000 per violation: Conn. Gen. Stat. §§ 42-471(h), 36a-701b(g), 42-110o,	Attorney General: Conn. Gen. Stat. §§ 42-471(h), 36a-701b(g), 42-110o,	
Connecticut Unfair, Deceptive, or Abusive Acts and Practices	Conn. Gen. Stat. § 42-110b	"No person shall engage in unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce."	Up to $25,000 per violation: Conn. Gen. Stat. § 42-110o	Attorney General: Conn. Gen. Stat. § 42-110o	
Connecticut Insurance Data Security Law	H.B. 7424 § 230	Requires any insurance licensee to implement an information security program by October 1, 2020. Requirements include the implementation and maintenance of a written information security program based upon a risk assessment as well as administrative, technical and physical safeguards to protect non-public information.	Suspending, revoking, or refusing to reissue a license; a civil penalty of not more than $50,000 for each violation of the provisions of this section	Insurance Commissioner	Becomes Effective October 1, 2019

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Definition of Personal Information	Conn. Gen. Stat. § 36a-701b(a)(2)	(2) "personal information" means an individual's first name or first initial and last name in combination with any one, or more, of the following data: (A) Social Security number; (B) driver's license number or state identification card number; (C) credit or debit card number; or (D) financial account number in combination with any required security code, access code or password that would permit access to such financial account. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.	NA	NA	
Delaware Breach Notification Law	Del. Code tit. 6, § 12B-102	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 500 residents • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay, but no more than 60 days • Substitute Notice: Yes, if over 100,000 residents or $75,000 • Credit Monitoring: Yes, if SSN breached, 12 months • Other:	"an action in law or equity to address the violations of this chapter and for other relief that may be appropriate to ensure proper compliance with this chapter or to recover direct economic damages resulting from a violation, or both." 6 Del. C. § 12B-104	Director of Consumer Protection of the Department of Justice: 6 Del. C. § 12B-104	
Delaware Personal Information Protection Act	Del. Code tit. 6, § 12B-100	"Any person who conducts business in this State and owns, licenses, or maintains personal information shall implement and maintain reasonable procedures and practices to prevent the unauthorized acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business."	"an action in law or equity to address the violations of this chapter and for other relief that may be appropriate to ensure proper compliance with this chapter or to recover direct economic damages resulting from a violation, or both." 6 Del. C. § 12B-104	Director of Consumer Protection of the Department of Justice: 6 Del. C. § 12B-104	
Delaware Unfair, Deceptive, or Abusive Acts and Practices	Del. Code tit. 6, § 2532	"A person engages in a deceptive trade practice when, in the course of a business, vocation, or occupation, that person:. . ."	Up to $10,000 per willful violation: Del. Code tit. 6, § 2533	Attorney General: Del. Code tit. 6, § 2533	
Delaware Insurance Data Security Act	H.B. 174 (Adding Del. Code tit. 18, § 4601 et seq.)	Requires insurance licensees to implement information security programs, report instances of data breaches in a timely manner to the Insurance Commissioner and to effected consumers, and allows the Department of Insurance to investigate violations and levy penalties against a violating insurer.	No more than $15,000 per violation for individuals and $50,000 per violation for insurance companies. Del. Code Tit. 18, § 329	Insurance Commissioner	Effective July 1, 2019

