APPENDIX TO *NOT SO PRIVATE*

STACEY A. TOVINO

71 DUKE L.J. (FEBRUARY 2022)

(State authorities are listed in alphabetical order followed by federal authorities)

Alabama. The Alabama Data Breach Notification Act (Alabama Act) protects "sensitive personally identifying information," defined as "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." The Alabama Act does not protect 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." ALA. CODE § 8-38-2(6) (pdf).

Alaska. The Alaska Breach of Security Involving Personal Information Act (Alaska Act) protects "personal information," defined as "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 … mean[ing] 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 … [defined as] 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." ALASKA STAT. § 45.48.090(7) (pdf).

Arizona. The Arizona Data Security Breaches Act (Arizona Act) protects "personal information," defined as either of the following: (i) An individual's first name or first initial and last name in combination with one or more specified data elements; or (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. The Arizona Act defines "specified data element" to include an individual's health insurance identification number, "[i]nformation about an individual's medical or mental health treatment or diagnosis by a health care professional," and "'[u]nique biometric data generated from a measurement or analysis of human body characteristics to authenticate an individual when the individual accesses an online account." The Arizona Act defines "redact" as "to alter or truncate a number so that not more than the last four digits are accessible and at least two digits have been removed." The Arizona Act does not require breach notification in breach cases involving "redacted "personal information. The Arizona Act also does not protect "publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media." ARIZ. REV. STAT. § 18-551 (pdf).

Arkansas. The Arkansas Personal Information Protection Act (Arkansas Act) protects "personal information," defined as "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; (E)(i) Biometric data." The Arkansas Act further defines "medical information" as "any individually identifiable information, in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional" and "biometric data" as "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." ARK. CODE § 4-110-103(7) (pdf).

California-1. The California Customer Records Act (California Act) protects "Personal information" defined as either of the following: "(A) An individual's first name or first initial and the individual's 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: (i) Social security number. (ii) Driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual. (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. (iv) Medical information. (v) Health insurance information. (vi) Unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual. Unique biometric data does not include a physical or digital photograph, unless used or stored for facial recognition purposes" or "(B) A username or email address in combination with a password or security question and answer that would permit access to an online account." The California Act defines "Medical information" as "any individually identifiable information,

in electronic or physical form, regarding the individual's medical history or medical treatment or diagnosis by a health care professional" and "Health insurance information" as "an individual's insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records." The California Act does not protect "publicly available information that is lawfully made available to the general public from federal, state, or local government records." CAL. CIV. CODE § 1798.81.5(d)(1) (pdf).

California-2. The California Consumer Privacy Act (CCPA) protects "Personal information," defined as "information that identifies, relates to, describes, is reasonably 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 if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household: (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 [CAL. CIV. CODE § 1798.80(e)], which includes '"any information that identifies, relates to, describes, or is capable of being associated with, a particular individual, including, but not limited to, his or her name, signature, social security number, physical characteristics or description, address, telephone number, passport number, driver's license or state identification card number, insurance policy number, education, employment, employment history, bank account number, credit card number, debit card number, or any other financial information, medical information, or health insurance information.'" (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 website, 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 . . . . (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, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes." The CCPA does not protect consumer information that is "deidentified "or "aggregate consumer information." The CCPA defines "Deidentified" as "information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer provided that the business that possesses the information: (1) Takes reasonable measures to ensure that the information cannot be associated with a consumer or household. (2) Publicly commits to maintain and use the information in deidentified form and not to attempt to reidentify the information, except that the business may attempt to reidentify the information solely for the purpose of determining whether its deidentification processes satisfy the requirements of this subdivision. (3) Contractually obligates any recipients of the information to comply with all provisions of this subdivision." The CCPA defines "Aggregate consumer information" as "information that relates to a group or category of consumers, from which individual consumer identities have been removed, that is not linked or reasonably linkable to any consumer or household, including via a device. The CCPA clarifies that "'Aggregate consumer information' does not mean one or more individual consumer records that have been deidentified." The CCPA also does not protect "publicly available information," defined as "information that is lawfully made available from federal, state, or local government records, or information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media, or by the consumer; or information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience." CAL. CIV. CODE § 1798.140(b), (m), and (v) (eff. January 1, 2023) (pdf).

California-3. The California Shine the Light Act (Shine the Light Act) protects "personal information," defined as "any information that when it was disclosed identified, described, or was able to be associated with an individual and includes all of the following: (A) An individual's name and address. (B) Electronic mail address. (C) Age or date of birth. (D) Names of children. (E) Electronic mail or other addresses of children. (F) Number of children. (G) The age or gender of children. (H) Height. (I) Weight. (J) Race. (K) Religion. (L) Occupation. (M) Telephone number. (N) Education. (O) Political party affiliation. (P) Medical condition. (Q) Drugs, therapies, or

medical products or equipment used. (R) The kind of product the customer purchased, leased, or rented. (S) Real property purchased, leased, or rented. (T) The kind of service provided. (U) Social security number. (V) Bank account number. (W) Credit card number. (X) Debit card number. (Y) Bank or investment account, debit card, or credit card balance. (Z) Payment history. (AA) Information pertaining to creditworthiness, assets, income, or liabilities." CAL. CIV. CODE § 1798.83(e)(7) (pdf).

California-4. The California Online Privacy Protection Act (CalOPPA) protects "personally identifying information," defined as "individually identifiable information about an individual consumer collected online by the operator from that individual and maintained by the operator in an accessible form, including any of the following: (1) A first and last name. (2) A home or other physical address, including street name and name of a city or town. (3) An e-mail address. (4) A telephone number. (5) A social security number. (6) Any other identifier that permits the physical or online contacting of a specific individual. (7) Information concerning a user that the Web site or online service collects online from the user and maintains in personally identifiable form in combination with an identifier described in this subdivision." CAL. BUS. & PROF. CODE § 22577 (pdf).

Colorado-1. In the context of data security, the Colorado Consumer Protection Act (Colorado Act) protects "personal identifying information," defined as "a social security number; a personal identification number; a password; a pass code; an official state or government-issued driver's license or identification card number; a government passport number; biometric data; an employer, student, or military identification number; or a financial transaction device." COLO. REV. STAT. § 6-1-713(2)(a), (b) (internal statutory references omitted) (pdf).

Colorado-2. In the context of data breach notification, the Colorado Act defines "personal information" as: "(A) 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." The Colorado Act does not protect "publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media." COLO. REV. STAT. § 6-1-716(1)(g) (pdf).

Colorado-3. The Colorado Privacy Act (CPA) protects "personal data," defined as "information that is linked or reasonably linkable to an identified or identifiable individual" and that "does not include de-identified data or publicly available information." The CPA defines "de-identified data" as "data that cannot reasonably be used to infer information about, or otherwise linked to, an identified or identifiable individual, or a device linked to such an individual, if the controller that possesses the data: (a) takes reasonable measures to ensure that the data cannot be associated with an individual; (b) publicly commits to maintain and use the data only in a de-identified fashion and not attempt to re-identify the data; and (c) contractually obligates any recipients of the information to comply with [certain other requirements]." The CPA defines "publicly available information" as "information that is lawfully made available from federal, state, or local government records and information that a controller has a reasonable basis to believe the consumer has lawfully made available to the general public." The CPA does not apply to personal data" that is "de-identified in accordance with the [HIPAA Privacy Rule's De-identification Safe Habor] and derived from any of the health-care related information described in the CPA." The CPA defines health-related information as "individually identifiable information relating to the past, present, or future health status of an individual." S.B. 21-190, signed into law on July 7, 2021, to be codified at COLO. REV. STAT. §§ 6-1-1301, -1303 (eff. July 1, 2023) (pdf).

Connecticut-1. The Connecticut Breach of Data Security Act (Connecticut Act) protects "personal information," defined as "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." The Connecticut Act clarifies that "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." CONN. GEN. STAT. § 36a-701b(a)(2) (pdf).

Connecticut-2. The Connecticut Safeguarding of Personal Information Act (Second Connecticut Act) protects "personal information," defined as "information capable of being associated with a particular individual through one or more identifiers, including, but not limited to, a Social Security number, a driver's license number, a state identification card number, an account number, a credit or debit card number, a passport number, an alien registration number, a health insurance identification number or any military identification information, and 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." CONN. GEN. STAT. § 42-471 (pdf).