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Definition of Personal Information	Del. Code tit. 6, § 12B-101(7)	(7) a. "Personal information" means a Delaware resident's first name or first initial and last name in combination with any 1 or more of the following data elements that relate to that individual: 1. Social Security number. 2. Driver's license number or state or federal identification card number. 3. Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account. 4. Passport number. 5. A username or email address, in combination with a password or security question and answer that would permit access to an online account. 6. Medical history, medical treatment by a healthcare professional, diagnosis of mental or physical condition by a healthcare professional, or deoxyribonucleic acid profile. 7. Health insurance policy number, subscriber identification number, or any other unique identifier used by a health insurer to identify the person. 8. Unique biometric data generated from measurements or analysis of human body characteristics for authentication purposes. 9. An individual taxpayer identification number. b. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely-distributed media.	NA	NA	
Florida Breach Notification Law	Fla. Stat. § 501.171(4)(a)	• Notify Affected Residents: Yes • Notify Department of Legal Affairs: Yes, if over 500 • Notify Credit Reporting Agencies: Yes, if over 1000 people • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: over 500,000 residents or $250,000 • Credit Monitoring: • Other:	Up to $500,000 and more penalties: Fla. Stat. § 501.171(9)	Department of Legal Affairs: Fla. Stat. § 501.171(9)	
Florida Personal Information Protection Act	Fla. Stat. § 501.171(2)	"Each covered entity, governmental entity, or third-party agent shall take reasonable measures to protect and secure data in electronic form containing personal information."	Up to $500,000 and more penalties: Fla. Stat. § 501.171(9)	Department of Legal Affairs: Fla. Stat. § 501.171(9)	
Florida Unfair, Deceptive, or Abusive Acts and Practices	Fla. Stat. § 501.204	"Unfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful"	Up to $10,000 per violation: Fla. Stat. § 501.2075	Department of Legal Affairs: Fla. Stat. § 501.2075	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Definition of Personal Information	Fla. Stat. § 501.171(1)(g)	1. “Personal information” means either of the following: a. An individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual: (I) A social security number; (II) A driver license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity; (III) A financial account number or credit or debit card number, in combination with any required security code, access code, or password that is necessary to permit access to an individual's financial account; (IV) Any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or (V) An individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual. b. A user name or e-mail address, in combination with a password or security question and answer that would permit access to an online account. 2. The term does not include information about an individual that has been made publicly available by a federal, state, or local governmental entity. The term also does not include information that is encrypted, secured, or modified by any other method or technology that removes elements that personally identify an individual or that otherwise renders the information unusable.	NA	NA	
Georgia Breach Notification Law	Ga. Code § 10-1-912	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 10,000 residents • If not data owner, notify data owner: Yes, within 24 hours • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: over 100,000 residents or $50,000 • Credit Monitoring: No	None	None	
Unfair, Deceptive, or Abusive Acts and Practices	Ga. Code § 10-1-393	"Unfair or deceptive acts or practices in the conduct of consumer transactions and consumer acts or practices in trade or commerce are declared unlawful."	Up to $5,000 per violation: Ga. Code § 10-1-397(a)(2)(B)	Attorney General: Ga. Code § 10-1-397	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Definition of Personal Information	Ga. Code § 10-1-911	"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: (A) Social security number; (B) Driver's license number or state identification card number; (C) Account number, credit card number, or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes, or passwords; (D) Account passwords or personal identification numbers or other access codes; or (E) Any of the items contained in subparagraphs (A) through (D) of this paragraph when not in connection with the individual's first name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised. The term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.	N/A	N/A	
Hawaii Breach Notification Law	Haw. Rev. Stat. § 487N-2	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 1000 residents • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 200,000 residents or $100,000 • Credit Monitoring: No	Up to $2,500 per violation: Haw. Rev. Stat. § 487N-3	Attorney General: Haw. Rev. Stat. § 487N-3	
Hawaii Unfair, Deceptive, or Abusive Acts and Practices	Haw. Rev. Stat. § 480-2	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are unlawful."	Up to $10,000 per violation (No less than $500): Haw. Rev. Stat. § 480-3.1	Attorney General or Director of the Office of Consumer Protections: :Haw. Rev. Stat. § 480-3.1	
Definition of Personal Information	Haw. Rev. Stat. § 487N-1	"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number; (2) Driver's license number or Hawaii identification card number; or (3) Account number, credit or debit card number, access code, or password that would permit access to an individual's financial account. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.	NA	NA	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Idaho Breach Notification Law	Idaho Code § 28-51-105	• Notify Affected Residents: Yes • Notify Attorney General: Yes, within 24 hours of breach • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 50,000 residents or $25,000 • Credit Monitoring: No	Up to $25,000 per breach: Idaho Code § 28-51-107	Attorney General: Idaho Code § 28-51-107	
Idaho Unfair, Deceptive, or Abusive Acts and Practices	Idaho Code § 48-603	"The following unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared to be unlawful, where a person knows, or in the exercise of due care should know, that he has in the past, or is:"	Up to $5,000 per violation: Idaho Code § 48-606(1)(e)	Attorney General: Idaho Code § 48-606	
Definition of Personal Information	Idaho Code § 28-51-104(5)	"Personal information" means an Idaho resident's first name or first initial and last name in combination with any one (1) or more of the following data elements that relate to the resident, when either the name or the data elements are not encrypted: (a) Social security number; (b) Driver's license number or Idaho identification card number; or (c) Account number, or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account. The term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media.	NA	NA	
Illinois Breach Notification Law	815 Ill. Comp. Stat. § 530/10	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: No	Up to $50,000: 815 ILCS §§ 530/20; 505/7	Attorney General: 815 ILCS §§ 530/20; 505/7	
Personal Information Protection Act	815 Ill. Comp. Stat. § 530/45	"A data collector that owns or licenses, or maintains or stores but does not own or license, records that contain personal information concerning an Illinois resident shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification, or disclosure."	Up to $50,000: 815 ILCS §§ 530/20; 505/7	Attorney General: 815 ILCS §§ 530/20; 505/7	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Unfair, Deceptive, or Abusive Acts and Practices	815 Ill. Comp. Stat. § 505/2	"Unfair methods of competition and unfair or deceptive acts or practices, including but not limited to the use or employment of any deception, fraud, false pretense, false promise, misrepresentation or the concealment, suppression or omission of any material fact, with intent that others rely upon the concealment, suppression or omission of such material fact, or the use or employment of any practice described in Section 2 of the "Uniform Deceptive Trade Practices Act", approved August 5, 1965,1 in the conduct of any trade or commerce are hereby declared unlawful whether any person has in fact been misled, deceived or damaged thereby. In construing this section consideration shall be given to the interpretations of the Federal Trade Commission and the federal courts relating to Section 5(a) of the Federal Trade Commission Act.2"	Up to $50,000: 815 Ill. Comp. Stat. § 505/7	Attorney General: 815 Ill. Comp. Stat. § 505/7	
Definition of Personal Information	815 Ill. Comp. Stat. § 530/5	"Personal information" means either of the following: (1) an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired without authorization through the breach of security: (A) Social Security number. (B) Driver's license number or State identification card number. (C) Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account. (D) Medical information. (E) Health insurance information. (F) Unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee to authenticate an individual, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data. (2) user name or email address, in combination with a password or security question and answer that would permit access to an online account, when either the user name or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the data elements have been obtained through the breach of security. "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, State, or local government records.	NA	NA	
Iowa Breach Notification Law	Iowa Code § 715C.2	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 500 residents • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 350,000 residents or $250,000 • Credit Monitoring: No	Up to $40,000 per violation: Iowa Code §§ 715C.2(9), 714.16(7)	Attorney General: Iowa Code §§ 715C.2(9), 714.16(7)	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Unfair, Deceptive, or Abusive Acts and Practices	Iowa Code § 714.16	"The act, use or employment by a person of an unfair practice, deception, fraud, false pretense, false promise, or misrepresentation, or the concealment, suppression, or omission of a material fact with intent that others rely upon the concealment, suppression, or omission, in connection with the lease, sale, or advertisement of any merchandise or the solicitation of contributions for charitable purposes, whether or not a person has in fact been misled, deceived, or damaged, is an unlawful practice."	Up to $40,000 per violation: Iowa Code § 714.16(7)	Attorney General: Iowa Code § 714.16(7)	
Definition of Personal Information	Iowa Code § 715C.1	11. a. "Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements that relate to the individual if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable or are encrypted, redacted, or otherwise altered by any method or technology but the keys to unencrypt, unredact, or otherwise read the data elements have been obtained through the breach of security: (1) Social security number. (2) Driver's license number or other unique identification number created or collected by a government body. (3) Financial account number, credit card number, or debit card number in combination with any required expiration date, security code, access code, or password that would permit access to an individual's financial account. (4) Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account. (5) Unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data. b. "Personal information" does not include information that is lawfully obtained from publicly available sources, or from federal, state, or local government records lawfully made available to the general public.	NA	NA	
Kansas Breach Notification Law	Kan. Stat. § 50-7a02	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 5,000 residents or $100,000 • Credit Monitoring: No	". . . an action in law or equity to address violations of this section and for other relief that may be appropriate": Kan. Stat. § 50-7a02(g)	Attorney General: Kan. Stat. § 50-7a02(g)	
Personal Information Protection Act	Kan. Stat. § 50-6,139b(b)(1)	" A holder of personal information shall: (1) Implement and maintain reasonable procedures and practices appropriate to the nature of the information, and exercise reasonable care to protect the personal information from unauthorized access, use, modification or disclosure. If federal or state law or regulation governs the procedures and practices of the holder of personal information for such protection of personal information, then compliance with such federal or state law or regulation shall be deemed compliance with this paragraph and failure to comply with such federal or state law or regulation shall be prima facie evidence of a violation of this paragraph; . . ."	Up to $10,000 per violation or $20,000 per willful violation: Kan. Stat. §§ 50-6139b(d, e), 50-636	Attorney General: Kan. Stat. §§ 50-636, 50-6139b(e)	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Unfair, Deceptive, or Abusive Acts and Practices	Kan. Stat. § 50-627	"No supplier shall engage in any deceptive act or practice in connection with a consumer transaction."	Up to $10,000 per violation or $20,000 per willful violation: Kan. Stat. § 50-636	Attorney General: Kan. Stat. §§ 50-636, 50-6139b(e)	
Definition of Personal Information	Kan. Stat. § 50-7a01(g)	"Personal information" means a consumer's first name or first initial and last name linked to any one or more of the following data elements that relate to the consumer, when the data elements are neither encrypted nor redacted: (1) Social security number; (2) driver's license number or state identification card number; or (3) financial account number, or credit or debit card number, alone or in combination with any required security code, access code or password that would permit access to a consumer's financial account. The term "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records.	NA	NA	
Kentucky Breach Notification Law	Ky. Rev. Stat. § 365.732	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 people • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if: 500,000 residents or $250,000 • Credit Monitoring: No	None	Private Right of Action: Ky. Rev. Stat. § 365.730	
Unfair, Deceptive, or Abusive Acts and Practices	Ky. Rev. Stat. § 367.170	"Unfair, false, misleading, or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."	Up to $2,000 per violation or up to $10,000 per violation for conduct directed at a person age 60 or older: Ky. Rev. Stat. § 367.990(2)	Attorney General: Ky. Rev. Stat. § 367.990(2)	
Definition of Personally Identifiable Information	Ky. Rev. Stat. § 365.732(c)	"Personally identifiable information" means an individual's first name or first initial and last name in combination with any one (1) or more of the following data elements, when the name or data element is not redacted: 1. Social Security number; 2. Driver's license number; or 3. Account number or credit or debit card number, in combination with any required security code, access code, or password to permit access to an individual's financial account.	NA	NA	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Louisiana Breach Notification Law	La. Rev. Stat. § 51:3074	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay but no later than 60 days • Substitute Notice: Yes, if over 100,000 residents or $100,000 • Credit Monitoring: No	". . . a fine not to exceed $5,000 per violation. Notice to the attorney general shall be timely if received within 10 days of distribution of notice to Louisiana citizens. Each day notice is not received by the attorney general shall be deemed a separate violation." 16 La. Admin. Code Pt III, 701	Attorney General: 16 La. Admin. Code Pt III, 701	Added "no later than 60 days." Changed "substitute notice" section from 50,000 people to 100,000 and $250,000 to $100,000. See La. Rev. Stat. § 51:3074G(3).
Unfair, Deceptive, or Abusive Acts and Practices	La. Stat. § 51:1405	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."	Up to $5,000 per violation: La. Rev. Stat. § 51:1407(B)	Attorney General: La. Rev. Stat. § 51:1407(A)	
Definition of Personal Information	La. Stat. § 51:3073(4)	(a) "Personal information" means the first name or first initial and last name of an individual resident of this state in combination with any one or more of the following data elements, when the name or the data element is not encrypted or redacted: (i) Social security number. (ii) Driver's license number or state identification card number. (iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. (iv) Passport number. (v) Biometric data. "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as fingerprints, voice print, eye retina or iris, or other unique biological characteristic that is used by the owner or licensee to uniquely authenticate an individual's identity when the individual accesses a system or account. (b) "Personal information" shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.	NA	NA	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Maine Breach Notification Law	10 M.R.S.A. §§ 1347-A, 1348	• Notify Affected Residents: Yes, if not regulated by the Department of Professional and Financial Regulation • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 1,000 people or $5,000 • Credit Monitoring: No	"[M]maximum of $2,500 for each day the person is in violation:" 10 M.R.S.A. § 1349	Attorney General: 10 M.R.S.A. § 1349 Appropriate state regulators within the Department of Professional and Financial Regulation: 10 M.R.S.A. § 1349	Added sentences including Department of Professional and Financial Regulation Added § 1347 (substitute notice citation)
Unfair, Deceptive, or Abusive Acts and Practices	5 M.R.S.A. § 207	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are declared unlawful."	$5,000 penalty for non-compliance with § 211: 5 M.R.S.A. § 212	Attorney General: 5 M.R.S.A. § 212	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Definition of Personal Information	10 M.R.S.A. § 1347(6)	"Personal information" means an individual's first name, or first initial, and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted: A. Social security number; B. Driver's license number or state identification card number; C. Account number, credit card number or debit card number, if circumstances exist wherein such a number could be used without additional identifying information, access codes or passwords; D. Account passwords or personal identification numbers or other access codes; or E. Any of the data elements contained in paragraphs A to D when not in connection with the individual's first name, or first initial, and last name, if the information if compromised would be sufficient to permit a person to fraudulently assume or attempt to assume the identity of the person whose information was compromised. "Personal information" does not include information from 3rd-party claims databases maintained by property and casualty insurers or publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.	NA	NA	
Maryland Breach Notification Law	Md. Code, Com. Law § 14-3504	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, over 1000 • If not data owner, notify data owner: Yes • How many days to Notify: As soon as reasonably practicable, but not later than 45 days after discovery of breach • Substitute Notice: Yes, if over 175,000 residents or $100,000 • Credit Monitoring: No • Other: Third party may not charge data owner a fee for providing information that the owner needs to make a notification.	up to $10,000 per violation: Md. Code, Com. Law §§ 14-3508, 13-410 up to $1,000 or imprisonment not exceeding one year: MD Code, Comm. Law, § 13-411	Division of Consumer Protection: Md. Code Comm. Law §§ 13-401, 13-101	Added Information for "Other" pursuant to Maryland HB 1154 (2019)
Personal Information Protection Act	Md. Code, Com. Law § 14-3503	"To protect personal information from unauthorized access, use, modification, or disclosure, a business that owns or licenses personal information of an individual residing in the State shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal information owned or licensed and the nature and size of the business and its operations."	$1,000 per violation: Md. Code, Com. Law §§ 14-3508, 13-410 up to $1,000 or imprisonment not exceeding one year: MD Code, Comm. Law, § 13-411	Division of Consumer Protection: Md. Code Comm. Law §§ 13-401, 13-101	
Unfair, Deceptive, or Abusive Acts and Practices	Md. Code, Com. Law §13-303	"A person may not engage in any unfair or deceptive trade practice, as defined in this subtitle or as further defined by the Division, in:. . ."	$1,000 per violation: Md. Code, Com. Law §§ 14-3508, 13-410 up to $1,000 or imprisonment not exceeding one year: MD Code, Comm. Law, § 13-411	Division of Consumer Protection: Md. Code Comm. Law §§ 13-401, 13-101	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Definition of Personal Information	Md. Code, Com. Law § 14-3501(e)	(1) "Personal information" means: (i) An individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name or the data elements are not encrypted, redacted, or otherwise protected by another method that renders the information unreadable or unusable: 1. A Social Security number, an Individual Taxpayer Identification Number, a passport number, or other identification number issued by the federal government; 2. A driver's license number or State identification card number; 3. An account number, a credit card number, or a debit card number, in combination with any required security code, access code, or password, that permits access to an individual's financial account; 4. Health information, including information about an individual's mental health; 5. A health insurance policy or certificate number or health insurance subscriber identification number, in combination with a unique identifier used by an insurer or an employer that is self-insured, that permits access to an individual's health information; or 6. Biometric data of an individual generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voice print, genetic print, retina or iris image, or other unique biological characteristic, that can be used to uniquely authenticate the individual's identity when the individual accesses a system or account; or (ii) A user name or e-mail address in combination with a password or security question and answer that permits access to an individual's e-mail account. (2) "Personal information" does not include: (i) Publicly available information that is lawfully made available to the general public from federal, State, or local government records; (ii) Information that an individual has consented to have publicly disseminated or listed; or (iii) Information that is disseminated or listed in accordance with the federal Health Insurance Portability and Accountability Act.	NA	NA	
Massachusetts Breach Notification Law	Mass. Gen. Laws Ch. 93H § 1, 3, 3A	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,00 residents or $250,000 • Credit Monitoring: 18 months	Up to $5,000 per violation: Mass. Gen. Laws Ch. 93A § 4	Attorney General: Mass. Gen. Laws § 93A § 4	
Unfair, Deceptive, or Abusive Acts and Practices	Mass. Gen. Laws Ch. 93A § 2	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."	Up to $5,000 per violation: Mass. Gen. Laws Ch. 93A § 4	Attorney General: Mass. Gen. Laws Ch. 93A § 4	
Definition of Personal Information	Mass. Gen. Laws Ch. 93H § 1	"Personal information" a resident's first name and last name or first initial and last name in combination with any 1 or more of the following data elements that relate to such resident: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account; provided, however, that "Personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.	NA	NA	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Michigan Breach Notification Law	Mich. Comp. Laws § 445.72	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: No	$250 per notice failure, or up to $750,000 per breach: Mich. Comp. Laws § 445.72(13)	Attorney General: Mich. Comp. Laws § 445.72(13)	
Unfair, unconscionable, or deceptive methods, acts, or practices; promulgation of rules	Mich. Comp. Laws § 445.903	"Unfair, unconscionable, or deceptive methods, acts, or practices in the conduct of trade or commerce are unlawful and are defined as follows:. . ."	Up to $25,000: Mich. Comp. Laws § 445.905	Attorney General: Mich. Comp. Laws § 445.905	
Definition of Personal Information	Mich. Comp. Laws § 445.63(r)	"Personal information" means the first name or first initial and last name linked to 1 or more of the following data elements of a resident of this state: (i) Social security number. (ii) Driver license number or state personal identification card number. (iii) Demand deposit or other financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to any of the resident's financial accounts.	NA	NA	
Definition of Personal Identifying Information	Mich. Comp. Laws § 445.63(q)	"Personal identifying information" means a name, number, or other information that is used for the purpose of identifying a specific person or providing access to a person's financial accounts, including, but not limited to, a person's name, address, telephone number, driver license or state personal identification card number, social security number, place of employment, employee identification number, employer or taxpayer identification number, government passport number, health insurance identification number, mother's maiden name, demand deposit account number, savings account number, financial transaction device account number or the person's account password, any other account password in combination with sufficient information to identify and access the account, automated or electronic signature, biometrics, stock or other security certificate or account number, credit card number, vital record, or medical records or information.	NA	NA	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Minnesota Breach Notification Law	Minn. Stat. § 325E.61,	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, if over 500 residents. Notification in 48 hours. • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: No	Unclear: Minn. Stat. §§ 325E.61(6), 8.31	Attorney General: Minn. Stat. §§ 325E.61(6), 8.31	
Unfair, Deceptive, or Abusive Acts and Practices	Minn. Stat. § 325F.69	Fraud, misrepresentation, deceptive practices. The act, use, or employment by any person of any fraud, false pretense, false promise, misrepresentation, misleading statement or deceptive practice, with the intent that others rely thereon in connection with the sale of any merchandise, whether or not any person has in fact been misled, deceived, or damaged thereby, is enjoinable as provided in section 325F.70.	Up to $25,000 (Does not specify per violation or all violations). Additional private remedies allowed including costs and disbursements, including costs of investigation and reasonable attorney's fees, and other equitable relief. Minn. Stat. Ann. § 8.31	Attorney General: Minn. Stat. § 8.31	
Definition of Personal Information	Minn. Stat. § 325E.61(e)-(f)	For purposes of this section and section 13.055, subdivision 6, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the data element is not secured by encryption or another method of technology that makes electronic data unreadable or unusable, or was secured and the encryption key, password, or other means necessary for reading or using the data was also acquired: (1) Social Security number; (2) driver's license number or Minnesota identification card number; or (3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. For purposes of this section and section 13.055, subdivision 6, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.	NA	NA	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Mississippi Breach Notification Law	Miss. Code § 75-24-29	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 5,000 residents or $5,000 • Credit Monitoring: • Other:	$10,000 per violation: Miss. Code § 75-24-19	Attorney General: Miss. Code § 75-24-29(8)	
Unfair, Deceptive, or Abusive Acts and Practices	Miss. Code § 75-24-5	Unfair methods of competition affecting commerce and unfair or deceptive trade practices in or affecting commerce are prohibited. Action may be brought under Section 75-24-5(1) only under the provisions of Section 75-24-9.	$10,000 per violation: Miss. Code § 75-24-19	Attorney General: Miss. Code § 75-24-9	
Definition of Personal Information	Miss. Code § 75-24-29(2)(b)	"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements: (i) Social security number; (ii) Driver's license number or state identification card number; or (iii) An account number or credit or debit card number in combination with any required security code, access code or password that would permit access to an individual's financial account; "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media; (iv) "Affected individual" means any individual who is a resident of this state whose personal information was, or is reasonably believed to have been, intentionally acquired by an unauthorized person through a breach of security.	NA	NA	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Missouri Breach Notification Law	Mo. Rev. Stat. § 407.1500	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 1000 residents • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 150,000 residents or $100,000 • Credit Monitoring: • Other:	Up to $150,000: Mo. Rev. Stat. § 407.1500(3)	Attorney General: Mo. Rev. Stat. § 407.1500(3)	Corrected substitute notice amount to $100,000, it was $150,000.
Unfair, Deceptive, or Abusive Acts and Practices	Mo. Rev. Stat. § 407.020	Any act, use or employment by any person of any deception, fraud, false pretense, false promise, misrepresentation, unfair practice or the concealment, suppression, or omission of any material fact in connection with the sale or advertisement of any merchandise in trade or commerce or the solicitation of any funds for any charitable purpose, as defined in section 407.453, in or from the state of Missouri, is declared to be an unlawful practice.	Up to $1000 per violation: Mo. Rev. Stat. § 407.100(6)	Attorney General: Mo. Rev. Stat. § 407.100	
Definition of Personal Information	Mo. Rev. Stat. § 407.1500(1)(9)	"Personal information", an individual's first name or first initial and last name in combination with any one or more of the following data elements that relate to the individual if any of the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable or unusable: (a) Social Security number; (b) Driver's license number or other unique identification number created or collected by a government body; (c) Financial account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; (d) Unique electronic identifier or routing code, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (e) Medical information; or (f) Health insurance information. "Personal information" does not include information that is lawfully obtained from publicly available sources, or from federal, state, or local government records lawfully made available to the general public;	NA	NA	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Montana Breach Notification Law	Mont. Code § 30-14-1704	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, coordination provision • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: • Other:	Up to $10,000 per willful violation: MCA §§ 30-14-1705; 30-14-142(2)	Department of Justice (Attorney General): MCA § 30-14-1705	
Unfair, Deceptive, or Abusive Acts and Practices	Mont. Code § 30-14-103	Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are unlawful.	Up to $10,000 per willful violation: MCA § 30-14-142(2)	Department of Justice (Attorney General): MCA § 30-14-1705	
Definition of Personal Information	Mont. Code § 30-14-1702(7)	"Personal information" means an individual's name, signature, address, or telephone number, in combination with one or more additional pieces of information about the individual, consisting of the individual's passport number, driver's license or state identification number, insurance policy number, bank account number, credit card number, debit card number, passwords or personal identification numbers required to obtain access to the individual's finances, or any other financial information as provided by rule. A social security number, in and of itself, constitutes personal information.	NA	NA	
Nebraska Breach Notification Law	Neb. Rev. Stat. §§ 87-802, 87-803	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 100,000 residents or $75,000 • Credit Monitoring: No	Direct economic damage: Neb. Rev. Stat. § 87-806	Attorney General: Neb. Rev. Stat. § 87-806	
Unfair, Deceptive, or Abusive Acts and Practices	Neb. Rev. Stat. § 59-1602	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce shall be unlawful."	Up to $2,000 per violation: Neb. Rev. Stat. § 59-1614	Attorney General: Neb. Rev. Stat. § 59-1614	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Definition of Personal Information	Neb. Rev. Stat. § 87-802(5)	Personal information means either of the following: (a) A Nebraska resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident if either the name or the data elements are not encrypted, redacted, or otherwise altered by any method or technology in such a manner that the name or data elements are unreadable: (i) Social security number; (ii) Motor vehicle operator's license number or state identification card number; (iii) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account; (iv) Unique electronic identification number or routing code, in combination with any required security code, access code, or password; or (v) Unique biometric data, such as a fingerprint, voice print, or retina or iris image, or other unique physical representation; or (b) A user name or email address, in combination with a password or security question and answer, that would permit access to an online account. Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records	NA	NA	
Nevada Breach Notification Law	Nev. Rev. Stat. § 603A.220	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: No	Injunction: Nev. Rev. Stat. § 603A.290	Attorney General: Nev. Rev. Stat. § 603A.290	
Personal Information Protection Act	Nev. Rev. Stat. § 603A.210	"A data collector that maintains records which contain personal information of a resident of this State shall implement and maintain reasonable security measures to protect those records from unauthorized access, acquisition, destruction, use, modification or disclosure."	Injunction: Nev. Rev. Stat. § 603A.290	Attorney General: Nev. Rev. Stat. § 603A.290	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Unfair, Deceptive, or Abusive Acts and Practices	Nev. Rev. Stat. § 598A.060	"Every activity enumerated in this subsection constitutes a contract, combination or conspiracy in constraint of trade, and it is unlawful to conduct any part of any such activity in this State . . ."	An amount not to exceed 5% of the gross income realized by the sale or commodities or services sold in each year: N.R.S. § 598A.170	Attorney General: N.R.S. § 598A.070	
Definition of Personal Information	Nev. Rev. Stat. § 603A.040	1. "Personal information" means a natural person's first name or first initial and last name in combination with any one or more of the following data elements, when the name and data elements are not encrypted: (a) Social security number. (b) Driver's license number, driver authorization card number or identification card number. (c) Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to the person's financial account. (d) A medical identification number or a health insurance identification number. (e) A user name, unique identifier or electronic mail address in combination with a password, access code or security question and answer that would permit access to an online account. 2. The term does not include the last four digits of a social security number, the last four digits of a driver's license number, the last four digits of a driver authorization card number or the last four digits of an identification card number or publicly available information that is lawfully made available to the general public from federal, state or local governmental records.	NA	NA	
New Hampshire Breach Notification Law	N.H. Rev. Stat. § 359-C:20	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if subject to N.H. Rev. Stat. § 358-A:3(I) • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: As soon as possible • Substitute Notice: Yes, if over 1,000 residents or $5,000 • Credit Monitoring: No	Actual damages; if willful or knowing--as much as 3x but not less than 2x actual damages: N.H. Rev. Stat. §§ 359-C:21	Attorney General: N.H. Rev. Stat. §§ 359-C:21; 358-A:4	
Unfair, Deceptive, or Abusive Acts and Practices	N.H. Rev. Stat. § 358-A:2	"It shall be unlawful for any person to use any unfair method of competition or any unfair or deceptive act or practice in the conduct of any trade or commerce within this state. Such unfair method of competition or unfair or deceptive act or practice shall include, but is not limited to, the following:"	Up to $10,000 per violation: N.H. Rev. Stat. § 358-A:4(III)(b)	Consumer Protection and Antitrust Bureau, Department of Justice: N.H. Rev. Stat. § 358-A:4(I)	
Definition of Personal Information	N.H. Rev. Stat. § 359-C:19(IV)	(a) "Personal information" means an individual's first name or initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number. (2) Driver's license number or other government identification number. (3) Account number, credit card number, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. (b) "Personal information" shall not include information that is lawfully made available to the general public from federal, state, or local government records.	NA	NA	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
New Jersey Breach Notification Law	N.J. Stat. § 56:8-163	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: No • Other: Report to the Division of State Police in the Department of Law and Public Safety, prior to notification to residents	Up to $10,000 for the first offense, and $20,000 for subsequent offenses: N.J. Stat. § 56:8-13	Attorney General: N.J. Stat. § 56:8-3.1	
Unfair, Deceptive, or Abusive Acts and Practices	N.J. Stat. § 56:8-2	"The act, use or employment by any person of any unconscionable commercial practice, deception, fraud, false pretense, false promise, misrepresentation, or the knowing, concealment, suppression, or omission of any material fact with intent that others rely upon such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise or real estate, or with the subsequent performance of such person as aforesaid, whether or not any person has in fact been misled, deceived or damaged thereby, is declared to be an unlawful practice; provided, however, that nothing herein contained shall apply to the owner or publisher of newspapers, magazines, publications or printed matter wherein such advertisement appears, or to the owner or operator of a radio or television station which disseminates such advertisement when the owner, publisher, or operator has no knowledge of the intent, design or purpose of the advertiser."	Up to $10,000 for the first offense, and $20,000 for subsequent offenses: N.J. Stat. § 56:8-13	Attorney General: N.J. Stat. § 56:8-3.1	
Definition of Personal Information	N.J. Stat. § 56:8-161	“Personal information” means an individual's first name or first initial and last name linked with any one or more of the following data elements: (1) Social Security number; (2) driver's license number or State identification card number; or (3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data. For the purposes of sections 10 through 15 of this amendatory and supplementary act (referring to N.J. Stat. §§ 56:8-161 to 166), personal information shall not include publicly available information that is lawfully made available to the general public from federal, state or local government records, or widely distributed media.	NA	NA	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
New Mexico Breach Notification Law	N.M. Stat. § 57-12c-6; N.M. Stat. § 57-12c-10	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 1000 residents or if the cost of providing notification would exceed $100,000, if the number of residents to be notifies exceeds 50,000, the person does not have on record physical address or sufficient contact information for the residents that the person or business is required to notify. • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: No later than 45 days after the breach discovery date • Substitute Notice: Yes, if over 50,000 residents or $100,000, or if the person does not have on record a physical address or sufficient contact information for the residents that the person or business is required to notify. • Credit Monitoring: No	The Court may issue an injunction and award damages for actual costs or losses, including consequential financial losses. Civil Penalty: the great of $25,000 or, $10 per instance of failed notification up to a maximum of $150,000: N.M. Stat. § 57-12c-11	Attorney General: N.M. Stat. § 57-12c-11	Updated the criteria that may require you to notify the Attorney General. Updated the options for why you can provide substitute notice. Updated the penalty information Included additional statue which stated the requirement to notify credit reporting agencies
Personal Information Protection Act	N.M. Stat. § 57-12c-4	"A person that owns or licenses personal identifying information of a New Mexico resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal identifying information from unauthorized access, destruction, use, modification or disclosure."	The Court may issue an injunction and award damages for actual costs or losses, including consequential financial losses. Civil Penalty: the great of $25,000 or, $10 per instance of failed notification up to a maximum of $150,000: N.M. Stat. § 57-12c-11	Attorney General: N.M. Stat. § 57-12c-11	Updated the penalty information
Unfair, Deceptive, or Abusive Acts and Practices	N.M. Stat. § 57-12-3	"Unfair or deceptive trade practices and unconscionable trade practices in the conduct of any trade or commerce are unlawful."	Up to $5,000 per violation: N.M. Stat. § 57-12-11	Attorney General: N.M. Stat. § 57-12-8	Corrected the citation stating that an attorney may bring an action for unfair practices.
Definition of Personal Identifying Information	N.M. Stat. § 57-12c-2(C)	"personal identifying information": (1) means an individual's first name or first initial and last name in combination with one or more of the following data elements that relate to the individual, when the data elements are not protected through encryption or redaction or otherwise rendered unreadable or unusable: (a) social security number; (b) driver's license number; (c) government-issued identification number; (d) account number, credit card number or debit card number in combination with any required security code, access code or password that would permit access to a person's financial account; or (e) biometric data; and (2) does not mean information that is lawfully obtained from publicly available sources or from federal, state or local government records lawfully made available to the general public	NA	NA	
New York Breach Notification Law	N.Y. Gen. Bus. Law § 899-AA; N.Y. State Tech. Law § 208	• Notify Affected Residents: Potentially: "Notice to affected persons under this section is not required if the expose of private information was an inadvertent disclosure by persons authorized to access private information, and the person or business reasonably determines such exposure will not likely result in misuse of such information or financial harm to the affected persons or emotional harm in the case of unknown disclose of online credentials." • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, if over 5000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 residents or $250,000 or the business does not have sufficient contact information • Credit Monitoring: No	The court may award damages for actual costs or losses incurred by a person entitled to notice, including consequential financial losses. Civil penalty: the greater of $5,000 or up to $20 per instance of failed identification, provided that the latter amount shall not exceed $250,000. N.Y. Gen. Bus. Law § 899-AA(6)(a).	Attorney General: N.Y. Gen. Bus. Law § 899-AA(6)(a).	Updated the penalty requirements and corrected citations.

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Unfair, Deceptive, or Abusive Acts and Practices	N.Y. Gen. Bus. Law § 349	"Deceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state are hereby declared unlawful."	Up to $5,000 per violation: N.Y. Gen. Bus. Law § 350-d	Attorney General: N.Y. Gen. Bus. Law § 349(f) & 350-d	
The SHIELD Act	N.Y. Bill 5635-B; N.Y. Gen. Bus. Law § 899-bb	Adds the following additional requirements to entities subject to various data security regulations and standards: (b) A person or business shall be deemed to be in compliance with paragraph (a) of this subdivision if it either: (i) is a compliant regulated entity as defined in subdivision one of this section; or (ii) implements a data security program that includes the following: (A) reasonable administrative safeguards such as the following, in which the person or business: (1) designates one or more employees to coordinate the security program; (2) identifies reasonably foreseeable internal and external risks; (3) assesses the sufficiency of safeguards in place to control the identified risks; (4) trains and manages employees in the security program practices and procedures; (5) selects service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract; and (6) adjusts the security program in light of business changes or new circumstances; and (B) reasonable technical safeguards such as the following, in which the person or business: (1) assesses risks in network and software design; (2) assesses risks in information processing, transmission and storage; (3) detects, prevents and responds to attacks or system failures; and (4) regularly tests and monitors the effectiveness of key controls, systems and procedures; and (C) reasonable physical safeguards such as the following, in which the person or business: (1) assesses risks of information storage and disposal; (2) detects, prevents and responds to intrusions; (3) protects against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information; and (4) disposes of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the information cannot be read or reconstructed.	Any person or business that fails to comply with this subdivision shall be deemed to have violated the New York Unfair and Deceptive Practices Act.	Attorney General: N.Y. Gen. Bus. Law § 899-bb(d)	
Definition of Personal Information	N.Y. Gen. Bus. Law § 899-AA(1)(a)	“Personal information” shall mean any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person	NA	NA	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Definition of Private Information	N.Y. Gen. Bus. Law § 899-AA(1)(b); N.Y. State Tech. Law § 208(1)(a)	"Private information" shall mean either: (i) personal information consisting of any information in combination with any one or more of the following data elements, when either the data element or the combination of personal information or plus the data element is not encrypted, or is encrypted with an encryption key that has also been accessed or acquired: (1) social security number; (2) driver's license number or non-driver identification card number; or (3) account number, credit or debit card number, in combination with any required security code, access code, password or other information that would permit access to an individual's financial account; (4) account number, credit or debit card number, if circumstances exist wherein such number could be used to access an individual's financial account without additional identifying information, security code, access code, or password; or (5) biometric information, meaning data generated by electronic measurements of an individual's unique physical characteristics, such as a fingerprint, voice print, retina or iris image, or other unique physical representation or digital representation of biometric data which are used to authenticate or ascertain the individual's identity; or (ii) a user name or e-mail address in combination with a password or security question and answer that would permit access to an online account. "Private information" does not include publicly available information which is lawfully made available to the general public from federal, state, or local government records.	NA	NA	As amended by N.Y. Bill. 5635-B
North Carolina Breach Notification Law	N.C. Gen. Stat § 75-65	• Notify Affected Residents: Yes • Notify Attorney General: Yes • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 or $250,000 • Credit Monitoring: No • Other:	Up to $5,000 per violation: N.C. Gen. Stat. §§ 75-65(i), 75-15.2	Attorney General: N.C. Gen. Stat. §§ 75-65(i), 75-15	
Unfair, Deceptive, or Abusive Acts and Practices	N.C. Gen. Stat. § 75-1.1	"Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are declared unlawful."	Up to $5,000 per violation: N.C. Gen. Stat. § 75-15.2	Attorney General: N.C. Gen. Stat. § 75-15	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Definition of Personal Information	N.C. Gen. Stat. § 75-61(10); N.C. Gen. Stat. § 14-113.20	"Personal information".--A person's first name or first initial and last name in combination with identifying information as defined in G.S. 14-113.20(b). Personal information does not include publicly available directories containing information an individual has voluntarily consented to have publicly disseminated or listed, including name, address, and telephone number, and does not include information made lawfully available to the general public from federal, state, or local government records. The term "identifying information" as used in this Article includes the following: (1) Social security or employer taxpayer identification numbers. (2) Drivers license, State identification card, or passport numbers. (3) Checking account numbers. (4) Savings account numbers. (5) Credit card numbers. (6) Debit card numbers. (7) Personal Identification (PIN) Code as defined in G.S. 14-113.8(6). (8) Electronic identification numbers, electronic mail names or addresses, Internet account numbers, or Internet identification names. (9) Digital signatures. (10) Any other numbers or information that can be used to access a person's financial resources. (11) Biometric data. (12) Fingerprints. (13) Passwords. (14) Parent's legal surname prior to marriage.	NA	NA	
North Dakota Breach Notification Law	N.D. Cent. Code §§ 51-30-02; 51-30-03;	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 250 persons • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 500,000 persons or $250,000 or if they have insufficient contact information • Credit Monitoring: No	Up to $5,000 per violation: N.D. Cent. Code §§ 51-30-07, 51-15-11	Attorney General: N.D. Cent. Code § 51-30-07	Added additional statutes to clarify compliance
Unfair, Deceptive, or Abusive Acts and Practices	N.D. Cent. Code § 51-15-02	"The act, use, or employment by any person of any deceptive act or practice, fraud, false pretense, false promise, or misrepresentation, with the intent that others rely thereon in connection with the sale or advertisement of any merchandise, whether or not any person has in fact been misled, deceived, or damaged thereby, is declared to be an unlawful practice. The act, use, or employment by any person of any act or practice, in connection with the sale or advertisement of any merchandise, which is unconscionable or which causes or is likely to cause substantial injury to a person which is not reasonably avoidable by the injured person and not outweighed by countervailing benefits to consumers or to competition, is declared to be an unlawful practice."	Up to $5,000 per violation: N.D. Cent. Code § 51-15-11	Attorney General: N.D. Cent. Code § 51-15-07	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Definition of Personal Information	N.D. Cent. Code § 51-30-01(4)	a. “Personal information” means an individual's first name or first initial and last name in combination with any of the following data elements, when the name and the data elements are not encrypted: (1) The individual's social security number; (2) The operator's license number assigned to an individual by the department of transportation under section 39-06-14; (3) A nondriver color photo identification card number assigned to the individual by the department of transportation under section 39-06-03.1; (4) The individual's financial institution account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial accounts; (5) The individual's date of birth; (6) The maiden name of the individual's mother; (7) Medical information; (8) Health insurance information; (9) An identification number assigned to the individual by the individual's employer in combination with any required security code, access code, or password; or (10) The individual's digitized or other electronic signature. b. “Personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.	NA	NA	
Ohio Breach Notification Law	Ohio Rev. Code § 1349.19	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: No longer than 45 days following the breach discovery date • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: No • Other: Substitute notice exception for small businesses.	Cascading penalties based on delay: Ohio Rev. Code § 1349.192	Attorney General: Ohio Rev. Code § 1349.19(i)	
Unfair, Deceptive, or Abusive Acts and Practices	Ohio Rev. Code § 1345.02	"No supplier shall commit an unfair or deceptive act or practice in connection with a consumer transaction. Such an unfair or deceptive act or practice by a supplier violates this section whether it occurs before, during, or after the transaction."	Up to $25,000: Ohio Rev. Code § 1345.07	Attorney General: Ohio Rev. Code § 1345.02(E)(3)	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Definition of Personal Information	Ohio Rev. Code § 1349.19(A)(7)	(a) “Personal information” means an individual's name, consisting of the individual's first name or first initial and last name, in combination with and linked to any one or more of the following data elements, when the data elements are not encrypted, redacted, or altered by any method or technology in such a manner that the data elements are unreadable: (i) Social security number; (ii) Driver's license number or state identification card number; (iii) Account number or credit or debit card number, in combination with and linked to any required security code, access code, or password that would permit access to an individual's financial account. (b) “Personal information” does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records or any of the following media that are widely distributed: (i) Any news, editorial, or advertising statement published in any bona fide newspaper, journal, or magazine, or broadcast over radio or television; (ii) Any gathering or furnishing of information or news by any bona fide reporter, correspondent, or news bureau to news media described in division (A)(7)(b)(i) of this section; (iii) Any publication designed for and distributed to members of any bona fide association or charitable or fraternal nonprofit corporation; (iv) Any type of media similar in nature to any item, entity, or activity identified in division (A)(7)(b)(i), (ii), or (iii) of this section	NA	NA	
Oklahoma Breach Notification Law	Okla. Stat. tit. 24, § 163	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 100,000 residents or $50,000 • Credit Monitoring: No	Up to $150,000: Okla. Stat. § 24-165	Attorney General: Okla. Stat. § 24-165	
Unfair, Deceptive, or Abusive Acts and Practices	Okla. Stat. tit. 15, § 753	"A person engages in a practice which is declared to be unlawful under the Oklahoma Consumer Protection Act when, in the course of the person's business, the person . . ."	Up to $2,000 per violation or up to $10,000 per willful violation: Okla. Stat. tit. 15, § 761.1	Attorney General: Okla. Stat. tit. 15, § 761.	
Definition of Personal Information	Okla. Stat. tit. 24, § 162(6)	“Personal information” means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of this state, when the data elements are neither encrypted nor redacted: a. social security number, b. driver license number or state identification card number issued in lieu of a driver license, or c. financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to the financial accounts of a resident. The term does not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public;	NA	NA	
Oregon Breach Notification Law	Oregon Rev. Stat. § 646A.604	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 250 residents • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay, but not later than 45 days after discovering or receiving notification of the breach of security. • Substitute Notice: Yes, if over 350,000 residents and $250,000 • Credit Monitoring: Yes	Or. Rev. Stat. §§ 646A.604(9)(a), 646.642(3)	Director of the Department of Consumer and Business Services: Or. Rev. Stat. § 646A.624	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Personal Information Protection Act	Or. Rev. Stat. § 646A.622	"covered entity and a vendor shall develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the personal information, including safeguards that protect personal information when the covered entity or vendor disposes of the personal information."	Up to $1000 per violation: Or. Rev. Stat. § 646A.624	Director of the Department of Consumer and Business Services: Or. Rev. Stat. § 646A.624	
Unfair, Deceptive, or Abusive Acts and Practices	Or. Rev. Stat. § 646.607	"A person engages in an unlawful trade practice if in the course of the person's business, vocation or occupation the person. . ."	Up to $250,000 per violation: Or. Rev. Stat. § 646.642(3)	Prosecuting attorney: Or. Rev. Stat. § 646.642(3)	
Definition of Personal Information	Or. Rev. Stat. § 646A.602(11)	(A) A consumer's first name or first initial and last name in combination with any one or more of the following data elements, if encryption, redaction or other methods have not rendered the data elements unusable or if the data elements are encrypted and the encryption key has been acquired: (i) A consumer's Social Security number; (ii) A consumer's driver license number or state identification card number issued by the Department of Transportation; (iii) A consumer's passport number or other identification number issued by the United States; (iv) A consumer's financial account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to a consumer's financial account, or any other information or combination of information that a person reasonably knows or should know would permit access to the consumer's financial account; (v) Data from automatic measurements of a consumer's physical characteristics, such as an image of a fingerprint, retina or iris, that are used to authenticate the consumer's identity in the course of a financial transaction or other transaction; (vi) A consumer's health insurance policy number or health insurance subscriber identification number in combination with any other unique identifier that a health insurer uses to identify the consumer; or (vii) Any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer. (B) A user name or other means of identifying a consumer for the purpose of permitting access to the consumer's account, together with any other method necessary to authenticate the user name or means of identification. (B) (C) Any of the data elements or any combination of the data elements described in subparagraph (A) or (B) of this paragraph without the consumer's user name, or the consumer's first name or first initial and last name, if: (i) Encryption, redaction or other methods have not rendered the data element or combination of data elements unusable; and (ii) The data element or combination of data elements would enable a person to commit identity theft against a consumer.	NA	NA	The definition for personal information was amended in May of 2019 by Or. S.B.No. 684 to include the phrase "A user name or other means of identifying a consumer for the purpose of permitting access to the consumer's account, together with any other method necessary to authenticate the user name or means of identification."
Pennsylvania Breach Notification Law	73 Pa. Stat. § 2303	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 175,000 people or $100,000 • Credit Monitoring: No	Up to $1,000 per violation: 73 Pa. Stat. §§ 2308, 201-8	Attorney General: 73 Pa. Stat. § 2308	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Unfair, Deceptive, or Abusive Acts and Practices	73 Pa. Stat. § 201-3	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce as defined by subclauses (i) through (xxi) of clause (4) of section 21 of this act and regulations promulgated under section 3.12 of this act are hereby declared unlawful. The provisions of this act shall not apply to any owner, agent or employee of any radio or television station, or to any owner, publisher, printer, agent or employee of an Internet service provider or a newspaper or other publication, periodical or circular, who, in good faith and without knowledge of the falsity or deceptive character thereof, publishes, causes to be published or takes part in the publication of such advertisement."	Up to $1,000 per violation: 73 Pa. Stat. § 201-8	Attorney General: 73 Pa. Stat. § 201-8	
Definition of Personal Information	73 Pa. Stat. § 2302	"Personal information." (1) An individual's first name or first initial and last name in combination with and linked to any one or more of the following data elements when the data elements are not encrypted or redacted: (i) Social Security number. (ii) Driver's license number or a State identification card number issued in lieu of a driver's license. (iii) Financial account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account. (2) The term does not include publicly available information that is lawfully made available to the general public from Federal, State or local government records.	NA	NA	
Rhode Island Breach Notification Law	R.I. Gen. Laws § 11-49.3-4	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 500 residents • Notify Credit Reporting Agencies: Yes, if over 500 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: • Credit Monitoring: • Other:	$100 per reckless violation, $200 per knowing/willful violation: R.I. Gen. Laws § 11-49.3-5	Attorney General: R.I. Gen. Laws § 11-49.3-5	Effective June 2016, add resident requirement to Credit Reporting agencies, change 1000 to 500 for resident requirement for credit reporting agencies. Could not find substitute notice requirement in citation.
Personal Information Protection Act	R.I. Gen. Laws § 11-49.3-2	A municipal agency, state agency or person that stores, collects, processes, maintains, acquires, uses, owns or licenses personal information about a Rhode Island resident shall implement and maintain a risk-based information security program that contains reasonable security procedures and practices appropriate to the size and scope of the organization; the nature of the information; and the purpose for which the information was collected in order to protect the personal information from unauthorized access, use, modification, destruction, or disclosure and to preserve the confidentiality, integrity, and availability of such information. A municipal agency, state agency, or person shall not retain personal information for a period longer than is reasonably required to provide the services requested; to meet the purpose for which it was collected; or in accordance with a written retention policy or as may be required by law. A municipal agency, state agency, or person shall destroy all personal information, regardless of the medium that such information is in, in a secure manner, including, but not limited to, shredding, pulverization, incineration, or erasure.	$100 per reckless violation, $200 per knowing/willful violation: R.I. Gen. Laws § 11-49.3-5	Attorney General: R.I. Gen. Laws § 11-49.3-5	
Unfair, Deceptive, or Abusive Acts and Practices	R.I. Gen. Laws § 6-13.1-2	Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are declared unlawful.	Up to $10,000 per violation: R.I. Gen. Laws § 6-13.1-8	Attorney General: R.I. Gen. Laws § 6-13.1-8	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Definition of Personal Information	R.I. Gen. Laws § 11-49.3-3(8)	"Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name and the data elements are not encrypted or are in hard copy, paper format: (i) Social security number; (ii) Driver's license number, Rhode Island identification card number, or tribal identification number; (iii) Account number, credit, or debit card number, in combination with any required security code, access code, password, or personal identification number, that would permit access to an individual's financial account; (iv) Medical or health insurance information; or (v) E-mail address with any required security code, access code, or password that would permit access to an individual's personal, medical, insurance, or financial account.	NA	NA	
South Carolina Breach Notification Law	S.C. Code § 39-1-90	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 1000 residents • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if the person demonstrates that the cost of providing notice exceeds two hundred fifty thousand dollars or that the affected class of subject persons to be notified exceeds five hundred thousand or the person has insufficient contact information. • Credit Monitoring: • Other:	$1,000 per resident for knowing or willful violation: S.C. Code § 39-1-90(H)	Attorney General: S.C. Code § 39-1-90(H)	
Unfair, Deceptive, or Abusive Acts and Practices	S.C. Code § 39-5-20	Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful.	Up to $5,000 per violation: S.C. Code § 39-5-110	Attorney General: S.C. Code § 39-5-110	
Definition of Personal Identifying Information	S.C. Code § 39-1-90(D)(3)	"Personal identifying information" means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of this State, when the data elements are neither encrypted nor redacted: (a) social security number; (b) driver's license number or state identification card number issued instead of a driver's license; (c) financial account number, or credit card or debit card number in combination with any required security code, access code, or password that would permit access to a resident's financial account; or (d) other numbers or information which may be used to access a person's financial accounts or numbers or information issued by a governmental or regulatory entity that uniquely will identify an individual. The term does not include information that is lawfully obtained from publicly available information, or from federal, state, or local governmental records lawfully made available to the general public.	NA	NA	
South Dakota Breach Notification Law	S.D. Codified Laws §§ 22-40-20 to 22-40-26	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 250 residents • Notify Credit Reporting Agencies: Yes • If not data owner, notify data owner: Yes • How many days to Notify: Within 60 days of breach discovery date. • Substitute Notice: Yes, if over 500,000 people or $250,000 • Credit Monitoring: • Other:	Up to $10,000 per day per violation: S.D. Codified Laws § 22-40-25	Attorney General: S.D. Codified Laws § 22-40-25	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Unfair, Deceptive, or Abusive Acts and Practices	S.D. Codified Laws § 37-24-6	"It is a deceptive act or practice for any person to: (1) Knowingly act, use, or employ any deceptive act or practice, fraud, false pretense, false promises, or misrepresentation or to conceal, suppress, or omit any material fact in connection with the sale or advertisement of any merchandise, regardless of whether any person has in fact been misled, deceived, or damaged thereby. . . "	Up to $2,000 per violation: S.D. Codified Laws § 37-24-27	Attorney General: S.D. Codified Laws § 37-24-23	
Definition of Personal Information	S.D. Codified Laws § 22-40-19(4)	"Personal information," a person's first name or first initial and last name, in combination with any one or more of the following data elements: (a) Social security number; (b) Driver license number or other unique identification number created or collected by a government body; (c) Account, credit card, or debit card number, in combination with any required security code, access code, password, routing number, PIN, or any additional information that would permit access to a person's financial account; (d) Health information as defined in 45 CFR 160.103; or (e) An identification number assigned to a person by the person's employer in combination with any required security code, access code, password, or biometric data generated from measurements or analysis of human body characteristics for authentication purposes. The term does not include information that is lawfully made available to the general public from federal, state, or local government records or information that has been redacted, or otherwise made unusable; and	NA	NA	