Delaware-1. The Delaware Computer Security Breaches Act (Delaware Act) protects "personal information," defined as "a Delaware 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 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." The Delaware Act does not protect "publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely-distributed media." DEL. CODE tit. 6, §§ 12B-100 12B-101 (pdf).

Delaware-2. Delaware's Safe Destruction of Records Containing Personal Identifying Information Act (Second Delaware Act) protects "personal identifying information," defined as "a consumer's first name or first initial and last name in combination with any [one] of the following data

elements that relate to the consumer, when either the name or the data elements are not encrypted: Social Security number; passport number; driver's license or state identification card number; insurance policy number; financial services account number; bank account number; credit card number; debit card number; tax or payroll information or confidential health-care information including all information relating to a patient's health-care history; diagnosis condition, treatment; or evaluation obtained from a health-care provider who has treated the patient which explicitly or by implication identifies a particular patient." DEL. CODE tit. 6 § 5001C(3) (pdf).

Delaware-3. The Delaware Online Privacy and Protection Act (DelOPPA) protects "personally identifiable information," defined as "any personally identifiable information about a user of a commercial internet website, online or cloud computing service, online application, or mobile application that is collected online by the operator of that commercial internet website, online service, online application, or mobile application from that user and maintained by the operator in an accessible form, including a first and last name, a physical address, an e-mail address, a telephone number, a Social Security number, or any other identifier that permits the physical or online contacting of the user, and any other information concerning the user collected by the operator of the commercial internet website, online service, online application, or mobile application from the user and maintained in personally identifiable form in combination with any identifier described in this paragraph." DEL. CODE tit. 6 § 1202C(15) (pdf).

District of Columbia. The District of Columbia Consumer Security Breach Notification Act (D.C. Act) protects "personal information," defined as "(i) An individual's first name, first initial and last name, or any other personal identifier, which, in combination with any of the following data elements, can be used to identify a person or the person's information: (I) Social security number, Individual Taxpayer Identification Number, passport number, driver's license number, District of Columbia identification card number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (II) Account number, credit card number or debit card number, or any other number or code or combination of numbers or codes, such as an identification number, security code, access code, or password, that allows access to or use of an individual's financial or credit account; (III) Medical information; (IV) Genetic information and deoxyribonucleic acid profile; (V) Health insurance information, including

a policy number, subscriber information number, or any unique identifier used by a health insurer to identify the person that permits access to an individual's health and billing information; (VI) 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 is used to uniquely authenticate the individual's identity when the individual accesses a system or account; or (VII) Any combination of data elements included in sub-sub-subparagraphs (I) through (VI) of this sub-subparagraph that would enable a person to commit identity theft without reference to a person's first name or first initial and last name or other independent personal identifier." The D.C. Act does not protect "publicly available information that is lawfully made available to the general public from federal, state, or local government records." D.C. CODE § 28-3851(3)(A) (pdf).

Florida. The Florida Information Protection Act (Florida Act) protects "personal information," defined as 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" or "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." The Florida Act does not protect "information about an individual that has been made publicly available by a federal, state, or local governmental entity." The Florida Act also does not protect "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." FLA. STAT. § 501.171(1)(g) (pdf).

Georgia-1. The Georgia Personal Identity Protection Act (Georgia Act) protects "personal information," defined to include "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 Georgia Act does not protect "publicly available information that is lawfully made available to the general public from federal, state, or local government records." GA. CODE § 10-1-911(6) (pdf).

Georgia-2. The Georgia Discarding Records Containing Personal Information Act (Second Georgia Act) protects "personal information," defined as: "(A) Personally identifiable data about a customer's medical condition, if the data are not generally considered to be public knowledge; (B) Personally identifiable data which contain a customer's account or identification number, account balance, balance owing, credit balance, or credit limit, if the data relate to a customer's account or transaction with a business; (C) Personally identifiable data provided by a customer to a business upon opening an account or applying for a loan or credit; or (D) Personally identifiable data about a customer's federal, state, or local income tax return." The Second Georgia Act clarifies that "personally identifiable" means "capable of being associated with a particular customer through one or more identifiers, including, but not limited to, a customer's fingerprint, photograph, or computerized image, social security number, passport number, driver identification number, personal identification card number, date of birth, medical information, or disability information." The Second Georgia Act further clarifies that "A customer's name, address, and telephone number shall not be considered personally identifiable data unless one or more of them are used in conjunction with one or more of the identifiers listed in subparagraph (A) of this paragraph." GA. STAT. § 10-15-1(9), (10) (pdf).

Hawaii-1. The Hawaii Act Relating to Protection from Security Breaches (Act) protects "personal information," defined as "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." The Hawaii Act does not require breach notification for personal information that is "redacted," defined as "the rendering of data so that it is unreadable or is truncated so that no more than the last four digits of the identification number are accessible as part of the data." The Hawaii Act does not protect "publicly available information that is lawfully made available to the general public from federal, state, or local government records." HAW. REV. STAT. § 487N-1 (pdf).

Hawaii-2. The Hawaii Destruction of Personal Information Records Act (Second Hawaii Act) protects "personal information," defined as "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." The Second Hawaii Act defines encrypted as "the use of an algorithmic process to transform data into a form in which the data is rendered unreadable or unusable without the use of a confidential process or key." The Second Hawaii Act does not protect "publicly available information that is lawfully made available to the general public from federal, state, or local government records." *See* HAW. REV. STAT. § 487R-1 (pdf).

Idaho. The Idaho Disclosure of Breach of Security of Computerized Personal Information Act (Idaho Act) protects "personal information," defined as "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 Idaho Act does not protect "publicly available information that is lawfully made available to the general public from federal, state, or local government records or widely distributed media." *See* IDAHO CODE § 28-51-104(5) (pdf).

Illinois. The Illinois Personal Information Protection Act (Illinois Act) protects "personal information," defined as "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" or "(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." The Illinois Act defines "health insurance information" as "an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any medical information in an individual's health insurance application and claims history, including any appeals records" and "medical information" as "any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional, including such information provided to a website or mobile application." The Illinois Act does not protect "publicly available information that is lawfully made available to the general public from federal, State, or local government records." *See* 815 ILCS § 530/5 (pdf).

Indiana. The Indiana Breach of the Security of Data Act (Indiana Act) protects "personal information," defined as either: "(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 Indiana Act defines "encrypted" as data that "(1)

have been transformed through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key; or (2) are secured by another method that renders the data unreadable or unusable." The Indiana Act defines "redacted" data as data that "have been altered or truncated so that not more than the last four (4) digits of: (1) a driver's license number; (2) a state identification number; or (3) an account number." The Indiana Act further clarifies that personal information has been "redacted" if the information "has been altered or truncated so that not more than five (5) digits of a Social Security number are accessible as part of personal information." The Indiana Act does not protect "information that is lawfully obtained from publicly available information or from federal, state, or local government records lawfully made available to the general public." IND. CODE § 24-4.9-2-5, -10, -11 (pdf).

Iowa. The Iowa Personal Information Security Breach Protection Act (Iowa Act) protects "personal information," defined as "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." The Iowa Act defines "redacted" as "altered or truncated so that no more than five digits of a social security number or the last four digits of other numbers . . . are accessible as part of the data." The Iowa Act does not protect "information that is lawfully obtained from publicly available sources, or from federal, state, or local government records lawfully made available to the general public." IOWA CODE § 715C.1(11), (12) (pdf).

Kansas. The Kansas Protection of Consumer Information Act (Kansas Act) protects "personal information," defined as "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 Kansas Act defines "encrypted" as the "transformation of data through the use of algorithmic process into a form in which there is a low probability of assigning meaning without the use of a confidential process or key, or securing the information by another method that renders the data elements unreadable or unusable." The Kansas Act defines "redact" as the "alteration or truncation of data such that no more than the following are accessible as part of the personal information: (1) Five digits of a social security number; or (2) the last four digits of a driver's license number, state identification card number or account number." The Kansas Act does not protect "publicly available information that is lawfully made available to the general public from federal, state or local government records." KANS. STAT. ANN. § 50-7a01(b), (d), (g) (pdf).