Definition of Protected Information	S.D. Codified Laws § 22-40-19(5)	"Protected information," includes: (a) A user name or email address, in combination with a password, security question answer, or other information that permits access to an online account; and (b) Account number or credit or debit card number, in combination with any required security code, access code, or password that permits access to a person's financial account;	NA	NA	
Tennessee Breach Notification Law	Tenn. Code § 47-18-2107	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes, within 45 of breach discovery date • How many days to notify: Within 45 day of breach discovery • Substitute Notice: Yes, if over 500,000 people or $250,000 • Credit Monitoring: No	civil penalty of whichever of the following is greater: ten thousand dollars ($10,000), five thousand dollars ($5,000) per day for each day that a person's identity has been assumed or ten (10) times the amount obtained or attempted to be obtained by the person using the identity theft.: Tenn. Code § 47-18-2105	Division of Consumer Affairs of the Department of Commerce and Insurance: Tenn. Code § 47-18-2105	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Personal Information Protection Act	Tenn. Code § 47-18-2110	On and after January 1, 2008, any person, nonprofit or for profit business entity in this state, including, but not limited to, any sole proprietorship, partnership, limited liability company, or corporation, engaged in any business, including, but not limited to, health care, that has obtained a federal social security number for a legitimate business or governmental purpose shall make reasonable efforts to protect that social security number from disclosure to the public.	civil penalty of whichever of the following is greater: ten thousand dollars ($10,000), five thousand dollars ($5,000) per day for each day that a person's identity has been assumed or ten (10) times the amount obtained or attempted to be obtained by the person using the identity theft.: TN ST § 47-18-2105	Division of Consumer Affairs of the Department of Commerce and Insurance: TN ST § 47-18-2105	
Unfair, Deceptive, or Abusive Acts and Practices	Tenn. Code § 47-18-104	The following unfair or deceptive acts or practices affecting the conduct of any trade or commerce are declared to be unlawful and in violation of this part:	Up to $1,000 per violation: TN ST § 47-18-108(b)(3)	Division of Consumer Affairs of the Department of Commerce and Insurance: TN ST § 47-18-108	
Definition of Personal Information	Tenn. Code § 47-18-2107(a)(4)	"Personal information": (A) Means an individual's first name or first initial and last name, in combination with any one (1) or more of the following data elements: (i) Social security number; (ii) Driver license number; or (iii) Account, credit card, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; and (B) Does not include information that is lawfully made available to the general public from federal, state, or local government records or information that has been redacted, or otherwise made unusable; and	NA	NA	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Texas Breach Notification Law	Tex. Bus. & Com. Code § 521.053	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 10,000 people • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay and in each case not later than the 60th day after the date on which the person determines that the breach occurred. • Substitute Notice: Yes, if: 500,000 people or $250,000 • Credit Monitoring: No	Between $2,000 and $50,000 per violation and up to $150,000 in additional penalties: Tex. Bus. & Com. Code § 521.151	Attorney General: Tex. Bus. & Com. Code § 521.151	Amended by 2019 Tex. Sess. Law Serv. Ch. 1326 (HB 4390): Privacy of Personal Identifying Information and the Creation of the Texas Privacy Protection Advisory Council - Disclosures of Data breach must be made without unreasonable delay and not later than the 60th day after the person determines a breach has occurred; person who finds the breach must notify the attorney general no later than 60 days after the breach is discovered and it effected at least 250 residents of Texas.
Personal Information Protection Act	Tex. Bus. & Com. Code § 521.052	"A business shall implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business."	Between $2,000 and $50,000 per violation: Tex. Bus. & Com. Code § 521.151	Attorney General: Tex. Bus. & Com. Code § 521.151	
Unfair, Deceptive, or Abusive Acts and Practices	Tex. Bus. & Com. Code § 17.45	"False, misleading, or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful and are subject to action by the consumer protection division. . ."	Up to $20,000 per violation: Tex. Bus. & Com. Code § 17.47	Consumer Protection Division, Attorney General: Tex. Bus. & Com. Code § 17.47	Amended by 2019 Tex. Sess. Law Serv. Ch. 759 (HB 1152): Deceptive Trade Practice of Charging Exorbitant or excessive prices for necessities during a declared disaster (focused primarily on building supplies).
Definition of Personal Identifying Information	Tex. Bus. & Com. Code § 521.002(a)(1)	"Personal identifying information" means information that alone or in conjunction with other information identifies an individual, including an individual's: (A) name, social security number, date of birth, or government-issued identification number; (B) mother's maiden name; (C) unique biometric data, including the individual's fingerprint, voice print, and retina or iris image; (D) unique electronic identification number, address, or routing code; and (E) telecommunication access device as defined by Section 32.51, Penal Code.	NA	NA	
Definition of Sensitive Personal Information	Tex. Bus. & Com. Code § 521.002(a)(2)	"Sensitive personal information" means, subject to Subsection (b): (A) an individual's first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted: (i) social security number; (ii) driver's license number or government-issued identification number; or (iii) account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account; or (B) information that identifies an individual and relates to: (i) the physical or mental health or condition of the individual; (ii) the provision of health care to the individual; or (iii) payment for the provision of health care to the individual. (b) For purposes of this chapter, the term "sensitive personal information" does not include publicly available information that is lawfully made available to the public from the federal government or a state or local government	NA	NA	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Utah Breach Notification Law	Utah Code § 13-44-202	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Not allowed • Credit Monitoring: No	Up to $100,000: Utah Code § 13-44-301	Attorney General: Utah Code § 13-44-301	Amendments effective May 14, 2019: 1. Provides that statute is not applicable to financial institutions 2. Provides for new notification requirement for residents who can't reached: you can announce in a newspaper of general circulation 3. Amends the penalties: there is no cap for fines if 10,000 or more consumers were effected and if the person effected settles on an amount larger than $100K 4. Statute of limitations for administrative action is 10 years after the day on which the data breach occurred; SOL for a civil action is 5 years 5. Provides for the ability to sue for treble damages 6. Creates an Attorney General Litigation fund for actions brought by the state and citizen education and outreach
Personal Information Protection Act	Utah Code § 13-44-201	"Any person who conducts business in the state and maintains personal information shall implement and maintain reasonable procedures to: (a) prevent unlawful use or disclosure of personal information collected or maintained in the regular course of business; and (b) destroy, or arrange for the destruction of, records containing personal information that are not to be retained by the person."	Up to $100,000: Utah Code § 13-44-301	Attorney General: Utah Code § 13-44-301	Amendments effective May 14, 2019: No longer a provision which states that this provision does not apply to a financial institution; the whole chapter does not apply to a financial institution as defined in 13-44-102
Unfair, Deceptive, or Abusive Acts and Practices	Utah Code § 13-11-5	"An unconscionable act or practice by a supplier in connection with a consumer transaction violates this act1 whether it occurs before, during, or after the transaction."	Up to $2,500 per violation (administrative fine): Utah Code § 13-11-17	Division of Consumer Protections: Utah Code § 13-11-17	
Definition of Personal Information	Utah Code § 13-44-102(4)	(a) “Personal information” means a person's first name or first initial and last name, combined with any one or more of the following data elements relating to that person when either the name or date element is unencrypted or not protected by another method that renders the data unreadable or unusable: (i) Social Security number; (ii)(A) financial account number, or credit or debit card number; and (B) any required security code, access code, or password that would permit access to the person's account; or (iii) driver license number or state identification card number. (b) “Personal information” does not include information regardless of its source, contained in federal, state, or local government records or in widely distributed media that are lawfully made available to the general public.	NA	NA	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Vermont Breach Notification Law	Vt. Stat. tit. 9 § 2435	• Notify Affected Residents: Yes • Notify Attorney General: Yes, within 14 business days of breach discovery • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 5,000 residents or $5,000 • Credit Monitoring: • Other:	Unclear from statute	Attorney General: Vt. Stat. tit. 9 § 2435(g)	Proposed changes: Feb. 19, 2019 - This bill proposes to create a chief privacy officer; to direct the State to conduct a privacy audit concerning the collection and use of citizens' data; to adopt a student online privacy protection act; to expand the definition of personally identifiable information subject to the Security Breach Notice Act and ensure consumer notice of a data breach; and to require internet service providers to provide notice concerning the potential sharing of private data. March 20, 2019 - The same bill above was engrossed in the Vermont Legislature.
Unfair, Deceptive, or Abusive Acts and Practices	Vt. Stat. tit. 9, § 2453	"Unfair methods of competition in commerce and unfair or deceptive acts or practices in commerce are hereby declared unlawful."	Up to $10,000 per violation: Vt. Stat. tit. 9, § 2461	Attorney General: Vt. Stat. tit. 9, § 2461	
Definition of Brokered Personal Information	Vt. Stat. tit. 9 § 2430(1)	(A) "Brokered personal information" means one or more of the following computerized data elements about a consumer, if categorized or organized for dissemination to third parties: (i) name; (ii) address; (iii) date of birth; (iv) place of birth; (v) mother's maiden name; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data; (vii) name or address of a member of the consumer's immediate family or household; (viii) Social Security number or other government-issued identification number; or (ix) other information that, alone or in combination with the other information sold or licensed, would allow a reasonable person to identify the consumer with reasonable certainty. (B) "Brokered personal information" does not include publicly available information to the extent that it is related to a consumer's business or profession.	NA	NA	
Definition of Personally Identifiable Information	Vt. Stat. tit. 9 § 2430(9)	(A) "Personally identifiable information" means a consumer's first name or first initial and last name in combination with any one or more of the following digital data elements, when either the name or the data elements are not encrypted or redacted or protected by another method that renders them unreadable or unusable by unauthorized persons: (i) Social Security number; (ii) motor vehicle operator's license number or nondriver identification card number; (iii) financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords; (iv) account passwords or personal identification numbers or other access codes for a financial account. (B) "Personally identifiable information" does not mean publicly available information that is lawfully made available to the general public from federal, State, or local government records.	NA	NA	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Virginia Breach Notification Law	Va. Code § 18.2-186.6	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 1000 residents • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 100,000 residents or $50,000 • Credit Monitoring: • Other: Special provisions for income tax data	Up to $150,000 per breach: Va. Code § 18.2-186.6(I)	Attorney General: Va. Code § 18.2-186.6(I)	Amended March 18, 2019 by HB 2396 - "Personal information" shall include passport number and military ID in addition to social security number, driver's license/ID number, and financial account numbers
Unfair, Deceptive, or Abusive Acts and Practices	Va. Code § 59.1-200	"The following fraudulent acts or practices committed by a supplier in connection with a consumer transaction are hereby declared unlawful . . ."	Up to $2,500 per violation: Va. Code § 59.1-206	Attorney General: Va. Code § 59.1-206	Amended by HB 2218 March 18, 2019 (unrelated to cyber security).
Definition of Personal Information	Va. Code § 18.2-186.6	"Personal information" means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted: 1. Social security number; 2. Driver's license number or state identification card number issued in lieu of a driver's license number; 3. Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts; 4. Passport number; or 5. Military identification number. The term does not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.	NA	NA	
Washington Breach Notification Law	Wash. Rev. Code § 19.255.010	• Notify Affected Residents: Yes • Notify Attorney General: Yes, if over 500 residents • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: No more than 30 days after the breach discovery • Substitute Notice: Yes, if over 500,000 residents or $250,000 • Credit Monitoring: • Other: Reimbursement from businesses to financial institutions provision	Up to $25,000: Wash. Rev. Code §§ 19.255.010(17), 19.86.140	Attorney General: Wash. Rev. Code § 19.255.010(17)	Changed 45 to 30 days notice. Passed Bill will be effective March 1, 2020. http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/House%20Passed%20Legislature/1071-S.PL.pdf
Unfair, Deceptive, or Abusive Acts and Practices	Wash. Rev. Code § 19.86.020	"Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."	Up to $25,000: Wash. Rev. Code § 19.86.140	Attorney General: Wash. Rev. Code § 19.86.080	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Definition of Personal Information	Wash. Rev. Code § 19.255.010	(i) An individual's first name or first initial and last name in combination with any one or more of the following data elements: (A) Social security number; (B) Driver's license number or Washington identification card number; (C) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account, or any other numbers or information that can be used to access a person's financial account; (D) Full date of birth; (E) Private key that is unique to an individual and that is used to authenticate or sign an electronic record; (F) Student, military, or passport identification number; (G) Health insurance policy number or health insurance identification number; (H) Any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer; or (I) Biometric data generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual; (ii) Username or email address in combination with a password or security questions and answers that would permit access to an online account; and (iii) Any of the data elements or any combination of the data elements described in (a)(i) of this subsection without the consumer's first name or first initial and last name if: (A) Encryption, redaction, or other methods have not rendered the data element or combination of data elements unusable; and (B) The data element or combination of data elements would enable a person to commit identity theft against a consumer. (b) Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.	NA	NA	
West Virginia Breach Notification Law	W.Va. Code § 46A-2A-102	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 100,000 residents or $50,000 • Credit Monitoring: No • Other:	Up to $5,000 per violation: W.Va. Code §§ 46A-2A-104, 46A-7-111	Attorney General: W.Va. Code § 46A-2A-104	
Unfair, Deceptive, or Abusive Acts and Practices	W. Va. Code § 46A-6-104	Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful."	Up to $5,000 per violation: W.Va. Code § 46A-7-111	Attorney General: W.Va. Code § 46A-7-111	
Definition of Personal Information	W. Va. Code § 46A-6-101(6)	"Personal information" means the first name or first initial and last name linked to any one or more of the following data elements that relate to a resident of this state, when the data elements are neither encrypted nor redacted: (A) Social security number; (B) Driver's license number or state identification card number issued in lieu of a driver's license; or (C) Financial account number, or credit card, or debit card number in combination with any required security code, access code or password that would permit access to a resident's financial accounts. The term does not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.	NA	NA	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Wisconsin Breach Notification Law	Wis. Stat. § 134.98	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Within 45 days of the breach discovery date • Substitute Notice: Yes, see statute • Credit Monitoring:	None	No one	
Unfair, Deceptive, or Abusive Acts and Practices	Wis. Stat. § 100.20	"Methods of competition in business and trade practices in business shall be fair. Unfair methods of competition in business and unfair trade practices in business are hereby prohibited."	From $100 to $10,000 per violation: Wis. Stat. § 100.26(6)	The Department of Agriculture, trade, and consumer protection: Wis. Stat. § 100.20	
Definition of Personal Information	Wis. Stat. § 134.98(1)(b)	"Personal information" means an individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable: 1. The individual's social security number. 2. The individual's driver's license number or state identification number. 3. The number of the individual's financial account number, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account. 4. The individual's deoxyribonucleic acid profile, as defined in s. 939.74(2d)(a). 5. The individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.	NA	NA	
Wyoming Breach Notification Law	Wyo. Stat. § 40-12-502	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, see statute • Credit Monitoring: No	Damages: Wyo. Stat. § 40-12-502	Attorney General: Wyo. Stat. § 40-12-502(f)	
Unfair, Deceptive, or Abusive Acts and Practices	Wyo. Stat. § 40-12-105	"A person engages in a deceptive trade practice unlawful under this act when, in the course of his business and in connection with a consumer transaction, he knowingly. . ."	Up to $5,000 per violation: Wyo. Stat. § 40-12-113	Attorney General: Wyo. Stat. § 40-12-113	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Definition of Personal Identifying Information	Wyo. Stat. § 40-12-501(a)(viii); Wyo. Stat. § 6-3-901(b)(iii)-(xiv)	"Personal identifying information" means the first name or first initial and last name of a person in combination with one (1) or more of the data elements specified in W.S. 6-3-901(b)(iii) through (xiv), when the data elements are not redacted; (iv) Driver's license number; (v) Account number, credit card number or debit card number in combination with any security code, access code or password that would allow access to a financial account of the person; (vi) Tribal identification card; (vii) Federal or state government issued identification card; (viii) Shared secrets or security tokens that are known to be used for data based authentication; (ix) A username or email address, in combination with a password or security question and answer that would permit access to an online account; (x) A birth or marriage certificate; (xi) Medical information, meaning a person's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; (xii) Health insurance information, meaning a person's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the person or information related to a person's application and claims history; (xiii) Unique biometric data, meaning data generated from measurements or analysis of human body characteristics for authentication purposes; (xiv) An individual taxpayer identification number.	NA	NA	
District of Columbia Breach Notification Law	D.C. Code § 28- 3852	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: Yes, if over 1000 residents • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 100,000 or $50,000 • Credit Monitoring: No	$100 per Affected Resident: D.C. Code § 28- 3853	US Attorney General: D.C. Code § 28- 3853	
Unfair, Deceptive, or Abusive Acts and Practices	D.C. Code § 28-3904	"It shall be a violation of this chapter, whether or not any consumer is in fact misled, deceived or damaged thereby, for any person to: . . ."	Up to $1000 per violation: D.C. Code § 28-3909	Corporation Counsel: D.C. Code § 28-3909	
Definition of Personal Information	D.C. Code § 28-3851(3)	(A) "Personal information" means: (i) An individual's first name or first initial and last name, or phone number, or address, and any one or more of the following data elements: (I) Social security number; (II) Driver's license number or District of Columbia Identification Card number; or (III) Credit card number or debit card number; or (ii) Any other number or code or combination of numbers or codes, such as account number, security code, access code, or password, that allows access to or use of an individual's financial or credit account. (B) For purposes of this paragraph, the term "personal information" shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.	NA	NA	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Guam Breach Notification Law	9 Guam Code § 48.30	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 5,000 residents or $10,000 • Credit Monitoring: No • Other:	Up to $150,000 per breach: 9 GCA § 48.50	The Attorney General: 9 GCA § 48.50	
Unfair, Deceptive, or Abusive Acts and Practices	5 Guam Code § 32201	False, misleading, or deceptive acts or practices, including, but not limited to those listed in this chapter, are hereby declared unlawful and are subject to action by the Attorney General or any person as permitted pursuant to this chapter or other provisions of Guam law. A violation consisting of any act prohibited by this title is in itself actionable, and may be the basis for damages, rescission, or equitable relief. The provisions of this chapter are to be liberally construed in favor of the consumer, balanced with substantial justice, and violation of such provisions may be raised as a claim, defense, crossclaim or counterclaim.	Up to $5,000 per violation: 5 GCA § 32127	Attorney General: 5 GCA § 32116	
Definition of Personal Information	9 Guam Code § 48.20(f)	Personal information means the first name, or first initial, and last name in combination with and linked to any one or more of the following data elements that relate to a resident of Guam, when the data elements are neither encrypted nor redacted: (1) Social Security number; (2)Driver's license number or Guam identification card number issued in lieu of a driver's license; or (3) Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts. (4) The term does not include information that is lawfully obtained from publicly available information, or from Federal, State, or local government records lawfully made available to the general public.	NA	NA	
Puerto Rico Breach Notification Law	P.R. Laws tit. 10 § 4052	• Notify Affected Residents: Yes • Notify the Secretary of Consumer Affairs: Yes, within 10 days • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 100,000 people or $100,000 • Credit Monitoring: No • Must make public announcement within 24 hours	Up to $5,000 per violation of the provisions of this chapter: 10 Laws of Puerto Rico § 4055	PR ST T. 10 § 4055	