Kentucky-1. The Kentucky Destruction of Customer's Records Containing Personally Identifiable Information (Kentucky Security Act) protects "personally identifiable information," defined as "data capable of being associated with a particular customer through one (1) or more identifiers, including but not limited to a customer's name, address, telephone number, electronic mail address, fingerprints, photographs or computerized image, Social Security number, passport number, driver identification number, personal identification card number or code, date of birth, medical information, financial information, tax information, and disability information." KY. REV. STAT. § 365.720(4) (pdf).

Kentucky-2. The Kentucky Notification to Affected Persons of Computer Security Breach Involving Their Unencrypted Personally Identifiable Information (Kentucky Breach Notification Act) protects "personally identifiable information," defined "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." KY. REV. STAT. § 365.732(1)(c) (pdf).

Louisiana. The Louisiana Database Security Breach Notification Act (Louisiana Act) protects "personal information," defined as "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." The Louisiana Act defines "biometric data" as "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." The Louisiana Act does not protect "publicly available information that is lawfully made available to the general public from federal, state, or local government records." LA. REV. STAT. § 51:3073(4) (pdf).

Maine. The Maine Notice of Risk to Personal Data Act (Maine Act) protects "personal information," defined as "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." The Maine Act does not protect "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." ME. REV. STAT. ANN. tit. 10 § 1347(6) (pdf).

Maryland. The Maryland Personal Information Protection Act (Maryland Act) protects "personal information," defined as: "(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." The Maryland Act does not protect: "(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." The Maryland Act defines "encrypted" as "the protection of data in electronic or optical form using an encryption technology that renders the data indecipherable without an associated cryptographic key necessary to enable decryption of the data." The Maryland Act defines "health information" as "any information created by an entity covered by [HIPAA] regarding an individual's medical history, medical condition, or medical treatment or diagnosis." MD. CODE. COM. LAW § 14-3501(c), (d), (e) (pdf).

Massachusetts. The Massachusetts Security Breaches Act (Massachusetts Act) protects "personal information," defined as "a resident's first name and last name or first initial and last name in combination with any [one] 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." The Massachusetts Act defines "encrypted" as the "transformation of data through the use of a 128-bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, unless further defined by regulation of the department of consumer affairs and business regulation." The Massachusetts Act further clarifies that "The department of consumer affairs and business regulation may adopt regulations, from time to time, to revise the definition of '"encrypted"', as used in this chapter, to reflect applicable technological advancements." The Massachusetts Act does not protect "information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public." MASS. GEN. LAWS ch. 93H § 1(a), (b) (pdf).

Michigan. The Michigan Identity Theft Protection Act (Michigan Act) protects unencrypted and unredacted "personal information," defined as "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." The Michigan Act defines "redact" as "to alter or truncate data so that no more than 4 sequential digits of a driver license number, state personal identification card number, or account number, or no more than 5 sequential digits of a social security number, are accessible as part of personal information" and "encrypted" as the "transformation of data through the use of an algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key, or securing information by another method that renders the data elements unreadable or unusable." MICH. COMP. LAWS § 445.63(g), (r), (t) (pdf).

Minnesota. The Minnesota Data Warehouses Act (Minnesota Act) protects "personal information," defined as "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." The Minnesota Act does not protect "publicly available information that is lawfully made available to the general public from federal, state, or local government records." MINN. STAT. § 325E.61(1)(e), (f) (pdf).

Mississippi. The Mississippi Notice of Breach of Security Act (Mississippi Act) protects "personal information," defined as "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." The Mississippi Act does not protect "publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media." MISS. CODE ANN. § 75-24-29(2)(b) (pdf).

Missouri. The Missouri Notice to Consumer for Breach of Security Act (Missouri Act) protects "personal information," defined as "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." The Missouri Act defines "redacted" as "altered or truncated such that no more than five digits of a Social Security number or the last four digits of a driver's license number, state identification card number, or account number is accessible as part of the personal information." The Missouri Act defines "medical information" as "any information

regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional" and "health insurance information" as "an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual." The Missouri Act does not protect "information that is lawfully obtained from publicly available sources, or from federal, state, or local government records lawfully made available to the general public." MO. REV. STAT. § 407.1500 (pdf).