Survey of Other States' Cyber Laws

Title or Description	Reference	Synopsis	Penalty	Enforcement	2019 Update
Unfair, Deceptive, or Abusive Acts and Practices	P.R. Laws Tit. 10 §259	Unfair methods of competition, and unfair or deceptive acts or practices in trade or commerce are hereby declared unlawful.	a civil penalty imposed by the Department of Consumer Affairs up to a maximum of five thousand dollars ($5,000). Each separate violation of said decision shall be considered as continuous noncompliance therewith, in which case, each day the decision is not complied with shall be considered as a separate violation. 10 Laws of Puerto Rico § 259	PR ST T. 10 § 259	
Definition of Personal Information File	P.R. Laws Tit. 10 § 4051(a)	Personal information file. Refers to a file containing at least the name or first initial and the surname of a person, together with any of the following data so that an association may be established between certain information with another and in which the information is legible enough so that in order to access it there is no need to use a special cryptographic code. (1) Social security number. (2) Driver's license number, voter's identification or other official l identification. (3) Bank or financial account numbers of any type with or without passwords or access code that may have been assigned. (4) Names of users and passwords or access codes to public or private information systems. (5) Medical information protected by the HIPAA. (6) Tax information. (7) Work-related evaluations. Neither the mailing nor the residential address is included in the protected information or information that is a public document and that is available to the citizens in general.	NA	NA	
Virgin Islands Breach Notification Law	V.I. Code tit. 14 § 2208	• Notify Affected Residents: Yes • Notify Attorney General: No • Notify Credit Reporting Agencies: No • If not data owner, notify data owner: Yes • How many days to Notify: Without unreasonable delay • Substitute Notice: Yes, if over 50,000 residents or $100,000 • Credit Monitoring: No • Other:	Actual damages: 14 V.I.C. § 2211	Private right of action: 14 V.I.C. § 2211	
Unfair, Deceptive, or Abusive Acts and Practices	V.I. Code tit. 12A § 101	No person shall engage in any deceptive or unconscionable trade practice in the sale, lease, rental or loan or in the offering for sale, lease, rental, or loan of any consumer goods or services, or in the collection of consumer debts.	Up to $5,000 per violation: V.I. Code tit. 12, § 104	The Commissioner: V.I. Code tit. 12, § 104	

Survey of Federal Cyber Laws

Date	Title	Subtitle	Reference	Information	2019 Update
1914	Executive Order 13571		15 U.S.C. § 45, et seq.	Gave the FTC the authority to enforce rules prohibiting "unfair or deceptive acts or practices in or affecting commerce."	
		FTC Section 5 Authority	15 U.S.C. § 45(a)(1), et seq.	The basic consumer protection statute enforced by the Commission is Section 5(a) of the FTC Act, which provides that "unfair or deceptive acts or practices in or affecting commerce…are…declared unlawful."	2006 amendment defines "unfair or deceptive acts or practices" to include acts or practices involving foreign commerce that "(i) cause or are likely to cause reasonably foreseeable injury within the United States; or (ii) involve material conduct occurring within the United States."
1966	Freedom of Information Act (FOIA) of 1966		5 U.S.C. § 552, et seq.	Under FOIA, "any person" may request "records" maintained by an executive agency. People or entities requesting records need not state a reason for requesting records. Today, all fifty states have freedom of information laws, many of which are based upon the FOIA.	The 2016 amendment added: •a requirement that agencies make information available to the public in an electronic, searchable, and downloadable format •when an agency may withhold information, which is only when (i) the agency reasonably foresees that disclosure would harm an interest protected by an exemption described in the statute; or (ii) disclosure is prohibited by law. The agency must also consider in these circumstances whether partial disclosure is warranted whenever full disclosure is not possible; the agency must take reasonable steps of segregate and release nonexempt information.
1968	Wiretap Act of 1968		18 U.S.C. § 2511, et seq.	Broadly prohibits the intentional interception, use, or disclosure of wire and electronic communications unless a statutory exception applies. In general, these prohibitions bar unauthorized third parties (including the government) from wiretapping telephones and installing electronic "sniffers" that read Internet traffic.	•The Electronic Communications Privacy Act of 1986 (ECPA) amended the Wiretap Act by extending to data and electronic transmissions the same protection afforded to oral and wire communications.
1968	Omnibus Crime and Control and Safe Streets Act of 1968		18 U.S.C. §§ 2510–22, et seq.	Extended the reach of wiretap regulations to state officials as well as to private parties. Despite its profound increase in the extent of protection, Title III had important limitations. It applied to the interception of "aural" communications; it did not apply to visual surveillance or other forms of electronic communication.	
1970	Fair Credit Reporting Act of 1970		15 U.S.C. § 1681, et seq.	The Fair Credit Reporting Act (FCRA) provides limited protections for individuals. It enables people to access their records, and restricts the manner in which records are disclosed. Individuals can challenge inaccuracies on their reports and can sue to collect damages for violations of the Act. However, FCRA immunizes creditors and credit reporting agencies from lawsuits for "defamation, invasion of privacy, or negligence" except when the information is "furnished with malice or willful intent to injure such consumer." Although the FCRA allows people to sue for negligent violations of the Act, there is a two-year statute of limitations "from the date on which the liability arises."	HR 3622 was introduced in the House of Representatives on July 5, 2019 to amend the Fair Credit Reporting Act "to restore the impaired credit of victims of predatory activities and unfair consumer reporting practices, to expand access to tools to protect vulnerable consumers from identity theft, fraud, or a related crime, and protect victims from further harm…"
1970	Racketeer Influenced and Corrupt Organizations (RICO) Act of 1970		118 U.S.C. ch. 96	Passed in 1970, the Racketeer Influenced and Corrupt Organizations Act (RICO) is a federal law designed to combat organized crime in the United States. It allows prosecution and civil penalties for racketeering activity performed as part of an ongoing criminal enterprise. Such activity may include illegal gambling, bribery, kidnapping, murder, money laundering, counterfeiting, embezzlement, drug trafficking, slavery, and a host of other unsavory business practices.	•Melanson v. US Forensic, LLC (2016): ED New York held the National Flood Insurance Program preempts RICO • In re Epogen & Aranesp Off-Label Marketing & Sales Practice Litigation (2008): CD California held specific representations that are literally false, misleading, or contain material omissions are actionable under RICO and not preempted by the FDCA
1970	Bank Secrecy Act of 1970		Pub. L. No. 91-508 12 U.S.C. §§ 1730(d), 1829b, 1951-59, et seq. 31 U.S.C. H9 1051-1122, et seq.	The Bank Secrecy Act, enacted in 1970, requires banks to retain records and create reports to help law enforcement investigations. The Act was passed due to concerns that the computerization of records would make white collar crime more difficult to detect. Federally insured banks must record the identities of account holders and maintain copies of each financial instrument. International transactions exceeding $5,000 are subject to reporting, as well as domestic transactions exceeding $10,000. In *California Bankers Ass'n v. Shultz* , 416 U.S. 21 (1974), the Supreme Court upheld the Act against a Fourth Amendment challenge by a group of bankers and account holders. The Court concluded that the bankers lacked Fourth Amendment rights in the data because "corporations can claim no equality with individuals in the enjoyment of a right to privacy." *Id* at 65. The account holders failed to allege that they engaged in transactions exceeding $10,000, and as a result, lacked standing.	•Title III of the USA Patriot Act amended the BSA to require financial institutions to establish anti-money-laundering programs by establishing internal policies, procedures, and controls, designating compliance officers, providing ongoing employee training, and testing programs through independent audits.
1974	Privacy Act of 1974		5 U.S.C. § 552a, et seq.	The Act responded to many of the concerns raised by the United States Department of Health Education and Welfare (HEW) report, "Records, Computers, and the Rights of Citizens." It regulates the collection and use of records by federal agencies, and affords individuals right to access and correct their personal information.	
1974	Family Educational Rights and Privacy Act of 1974		20 U.S.C. § 1232g, et seq.	The Family Educational Rights and Privacy Act of 1974 (FERPA), otherwise known as the "Buckley Amendment," regulates the accessibility of student records. FERPA does not apply to records maintained by school law enforcement officials or health and psychological records.	
1978	Protection of Pupil Rights Amendment ("PPRA") of 1978		20 U.S.C. § 1232h, et seq.; 34 C.F.R. part 98, et seq.	PPRA is a federal law that affords certain rights to parents of minor students with regard to surveys that ask questions of a personal nature. Briefly, the law requires that schools obtain written consent from parents before minor students are required to participate in any U.S. Department of Education funded survey, analysis, or evaluation that reveals information certain topics.	
1978	Foreign Intelligence Surveillance Act of 1978		50 U.S.C. §§ 1801–11, et seq.	The Foreign Intelligence Surveillance Act (FISA) of 1978, created a distinct regime for electronic surveillance to gather foreign intelligence. Whereas Title III regulated electronic surveillance for domestic law enforcement purposes, FISA applied when foreign intelligence gathering was "the purpose" of the investigation. FISA permits electronic surveillance and covert searches pursuant to court orders, which are reviewed ex parte by a special court of seven federal judges.	

Survey of Federal Cyber Laws

Date	Title	Subtitle	Reference	Information	2019 Update
1978	Right to Financial Privacy Act of 1978		29 U.S.C. § 3407, et seq.	The Right to Financial Privacy Act (RFPA) provided limited protection of financial records to fill the gap left by *United States v. Miller* , 425 U.S. 435, 435 (1976). Pursuant to the RFPA, government officials must use a warrant or subpoena to obtain financial information. There must be "reason to believe that the records sought are relevant to a legitimate law enforcement inquiry." Subject to certain exceptions, the customer must receive prior notice of the subpoena.	
1978	Airline Deregulation Act - Preemption of authority over prices, routes, and service		49 U.S.C.A. § 41713, et seq.	"[A] State, political subdivision of a State, or political authority of at least 2 States may not enact or enforce a law, regulation, or other provision having the force and effect of law related to a price, route, or service of an air carrier that may provide air transportation under this subpart."	Language is different from what is cited under the information column, the general rule reads: "Except as provided in subparagraph (B), a State, political subdivision of a State, or political authority of 2 or more States may not enact or enforce a law, regulation, or other provision having the force and effect of law related to a price, route, or service of an air carrier or carrier affiliated with a direct air carrier through common controlling ownership when such carrier is transporting property by aircraft or by motor vehicle (whether or not such property has had or will have a prior or subsequent air movement)." "Matters not covered: Subparagraph (A)-- (i) shall not restrict the safety regulatory authority of a State with respect to motor vehicles, the authority of a State to impose highway route controls or
1979	Drug Abuse Prevention, Treatment, and Rehabilitation Act of 1979		42 C.F.R. part 2, et seq.	Drug Abuse Prevention, Treatment, and Rehabilitation Act (Act) is a federal statute designed to be a practical resource for governments, policy planners, service commissioners and treatment providers against drug abuse. The Act makes provision for federal drug abuse programs and activities. The Act also provides for education, treatment, rehabilitation, research, training, and law enforcement efforts to prevent drug abuse.	Add to summary: The Act also provides for the confidentiality of substance use disorder patient records. Statutory Authority: 42 U.S.C.A. § 290dd-2; this statute has proposed legislation which strikes 'substance abuse' and inserts 'substance abuse disorder' Proposed Legislation: See "Overdose Prevention and Patient Safety Act" below
1980	Privacy Protection Act of 1980		42 U.S.C. § 2000aa, et seq.	Dissatisfaction over *Zurcher v. Stanford Daily* , 436 U.S. 547 (1978) led Congress to pass the Privacy Protection Act in 1980. The Act restricts the search or seizure of "any 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." As a result of the Act, a subpoena is needed to obtain work product materials, which permits the party to challenge the request in court and to produce the documents without having law enforcement officials intrude on the premises.	
1984	Cable Communications Policy Act of 1984		42 U.S.C. § 551, et seq.	The Cable Communications Policy Act (CCPA) of 1984 protects the privacy of cable records. Cable companies must notify subscribers about the collection and use of personal information. Companies cannot disclose a subscriber 's viewing habits. The Act is enforced with a private right of action.	
1986	Computer Fraud and Abuse Act of 1986		18 U.S.C. § 1030, et seq.	A United States cybersecurity bill that was enacted in 1986 as an amendment to existing computer fraud law (18 U.S.C. § 1030), which had been included in the Comprehensive Crime Control Act of 1984. The law prohibits accessing a computer without authorization, or in excess of authorization. The original 1984 bill was enacted in response to concern that computer-related crimes might go unpunished. The House Committee Report to the original computer crime bill characterized the 1983 techno-thriller film WarGames—in which a young Matthew Broderick breaks into a U.S. military supercomputer programmed to predict possible outcomes of nuclear war and unwittingly almost starts World War III—as "a realistic representation of the automatic dialing and access capabilities of the personal computer."	
1988	Computer Matching and Privacy Protection Act of 1988		5 U.S.C. § 552a(a)(8)–(13), (e)(12), (o)–(r), (u)), et seq.	A major loophole in the Privacy Act of 1974 has been the "routine use" exception. Under this exception, to detect fraud, the federal government in 1977 began running computer comparisons of employee records with the records of people receiving benefits. In 1988, Congress addressed this practice, known as "computer matching" by passing the Computer Matching and Privacy Protection Act. The law established procedures for computer matchings, but did not halt the practice.	Held unconstitutional as not severable in Texas v. United States, 340 F. Supp. 3d 579 (N.D. Tex. 2018).
1988	Employee Polygraph Protection Act of 1988		29 U.S.C. §§ 2001-09, et seq.	In 1988, Congress passed the Employee Polygraph Protection Act (EPPA). The EPPA prohibits private sector employers from using polygraph examinations on employees and prospective employees. The Act does not apply to public sector employers. Employers can, however, use polygraphs "in connection with an ongoing investigation involving economic loss or injury to the employer's business, such as theft, embezzlement, misappropriation, or an act of unlawful industrial espionage or sabotage" when "the employer has a reasonable suspicion that the employee was involved in the incident or activity under investigation." Private sector employers who provide security services are exempt.	
1988	Video Privacy Protection Act of 1988		18 U.S.C. § 2710(b), et seq.	The confirmation hearings of Supreme Court Justice nominee Robert Bork sparked a law to protect videocassette rental data. Reporters attempted to obtain a list of the videos Bork had rented from his video store. Incensed at this practice, Congress passed the Video Privacy Protection Act (VPPA) of 1988.251 The VPPA forbids videotape service providers from disclosing customer video rental or purchase information.	
1986	Electronic Communications Privacy Act of 1986		18 U.S.C. §§ 2510-22, 2701-11, 3121-27, et seq.	In 1986, Congress revisited its wiretapping law by substantially reworking Title III of 1968. The Electronic Communications Privacy Act (ECPA) expanded Title III to new forms of communications, with a particular focus on computers. The ECPA restricts the interception of transmitted communications and the searching of stored communications. Title I of the ECPA, known as the "Wiretap Act," regulates the interception of communications. Title II, referred to as the "Stored Communications Act," governs access to stored communications and records held by communications service providers (such as ISPs). Title III, called the "Pen Register Act," provides limited regulation of pen registers and trap and trace devices.	

Survey of Federal Cyber Laws

Date	Title	Subtitle	Reference	Information	2019 Update
1991	Telephone Consumer Protection Act of 1991		47 U.S.C. § 227, et seq.	In 1991, Congress enacted the Telephone Consumer Protection Act (TCPA), which permits people to request that telemarketers not call them again. If the telemarketer continues to call, people can sue for damages of up to $500 for each call.	47 USC § 227(b)(1)(A)(iii) debt-collection exception found unconstitutional in Duguid v. Facebook, Inc. (9th Circuit, 2019)
1993	Government Performance and Results Act of 1993		Pub. L. No. 103-62	Requires executive agency heads to submit to the Director of the Office of Management and Budget (OMB) and the Congress a strategic plan for performance goals of their agency's program activities. Requires such plan to cover at least a five-year period and to be updated at least every three years. See: https://www.congress.gov/bill/103rd-congress/senate-bill/20	
1994	Driver's Privacy Protection Act of 1994		18 U.S.C. §§ 2721-25, et seq.	In 1994, Congress passed the Driver 's Privacy Protection Act (DPPA), which requires that states first obtain a person's consent before disclosing her motor vehicle record information to marketers.	
1995	Paperwork Reduction Act (PRA) of 2005		44 U.S.C. § 3501, et seq.	Designed to reduce the public's burden of answering unnecessary, duplicative, and burdensome government surveys.	
1996	Health Insurance Portability and Accountability Act (HIPAA) of 1996		Pub. L. No. 104-191, 110 Stat. 1936	The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is the first federal statute to directly address health privacy. HIPPA required the Department of Health and Human Services (HHS) to draft regulations to protect the privacy of medical records. HHS's regulations, among other things, require that people authorize all uses and disclosures of their health information that are not for treatment, payment, or health care operation (such as for marketing purposes).	
		HIPAA Privacy Rule	45 C.F.R. part 160, et seq. and 45 C.F.R. part 164, subparts A and E, et seq.	The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.	
		HIPAA Security Rule	45 C.F.R. part 160 and 45 C.F.R. part 164, subparts A and C, et seq.	The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.	
		HIPAA Breach Notification Rule	45 CFR part 164, subpart D, et seq.	Requires HIPAA covered entities and their business associates to provide notification following a breach of unsecured protected health information.	
		Uses and disclosures for which an authorization or opportunity to agree or object is not required.	45 C.F.R. § 164.512, et seq.	Provides when covered entities or business associates are nor required to obtain valid authorization to use or disclose protected health information. General exceptions exist for public health activities.	
		Uses and disclosures to carry out treatment, payment, or health care operations.	45 C.F.R. § 164.506, et seq.	Provides when covered entities or business associates are nor required to obtain valid authorization to use or disclose protected health information. General exceptions exist for collection of payments for medical services.	
		Imposition of Civil Money Penalties	45 CFR, part 160, subpart D, et seq.	Provides guidelines for determining what amount an entity should be penalized for violating HIPAA.	
1996	Economic Espionage Act of 1996		18 U.S.C. §§ 1831-39, et seq.	This regulation is intended to protect from disclosure outside the government proprietary information that is provided to the government during a bidding process. Exemption 4 of the Freedom of Information Act exempts from mandatory disclosure information such as trade secrets and commercial or financial information obtained by the government from a company on a privileged or confidential basis that, if released, would result in competitive harm to the company, impair the government's ability to obtain like information in the future, or protect the government's interest in compliance with program effectiveness. The law on Disclosure of Confidential Information (18 U.S.C. § 1905) makes it a crime for a federal employee to disclose such information.	
1997	No Electronic Theft Act of 1997		Pub. L. No. 105-147	Provides for criminal prosecution of individuals who engage in copyright infringement under certain circumstances, even when there is no monetary profit or commercial benefit from the infringement.	