Montana-1. The Montana Impediment of Identity Theft Act (Montana Act) protects, through record destruction provisions, "personal information," defined as "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." MONT. CODE ANN. § 30-14-1702 (pdf).

Montana-2. The Montana Computer Security Breach Act (Second Montana Act) protects, through breach notification provisions, "personal information," defined as "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: (A) social security number; (B) driver's license number, state identification card number, or tribal 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; (D) medical record information, [defined as "personal information that: (a) relates to an individual's physical or mental condition, medical history, medical claims history, or medical treatment; and (b) is obtained from a medical professional or medical care institution, from the individual, or from the individual's spouse, parent, or legal guardian." MONT. CODE ANN. § 33-19-104.]; (E) a taxpayer identification number; or (F) an identity protection personal identification number issued by the United States internal revenue service." The Second Montana Act does not protect "publicly available information that is lawfully made available to the general public from federal, state, or local government records." MONT. CODE ANN. § 30-14-1704 (pdf).

Nebraska. The Nebraska Financial Data Protection and Consumer Notification of Data Security Breach Act (Nebraska Act) protects "personal information," defined as 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." The Nebraska Act defines "redact" to mean "to alter or truncate data such that no more than the last four digits of a social security number, motor vehicle operator's license number, state identification card number, or account number is accessible as part of the personal information." The Nebraska Act does not protect "publicly available information that is lawfully made available to the general public from federal, state, or local government records." NEB. REV. STAT. § 87-802 (pdf).

Nevada-1. The Nevada Security of Information Maintained by Data Collectors and Other Businesses (Nevada Act) protects "personal information," defined as "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." The Nevada Act clarifies that "personal information" 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." NEV. REV. STAT. § 603A.040 (pdf).

Nevada-2. The Nevada Act Relating to Internet Privacy protects "covered information," defined as "any one or more of the following items of personally identifiable information about a consumer collected by an operator through an Internet website or online service and maintained by the operator in an accessible form: 1. A first and last name. 2. A home or other physical address which includes the name of a street and the name of a city or town. 3. An electronic mail address. 4. A telephone number. 5. A social security number. 6. An identifier that allows a specific person to be contacted either physically or online. 7. Any other information concerning a person collected from the person through the Internet website or online service of the operator and maintained by the operator in combination with an identifier in a form that makes the information personally identifiable." NEV. REV. STAt. § 603A.320 (pdf).

New Hampshire. The New Hampshire Notice of Security Breach Act (New Hampshire Act) protects "personal information," defined as 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." The New Hampshire Act does not protect "information that is lawfully made available to the general public from federal, state, or local government records." N.H. REV. STAT. § 359-C:19(IV) (pdf).

New Jersey. The New Jersey Security of Personal Information Act (New Jersey Act) protects "personal information," defined as "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; (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; or (4) user name, email address, or any other account holder identifying information, in combination with any password or security question and answer that would permit access to an online account."

The New Jersey Act clarifies that "[d]issociated 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." The New Jersey Act does not protect "publicly available information that is lawfully made available to the general public from federal, state or local government records, or widely distributed media." N.J. STAT. § 56:8-161 (pdf).

New Mexico. The New Mexico Data Breach Notification Act (New Mexico Act) protects "personal identifying information," defined as "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." The New Mexico Act defines "biometric data" as "a record generated by automatic measurements of an identified individual's fingerprints, voice print, iris or retina patterns, facial characteristics or hand geometry that is used to uniquely and durably authenticate an individual's identity when the individual accesses a physical location, device, system or account." The New Mexico Act does not protect "information that is lawfully obtained from publicly available sources or from federal, state or local government records lawfully made available to the general public." N.M. STAT. ANN. § 57-12C-2 (pdf).

New York. The New York Notification of Unauthorized Acquisition of Private Information Act (New York Act) protects "private information," defined as "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 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; (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." The New York Act defines "personal information" as "any information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person." The New York Act does not protect "publicly available information which is lawfully made available to the general public from federal, state, or local government records." N.Y. GEN. BUS. LAW § 899-aa (pdf).

North Carolina. The North Carolina Identity Theft Protection Act (North Carolina Act) protects "personal information," defined as a "person's first name or first initial and last name in combination with identifying information [defined to include: (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; (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.]" The North Carolina Act defines "redaction" as "[t]he rendering of data so that it is unreadable or is truncated so that no more than the last four digits of the identification number is accessible as part of the data." The North Carolina Act does not protect "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." N.C. GEN. STAT. § 75-61 (pdf).

North Dakota. The North Dakota Notice of Security Breach for Personal Information Act (North Dakota Act) protects "personal information," defined as "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." The North Dakota Act defines "health insurance information" as "an individual's health insurance policy number or subscriber identification number and any unique identifier used by a health insurer to identify the individual" and "medical information" as "any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional." The North Dakota Act does not protect "publicly available information that is lawfully made available to the general public from federal, state, or local government records." N.D. CEN. CODE § 51-30-01 (pdf).

Ohio. The Ohio Breach of System Containing Personal Information Act (Ohio Act) protects "personal information," defined as "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." The Ohio Act defines "redacted" as "altered or truncated so that no more than the last four digits of a social security number, driver's license number, state identification card number, account number, or credit or debit card number is accessible as part of the data." The Ohio Act does not protect "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 [the foregoing sub-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 [the last three sub-sections]." OHIO REV. CODE ANN. § 1349.19 (pdf).

Oklahoma. The Oklahoma Security Breach Notification Act (Oklahoma Act) protects "personal information," defined as "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 Oklahoma Act defines "redact" as "alteration or truncation of data such that no more than the following are accessible as part of the personal information: a. five digits of a social security number, or b. the last four digits of a driver license number, state identification card number or account number." The Oklahoma Act does not protect "information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public." OKLA. STAT. ANN. tit. 24, § 162 (pdf).

Oregon. The Oregon Identity Theft Protection Act (Oregon Act) protects "personal information," defined as "(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. (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." The Oregon Act defines "redacted" as "altered or truncated so that no more than the last four digits of a Social Security number, driver license number, state identification card number, passport number or other number issued by the United States, financial account number, credit card number or debit card number is visible or accessible." The Oregon Act does not protect "information in a federal, state or local government record, other than a Social Security number, that is lawfully made available to the public." OR. REV. STAT. ANN. § 646A.602 (pdf).

Pennsylvania. The Pennsylvania Breach of Personal Information Notification Act (Pennsylvania Act) protects "personal information," defined as "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." The Pennsylvania Act defines "redact" as "alteration or truncation such that no more than the last four digits of a Social Security number, driver's license number, State identification card number or account number is accessible as part of the data." The Pennsylvania Act does not protect "publicly available information that is lawfully made available to the general public from Federal, State or local government records." 73 PA. STAT. § 2302 (pdf).

Rhode Island. The Rhode Island Identity Theft Protection Act (Rhode Island Act) protects "personal information," defined as "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." The Rhode Island Act defines "health insurance information" as "an individual's health insurance policy number, subscriber identification number, or any unique identifier used by a health insurer to identify the individual" and "medical information" as "any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional or provider." The Rhode Island Act does not protect "publicly available information that is lawfully made available to the general public from federal, state, or local government records." R.I. GEN. LAWS § 11-49.3-3 (pdf).

South Carolina. The South Carolina Breach of Security of Business Data Act (South Carolina Act) protects "personal identifying information," defined as "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 South Carolina Act does not protect "information that is lawfully obtained from publicly available information, or from federal, state, or local governmental records lawfully made available to the general public." S.C. CODE ANN. § 39-1-90(D)(3) (pdf).

South Dakota. The South Dakota Notice of Breach of System Security Act (South Dakota Act) protects "personal information," defined as "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 [the HIPAA Administrative Simplification Rules]; 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 South Dakota Act clarifies that 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." The South Dakota Act also protects "protected information," defined to include: "(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." S.D. COD. LAWS § 22-40-19 (pdf).

Tennessee-1. The Tennessee Breaches of Security Systems Act (Tennessee Act) protects "personal information," defined as "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." The Tennessee Act does not protect "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." TENN. CODE § 47-18-2107(a)(4) (pdf).