Survey of Federal Cyber Laws

Date	Title	Subtitle	Reference	Information	2019 Update
1998	Children's Online Privacy Protection Act of 1998		15 U.S.C. §§ 6501-06, et seq.	The Children's Online Privacy Protection Act (COPPA) of 1998 governs the collection of children's personal information on the Internet. The law only applies to children under the age of thirteen. Children's websites must post privacy policies and obtain "parental consent for the collection, use, or disclosure of personal information from "children." COPPA applies only to websites "directed to children" or where the operator of the website "has actual knowledge that it is collecting personal information from a child."	
1998	Digital Millennium Copyright Act (DMCA) of 1998		Pub. L. No. 105-304; 17 U.S.C. §§ 101, 104, 104A, 108, 112, 114, 117, 701, et seq.; 17 U.S.C. §§ 512, 1201–1205, 1301–1332, et seq.; 28 U.S.C. § 4001, et seq.	A U.S. copyright law that implements two 1996 treaties of the World Intellectual Property Organization (WIPO). It criminalizes production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works (commonly known as digital rights management or DRM). It also criminalizes the act of circumventing an access control, whether or not there is actual infringement of copyright itself. In addition, the DMCA heightens the penalties for copyright infringement on the Internet.	
1999	U.S. Uniform Computer Information Transactions Act (UCITA) of 1999 (Last Amended or Revised in 2002)		Uniform Laws Annotated. Uniform Computer Information Transactions Act (Last Amended or Revised in 2002)	UCITA provides a comprehensive set of rules for licensing computer information, whether computer software or other clearly identified forms of computer information. Computerized databases and computerized music are other examples of computer information that would be subject to UCITA. It would also govern access contracts to sites containing computer information, whether on or off the Internet. UCITA would also apply to storage devices, such as disks and CDs that exist only to hold computer information. Professional services by a member of a regulated profession (doctor, lawyer, accountant, for example) are not within UCITA even though communications about the transaction will be in the form of computer information.	
1999	The Gramm-Leach-Bliley Act of 1999		15 U.S.C. § 6802(a)-(b), et seq.	In 1999, Congress passed the Gramm-Leach-Bliley (GLB) Act, which allows financial institutions with different branches or affiliates engaging in different services to share the "nonpublic personal information" among each branch of the company. Affiliates must inform customers of the information sharing, but people have no right to stop the companies from sharing it. However, when financial institutions desire to share customer data with third parties, people have a right to opt-out.	
2000	Security and Exchange Commission ("SEC") Privacy of Consumer Financial Information Regulations of 2000		17 C.F.R. part 248, subpart A, et seq.	The SEC adopted Regulation S-P, privacy rules promulgated under section 504 of the Gramm-Leach-Bliley Act. Section 504 of GLBA required the Commission to adopt rules implementing notice requirements and restrictions on a financial institution's ability to disclose nonpublic personal information about consumers. The Regulation implements these requirements of the GLBA with respect to investment advisers registered with the Commission, brokers, dealers, and investment companies, which are the financial institutions subject to the Commission's jurisdiction under that Act.	
2000	U.S. Congress Electronic Signatures in Global National ("ESIGN") Commerce Act of 2000		Pub. L. No. 106–229, 15 U.S.C.A. § 7001	The ESIGN Act is a landmark federal law in the United States. Passed in 2000, it granted legal recognition to electronic signatures and records in the USA based on the understanding that if all parties to a contract choose to use electronic documents and to sign them electronically, they are legal. The ESIGN Act (along with its precursor UETA) provided the legal foundation for use of electronic records and electronic signatures in commerce. It confirmed that electronic records and signatures carry the same weight and have the same legal effect as traditional paper documents and wet ink signatures.	Added 15 U.S.C.A. § 7001 under reference
2001	The U.S. Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act of 2001		Pub. L. No. 107-56	In a very short time after the September 11 terrorist attack, Congress passed the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act" (USA PATRIOT Act) of 2001. The Act made several significant changes to the ECPA and FISA, among other statutes. In one amendment, the USA PATRIOT Act enlarged the definition of pen registers and trap and trace devices to apply to addressing information on emails and to "IP addresses." The Act also provided for new justifications for delayed notice of search warrants, increasing the types of subscriber records that could be obtained from ISPs and communications providers, and allowing for a nationwide scope for pen register orders and search warrants for email. The Act also provided for roving wiretaps under FISA as well as increased sharing of foreign intelligence information between law enforcement entities.	

Survey of Federal Cyber Laws

Date	Title	Subtitle	Reference	Information	2019 Update
2002	Confidential Information Protection and Statistical Efficiency Act (CIPSEA) of 2002		44 USCA § 101, TITLE V—CONFIDENTIAL INFORMATION PROTECTION AND STATISTICAL EFFICIENCY, PUBLIC LAW 107-347	CIPSEA establishes uniform confidentiality protections for information collected for statistical purposes by U.S. statistical agencies, and it allows some data sharing between the Bureau of Labor Statistics, Bureau of Economic Analysis, and Census Bureau. The agencies report to OMB on particular actions related to confidentiality and data sharing. The law give the agencies standardized approaches to protecting information from respondents so that it will not be exposed in ways that lead to inappropriate or surprising identification of the respondent. By default the respondent's data is used for statistical purposes only. If the respondent gives informed consent, the data can be put to some other use.	added PUBLIC LAW 107-347 and TITLE V—CONFIDENTIAL INFORMATION PROTECTION AND STATISTICAL EFFICIENCY,
2002	Sarbanes-Oxley Act ("SOX") of 2002		15 U.S.C. ch. 2A, 98, et seq., Public Law 107-204	SOX protects shareholders and the general public from accounting errors and fraudulent practices of organizations. It imposes criminal penalties for misleading shareholders and altering documents to impede an investigation. Sarbanes-Oxley also established an oversight board for the accounting profession, regulates the relationship between corporations and accounting firms, and shields corporate whistleblowers from retaliation. It was tailored to improve the accuracy of corporate disclosures. SOX compliance has recently shifted to include cybersecurity.	Added: imposes criminal penalties for misleading shareholders and altering documents to impede an investigation. Sarbanes-Oxley also established an oversight board for the accounting profession, regulates the relationship between corporations and accounting firms, and shields corporate whistleblowers from retaliation; AND Public Law 107-204 in reference
2002	E-Government Act of 2002		44 U.S.C. § 3501, et seq.,	Established procedures to ensure the privacy of personal information in electronic records. Section 208 of the E-Government Act of 2002 requires agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. PIAs must be made publicly available, unless the agency determines not to make the PIA publicly available if such publication would raise security concerns, reveal classified (i.e., national security), or reveal sensitive information (e.g., potentially damaging to a national interest, law enforcement effort, or competitive business interest).	
2002	The Homeland Security Act of 2002		6 U.S.C. § 222, et seq. 6 U.S.C.A. Ch. 6, Refs & Annos - EXECUTIVE ORDER NO. 13800. 6 U.S.C. ch. 1 § 101	In 2002, Congress passed the Homeland Security Act, which created the Department of Homeland Security (DHS), consisting of twenty-two federal agencies. The Act created a Privacy Office for ensuring compliance with privacy laws. Executive Order was published in May of 2017 to strengthen the cybersecurity of Federal networks and infrastructure.	added 6 U.S.C.A. Ch. 6, Refs & Annos - EXECUTIVE ORDER NO. 13800 and information on the executive order
2002	Federal Information Security Management Act ("FISMA") of 2002		44 U.S.C. § 3551, et seq. 44 U.S.C. § 3541, et seq.	FISMA is United States legislation that defines a comprehensive framework to protect government information, operations and assets against natural or man-made threats. FISMA assigns responsibilities to various agencies to ensure the security of data in the federal government. The act requires program officials, and the head of each agency, to conduct annual reviews of information security programs, with the intent of keeping risks at or below specified acceptable levels in a cost-effective, timely and efficient manner.	
2003	Do-Not-Call Implementation Act (National Do-Not-Call Registery) of 2003		15 U.S.C. ch. 87-87A, et seq. 15 U	In an effort to address unwanted telemarketing calls, the Federal Trade Commission (FTC) and the Federal Communications Commission (FCC) created a do-not-call registry. People can voluntarily register their telephone numbers, and commercial telemarketers are prohibited from calling the numbers. Telemarketers challenged the do-not-call registry as a violation of their First Amendment rights. In 2004, a federal circuit court concluded in *Mainstream Marketing Services, Inc. v. Federal Trade Commission* , 358 F.3d 1228 (10th Cir. 2004) that the do-not-call registry satisfied the *Central Hudson Gas & Elec. Corp. v. Public Service Commission of New York* , 447 U.S. 557 (1980) balancing test for commercial speech and therefore did not run afoul of the First Amendment.	
2003	The CAN-SPAM Act of 2003		15 U.S.C. § 7701, et seq.	The Act establishes requirements for those who send unsolicited commercial email. The Act bans false or misleading header information and prohibits deceptive subject lines. It also requires that unsolicited commercial email be identified as advertising and provide recipients with a method for opting out of receiving any such email in the future. In addition, the Act directs the FTC to issue rules requiring the labeling of sexually explicit commercial email as such and establishing the criteria for determining the primary purpose of a commercial email.	
2003	The Fair and Accurate Credit Transactions Act of 2003		Pub. L. No. 108-159, 117 Stat. 1952, codified to 15 U.S.C. §§ 1681-1681x	In 2003, Congress passed the Fair and Accurate Credit Transactions Act (FACTA), which amended the Fair Credit Reporting Act and extended its preemption on certain state law provisions addressing identity theft and credit reporting. Among other things, the FACTA provided some limited protections against identity theft. For example, FACTA requires credit reporting agencies to provide people with a free credit report each year. It requires credit reporting agencies to disclose to a consumer her credit score, and it allows victims of fraud to alert just one credit reporting agency, which then must notify the others. These provisions and others were criticized by many as not going far enough to address the problem of identity theft.	
2004	The Intelligence Reform and Terrorism Prevention Act of 2004		Pub. L. No. 108-458. 50 U.S.C. ch. 15 § 401 et seq.	In 2004, Congress passed the Intelligence Reform and Terrorism Prevention Act to facilitate greater information sharing between federal agencies. The Act requires that intelligence be "provided in its most shareable form" and it aims to "promote a culture of information sharing.	
2005	The Real ID Act of 2005		Pub. L. No. 109-13. 8 U.S.C. ch. 12, subch. I § 1101 et seq.	Attached to a military spending bill, and passed without debate, the Real ID Act of 2005 mandated that state driver 's licenses meet federal standards set forth by the DHS. Critics claimed that it would establish a de facto national identification card and that it would be extremely costly for the states to implement.	Amended by PL 115–323 [HR 3398]. An Act To amend the Real ID Act of 2005 to permit Freely Associated States to meet identification requirements under such Act, and for other purposes. SEC. 2. AMENDMENT. (a) DEFINITION OF STATE.—Section 201(5) of the Real ID Act of 2005 (49 U.S.C. 30301 note; Public Law 109–13) is amended by striking "the Trust Territory of the Pacific Islands,". (b) EVIDENCE OF LAWFUL STATUS.—Section 202(c)(2)(B) of the REAL ID Act of 2005 (49 U.S.C. 30301 note; Public Law 109–13) is amended—

Survey of Federal Cyber Laws

Date	Title	Subtitle	Reference	Information	2019 Update
2006	U.S. SAFE WEB Act of 2006		Pub. L. No. 109-455, 120 Stat. 3372, extended by Pub. L. No. 116-173, 134 Stat. 837, codified at 15 U.S.C. §§ 41 et seq.	This Act, amending the FTC Act of 1914, provides the FTC with a number of tools to improve enforcement regarding consumer protection matters, particularly those with an international dimension, including increased cooperation with foreign law enforcement authorities through confidential information sharing and provision of investigative assistance. The Act also allows enhanced staff exchanges and other international cooperative efforts.	
2007	Open Government Act of 2007		Public Law No. 110-175; 5 U.S.C. § 552, et seq.	Promotes accessibility, accountability, and openness in Government by strengthening 5 U.S.C. § 552 and codifies several provisions of Executive Order 13,392, "Improving Agency Disclosure of Information."	
2007	The Freedom of Information Act (FOIA) of 2007		5 U.S.C. § 552, et seq.	Amended Freedom of Information Act (FOIA) of 1966. Provides that any person has a right, enforceable in court, to obtain access to federal agency records, except to the extent that such records (or portions of them) are protected from public disclosure by one of nine exemptions or by one of three special law enforcement record exclusions.	
2008	Genetic Information Nondiscrimination Act ("GINA") of 2008		42 U.S.C.A. §§ 2000ff - 2000ff(11), et seq. Pub.L. 110–233	GINA protects individuals against discrimination based on their genetic information in health coverage and in employment. GINA is divided into two sections, or Titles. Title I of GINA prohibits discrimination based on genetic information in health coverage. Title II of GINA prohibits discrimination based on genetic information in employment.	
2009	Health Information Technology for Economic and Clinical Health Act ("HITECH Act")		42 C.F.R. parts 412, 413, 422, and 495, et seq. Pub.L. 111–5.	Promotes the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.	Multiple edits were made to 42 C.F.R. parts 412, 413, 422, and 495 by 83 FR 41144-01, 2018 WL 3918164(F.R.) that were effective Oct. 1, 2018.
		Access to systems and records.	42 C.F.R. § 495.346, et seq.	"The State agency must allow HHS access to all records and systems operated by the State in support of this program, including cost records associated with approved administrative funding and incentive payments to Medicaid providers. State records related to contractors employed for the purpose of assisting with implementation or oversight activities or providing assistance, at such intervals as are deemed necessary by the Department to determine whether the conditions for approval are being met and to determine the efficiency, economy, and effectiveness of the program."	
		Combating fraud and abuse.	42 C.F.R. § 495.368, et seq.	"(a) General rule. (1) The State must comply with Federal requirements to— (i) Ensure the qualifications of the providers who request Medicaid EHR incentive payments; (ii) Detect improper payments; and (iii) In accordance with § 455.15 and § 455.21 of this chapter, refer suspected cases of fraud and abuse to the Medicaid Fraud Control Unit. (2) The State must take corrective action in the case of improper EHR payment incentives to Medicaid providers."	
2010	Government Performance and Results Modernization (GPRM) Act of 2010 (Amends the Government Performance and Results Act of 1993)		Pub. L. No. 111-352 (Amends the Government Performance and Results Act of 1993)	Amends the Government Performance and Results Act of 1993 to require each executive agency to make its strategic plan available on its public website on the first Monday in February of any year following that in which the term of the President commences and to notify the President and Congress. Requires such plan to cover at least a four-year period and to include a description of how the agency is working with other agencies to achieve its goals and objectives, as well as relevant federal government priority goals. Requires the Director of the Office of Management and Budget (OMB) to coordinate with agencies to develop a federal government performance plan, which shall be submitted with the annual federal budget and concurrently made available on an OMB website of agency programs. Requires such plan to: (1) establish government performance goals for the current and next fiscal years; (2) identify activities, entities, and policies contributing to each goal; (3) identify a lead government official responsible for coordinating efforts to achieve the goal; (4) establish common federal government performance indicators with quarterly targets; (5) establish clearly defined quarterly milestones; and (6) identify major management challenges and plans to address such challenges.	
2014	Federal Information Security Modernization Act of 2014		44 U.S.C. § 3541, et seq. Pub.L. 1	This Act amends the Federal Information Security Management Act of 2002, 44 U.S.C. § 3541, and requires agencies to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of an agency.	
2017	Social Security Number Fraud Prevention Act of 2017		Pub. L. No. 115-59. 5 U.S.C. 551. 31 U.S.C. 901	This Act: (1) prohibits federal agencies from including any individual's Social Security account number on any document sent by mail unless the agency head determines that such inclusion is necessary; and (2) requires agencies that have Chief Financial Officers to issue regulations, within five years of this bill's enactment, that specify the circumstances under which such inclusion is necessary.	

Survey of Federal Cyber Laws

Date	Title	Subtitle	Reference	Information	2019 Update
2017	The Protecting Patient Access to Emergency Medications Act of 2017		21 U.S.C. § 823, et seq. Public Law No: 115-83.	In 1970, the Controlled Substances Act (CSA) was created to regulate substances that have the potential to be abused. At the time, the CSA lacked instructions for the maintenance and use of these substances by emergency medical services (EMS). States, therefore, created their own EMS-related controlled substances requirements. In 2017, the Protecting Patient Access to Emergency Medications Act (PPAEMA) was introduced in the United States Congress to amend the CSA to include EMS requirements and end confusion among states and EMS agencies.	
2018	Defense Federal Acquisition Regulation Supplement ("DFARS")		48 C.F.R. § 201.104, et seq.	DFARS Safeguarding riles and clauses, for the basic safeguarding of contractor information systems that process, store or transmit Federal contract information. DFARS provides a set of "basic" security controls for contractor information systems upon which this information resides. These security controls must be implemented at both the contractor and subcontractor levels based on the information security guidance in NIST Special Publication 800-171 "Protecting Controlled Unclassified Information in Non-Federal Information Systems and Organizations."	

FEDERAL AGENCY POLICIES

Date	Title	Subtitle	Reference	Information
1973	Organization of Economic Cooperation and Development (OECD) Fair Information Practices		U.S. Department of Health, Education, and Welfare, Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Comm. On Automated Personal Data Systems 29 (1973)	The OCED Fair Information Practices were articulated by the United States Department of Health Education and Welfare (HEW) in 1973. HEW investigated the issues with increasing computerization of information and growing depositories of personal data. The report recommended the page of a code of Fair Information Practices, which were later codified in the Privacy Act of 1974. The recommended practices included the following: 1. There must be no personal data record-keeping systems whose very existence is secret. 2. There must be a way for an individual to find out what information about him is in a record and how it is used. 3. There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent. 4. There must be a way for an individual to correct or amend a record of identifiable information about him. 5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.
1980	Organization of Economic Cooperation and Development (OECD) Privacy Guidelines		Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available in Marc Rotenburg, Privacy Law Sourcebook (2002)	The OECD Privacy Guidelines built upon the Fair Information Practices articulated by the United States Department of Health Education and Welfare (HEW). The OECD Guidelines contain eight principles: (1) collection limitation—data should be collected lawfully with the individual's consent; (2) data quality—data should be relevant to a particular purpose and be accurate; (3) purpose specification—the purpose for data collection should be stated at the time of the data collection and the use of the data should be limited to this purpose; (4) use limitation—data should not be disclosed for different purposes without the consent of the individual; (5) security safeguards—data should be protected by reasonable safeguards; (6) openness principle—individuals should be informed about the practices and polices of those handling their personal information; (7) individual participation—people should be able to learn about the data that an entity possesses about them and to rectify errors or problems in that data; (8) accountability—the entities that control personal information should be held accountable for carrying out these principles.

Survey of Institutions

Title	Information	URL	2019 Update
Cloud Security Alliance	Offers a number of certifications including: CSA Security, Trust & Assurance Registry (STAR) Certificate of Cloud Security Knowledge (CCSK) Certified Cloud Security Professional (CCSP) Global Consultancy Program	https://cloudsecurityalliance.org/	
Commission on Accreditation for Law Enforcement Agencies ("CALEA")	CALEA is intended to preserve the ability of law enforcement agencies to conduct electronic surveillance while protecting the privacy of information outside the scope of the investigation. It requires that telecommunications carriers and manufacturers of telecommunications equipment design their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities to comply with legal requests for information.	http://www.calea.org/	
Control Objectives for Information and Related Technologies ("COBIT")	COBIT 5 is the only business framework for the governance and management of enterprise IT. COBIT 5 integrates other major frameworks, standards and resources, including ISACA's Val IT and Risk IT, Information Technology Infrastructure Library (ITIL®) and related standards from the International Organization for Standardization (ISO).	http://www.isaca.org/Knowledge-Center/COBIT/Pages/Overview.aspx	
Federal Energy Regulatory Commission (FERC) Revised Critical Infrastructure Protection (CIP) Reliability Standards	NERC, which FERC has certified as the nation's Electric Reliability Organization, developed Critical Infrastructure Protection (CIP) cyber security reliability standards. On January 18, 2008, the Commission issued Order No. 706, the Final Rule approving the CIP reliability standards, while concurrently directing NERC to develop significant modifications addressing specific concerns. In January 2016, FERC issued a Final Rule revising the CIP reliability standards. Docket No. RM15-14-000. As of December 2017, FERC release a Notice of Proposed Rulemaking to direct NERC to develop and submit modifications to improve mandatory reporting of Cyber Security Incidents. [Docket Nos. RM18-2-000 and AD17-9-000.	https://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity.asp	

Survey of Institutions

Title	Information	URL	2019 Update
Federal Financial Institutions Examination Councils ("FFIEC")	The Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB) and to make recommendations to promote uniformity in the supervision of financial institutions. Guidance includes: Online Banking: https://www.ffiec.gov/pdf/authentication_guidance.pdf FFIEC Cybersecurity Assessment Tool: https://www.ffiec.gov/cyberassessmenttool.htm	https://www.ffiec.gov/	
Health Insurance Trust Alliance (HITRUST) CSF	HITRUST CSF is a certifiable framework that provides organizations with a comprehensive, flexible and efficient approach to regulatory compliance and risk management.	https://hitrustalliance.net/hitrust-csf/	
Indiana Department of Financial Institutions (DFI)	Enforces FFIEC standards.	https://www.in.gov/dfi/	
Indiana State Insurance Commissioners Navigators and Application Organizations		https://www.in.gov/idoi/	
International Organization for Standardization ("ISO")	ISO creates documents that provide requirements, specifications, guidelines or characteristics that can be used consistently to ensure that materials, products, processes and services are fit for their purpose.	https://www.iso.org/home.html	
ISA/IEC 62443 (ISA99)	The ISA-99/IEC 62443 standard is the worldwide standard for security of the Industrial Control Systems in the Operational Technology (OT) domain of organizations. The standard was created by the International Society of Automation, a leading worldwide nonprofit organization. The standard offers organizations handles to improve the digital security and safety of their process and SCADA environments.	https://www.isa.org/isa99/	

Survey of Institutions

Title	Information	URL	2019 Update
National Institute of Standards and Technology ("NIST")	NIST is a measurement standards laboratory, and a non-regulatory agency of the United States Department of Commerce.	https://www.nist.gov/	
North American Electric Reliability Corporation ("NERC")	The North American Electric Reliability Corporation (NERC) is a not-for-profit international regulatory authority whose mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid. NERC develops and enforces Reliability Standards; annually assesses seasonal and long-term reliability; monitors the bulk power system through system awareness; and educates, trains, and certifies industry personnel.	https://www.nerc.com/Pages/default.aspx	
PCI Security Standards Council	Helps merchants and financial institutions understand and implement standards for security policies, technologies and ongoing processes that protect their payment systems from breaches and theft of cardholder data. Also helps vendors understand and implement standards for creating secure payment solutions.	https://www.pcisecuritystandards.org/	
SSAE-18/ ISAE 3402	ISAE 3402 was developed to provide an international assurance standard for allowing public accountants to issue a report for use by user organizations and their auditors (user auditors) on the controls at a service organization that are likely to impact or be a part of the user organization's system of internal control over financial reporting.	https://www.ssae-16.com/soc-1-report/the-ssae-18-audit-standard/	

Survey of International Cyber Laws

Title	Country	Information	Applies to	Notes	Clerk Notes
China Cybersecurity Law (CSL)	CHINA	CSL regulates the construction, operation, maintenance and use of networks, as well as network security supervision and management within mainland China. The Cyberspace Administration of China (CAC) is the primary governmental authority supervising and enforcing the CSL.	China	New provisions made to China's Cybersecurity Law last November gives state agencies the legal authority to remotely conduct penetration testing on any internet-related business operating in China, and even copy and later share any data government officials find on inspected systems. https://www.zdnet.com/article/chinas-cybersecurity-law-update-lets-state-agencies-pen-test-local-companies/	Added the whole notes section.
Network and Information Systems Regulations of 2018 (NIS Regulations)	UK	NIS directive was put into place 5/10/2018. The directive increases cyber-security, while also providing members of EU the opportunity to be flexible in containing more or less restrictions than expected by the Directive. 3 important elements of the directive: 1. National Capabilities (set of requirements i.e. national CSIRT) 2. Cross Border Collaborations 3. National supervision of Critical Sectors https://theprivacyreport.com/2019/01/16/the-uks-new-cybersecurity-regulations-what-u-s-tech-companies-need-to-know/. https://www.enisa.europa.eu/topics/nis-directive. https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection	United Kingdom	On 6 December 2020, the EU Commission published its proposal for a Directive on Security of Network and Information Systems (NIS 2 Directive). The NIS2 Directive is designed to update the current NIS Directive. The proposal for the NIS2 Directive will be subject to negotiations between the EU Council and the EU Parliament and, once it is adopted, Member States will have to transpose the NIS2 Directive within 18 months.	Added the whole information section.
General Data Privacy Regulation (GDPR)	EUROPEAN UNION	The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy. https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection	Countries that belong to the EEA include EU + 3. Austria, Belgium, Bulgaria, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden. Non-EU countries in the EEA Norway, Iceland, Liechtenstein	While GDPR is in place as law, there is not yet specific country by country adoption of laws to align or go stricter than GDPR. It should be expected that Germany, France and Spain will go above and beyond the standard GDPR language and add more provisions. [CLERK ADDED SECTION]: Countries that are not a part of the EU, but process EU information must also comply to the GDPR/NIS Directive. Otherwise, there is potential for an up to 4% penalty of the international company's global annual revenue. See https://gov-relations.com/itar/	Added section to notes. Deleted UK from the EU list (pending Brexit - continue to monitor).
NIS Directive	EUROPEAN UNION	Enforced by NIS Regulation	Countries that belong to the EEA include EU + 3. Austria, Belgium, Bulgaria, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden. Non-EU countries in the EEA Norway, Iceland, Liechtenstein	On 16.12.2020, the European Commission presented a proposal for a Directive on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). This proposal aims to replace and further develop the NIS Directive.	Updated information section, deleted UK (pending Brexit - continue to monitor).
International Traffic in Arms Regulations (ITAR)	UNITED STATES	A United States regulatory regime to restrict and control the export of defense and military related technologies to safeguard U.S. national security and further U.S. foreign policy objectives ITAR is the International Traffic in Arms Regulations and requires, in part, that defense-related articles and technical data listed on the United States Munitions List USML only be shared with U.S. citizens absent special authorization or exemption. Furthermore, ITAR is a set of standards that deals with information security involving any parties that handle technical data related to the manufacturing	U.S. Government	While this act is set to ensure the safety of highly classified information, 'US persons' does not exclusively mean US citizens i.e. Clifford Chance (Law Firm) was subject to a $132,000 fine for excluding non/dual citizens from receiving authorized exports. See http://exportcompliancesolutions.com/blog/2018/09/20/u-s-persons-include-just-citizens/	Added the whole notes section.

Survey of International Cyber Laws

Title	Country	Information	Applies to	Notes	Clerk Notes
Encryption and Export Administration Regulations (EAR)	United States	The Export Administration Regulations (EAR) is a set of US government regulations on the export and import of most commercial items. The U.S. Department of Commerce is responsible for implementing and enforcing EAR. Specifically, working with items deemed dual-use and having both commercial and military applications. In particular, encryption or Cryptographic Information Security	U.S. Government	EAR is used for some items that do not qualify under the specified lists of ITAR (considered 'dual use') but may also be useful in civilian or military purposes	Added in the whole Notes section.
Privacy Act 1988	Australia	The Privacy Act includes thirteen Australian Privacy Principles (APPs). The APPs set out standards, rights and obligations for the handling, holding, use, accessing and correction of personal information (including sensitive information).	Australia	Sensitive information includes information regarding not just facts, but opinions regarding persons or readily identifiable persons. See https://www.oaic.gov.au/privacy-law/. https://www.apnews.com/f7055883421c4082a0d8bbb	Added in the whole Notes section.
Anti-Encryption Act	Australia	The Anti-Encryption Act forces corporations i.e. Google to disable encryptions protection to better allow police officials to stay alert. Implementation of the unprecedented law is controversial since many believe its undermining global privacy. The encryptions are also protected under cryptography. See https://fee.org/articles/australia-s-unprecedented-encryption-law-is-a-threat-to-global-privacy/	Australia		Added row
Information Technology Amendment Act and the Information Act	India	India is not a part of any convention on protection of personal data that is equivalent to the GDPR. India has adopted other international declarations and conventions including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, these acts recognize the right to privacy. The Supreme Court of India recognized the right to privacy as a fundamental right under the Indian Constitution in 2017. Privacy and data is protected by Information Technology Amendment Act and the Information Act.	India		Added the last two sentences to the "information" section. See https://www.opengovasia.com/the-current-state-of-cyber-security-in-india/
European Union (EU)-Japan Economic Partnership Agreement (EPA)	Japan	European Union (EU) Japan Economic Partnership Agreement (EPA) is a reciprocal adequacy arrangement that established the equivalence of the EU's General Data Protection Regulation (GDPR) and Japan's Act on the Protection of Personal Information (APPI) and enabling cross-border data transfers between the two. Japan was previously not included in the EU's 'whitelist' of countries considered as having adequate levels of personal data protection.	EU and Japan	The agreement became effective on Feb. 1st, 2019. It has allowed for easier transfer of private information between the two and has now initiated Japan as the 1st G7 nations to be included. This eliminated the need for clauses and contractual agreements. See ://iapp.org/news/a/gdpr-matchup-japans-act-on-the-	Added the whole notes section.
1. Personal Data Law 2. Data Localization Plan	Russia	In 2014, Russia adopted personal data localization rules. These rules required all operators that collect and process Russian citizens personal data to use databases located in Russia. These requirements apply to the personal data of all Russian citizens, regardless of their relation with the company. The new rules do not cross-border transfer of personal data. However, the requirement for primary data processing via Russian databases is considered to be onerous.	Russia	Data Localization Plans now backed with big fines. https://www.jdsupra.com/legalnews/data-localization-in-russia-now-backed-18981/	
Personal Information Protection and Electronic Documents Act (PIPDEA)	Canada	Canada has adequacy with the EU and GDPR (as of the launch of GDPR) based on the PIPDEA law that covers data privacy in Canada. In general, Canada privacy is sufficient. However, organizations in British Columbia and Nova Scotia that do businesses with quasi-governmental entities such as banks & transportation are subject to FIPPA, especially article 30, which prohibits transfer of data outside of Canada. PIPDEA laws regard the requirements necessary for private-sector commercial activities. Individual consent must be obtained for the collection, use, and disclosure of any personal information, and must also be used in the manner it was intended for. Also, if a province has laws that are deemed 'substantially similar' to PIPDEA, a class of organizations or activities can be exempt.https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/	Canada		Added in the whole line