Tennessee-2. A second Tennessee law protects "personal identifying information," defined as "a customer's: (A) Social security number; (B) Driver license identification number; (C) Savings account number; (D) Checking account number; (E) PIN (personal identification number) or password; (F) Complete credit or debit card number; (G) Demand deposit

account number; (H) Health insurance identification number; or (I) unique biometric data." TENN. CODE § 39-14-150(g)(2) (pdf).

Texas-1. The Texas Identity Theft Protection and Enforcement Act (Texas Act) provides certain protections to "personal identifying information," defined as "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." The Texas Act provides other protections to "sensitive personal information," defined as "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." The Texas Act clarifies that the definition of "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." TEX BUS. & COM. CODE § 521.002 (pdf).

Texas-2. The Texas Medical Records Privacy Act (TMRPA) protects "protected health information," internally referencing the HIPAA Privacy Rule's definition of protected health information. (*See* entry for "HIPAA" under Federal Authorities, below.) The TMRPA contains the following prohibition: "A person may not reidentify or attempt to reidentify an individual who is the subject of any protected health information without obtaining the individual's consent or authorization if required under this chapter or other state or federal law." TEX. HEALTH & SAFETY CODE §§ 181.001, 181.151 (pdf).

Utah-1. The Utah Protection of Personal Information Act (Utah Act) protects "personal information," defined as "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." The Utah Act does not protect "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." UTAH CODE § 13-44-102(4) (pdf).

Utah-2. The Utah Notice of Intent to Sell Nonpublic Personal Information Act protects "nonpublic personal information," defined as information that: "(i) is not public information; and (ii) either alone or in conjunction with public information, identifies a person in distinction from other persons." The Second Utah Act clarifies that "nonpublic personal information includes: (i) a person's Social Security number; (ii) information used to determine a person's credit worthiness including a person's: (A) income; or (B) employment history; (iii) the purchasing patterns of a person; or (iv) the personal preferences of a person." The Second Utah Act defines "public information" as a person's "(a) name; (b) telephone number; or (c) street address." UTAH CODE § 13-37-102 (pdf).

Vermont-1. The Vermont Protection of Personal Information Act (Vermont Act), through secure destruction standards, protects "personal information," defined as "the following information that identifies, relates to, describes, or is capable of being associated with a particular individual: his or her signature, Social Security number, physical characteristics or description, passport number, driver's license or State identification card number, insurance policy number, bank account number, credit card number, debit card number, or any other financial information." VT. STAT. tit. 9 § 2445(a)(3) (pdf).

Vermont-2. The Vermont Act, through separate provisions requiring notification following a data security breach, protects "personally identifiable information," defined as "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 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) a driver license or nondriver State identification card number, individual taxpayer identification number, passport number, military identification card number,

or other identification number that originates from a government identification document that is commonly used to verify identity for a commercial transaction;' (iii) a financial account number or credit or debit card number, if the number could be used without additional identifying information, access codes, or passwords; (iv) a password, personal identification number, or other access code for a financial account." This provision of the Vermont Act does not protect "publicly available information that is lawfully made available to the general public from federal, State, or local government records." This provision of the Vermont Act defines "redaction" as "the rendering of data so that the data are unreadable or are truncated so that no more than the last four digits of the identification number are accessible as part of the data." VT. STAT. tit. 9 § 2430(10), (12) (pdf).

Virginia-1. The Virginia Breach of Personal Information Notification Act (Virginia Act) protects "personal information," defined as "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 Virginia Act defines "redact" as the "alteration or truncation of data such that no more than the following are accessible as part of the personal information: 1. Five digits of a social security number; or 2. The last four digits of a driver's license number, state identification card number, or account number." The Virginia Act does not protect "information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public." VA. CODE ANN. § 18.2-186.6(A) (pdf).

Virginia-2. The Virginia Breach of Medical Information Notification Act (Second Virginia Act) protects "medical information," defined as "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. Any information regarding an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or 2. An individual's health insurance policy

number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records." The Second Virginia Act defines "redact" as the "alteration or truncation of data such that no information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis or no more than four digits of a health insurance policy number, subscriber number, or other unique identifier are accessible as part of the medical information." The Second Virginia Act does not protect "information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public." VA. CODE ANN. § 32.1-127.1:05(A) (pdf).

Virginia-3. The Virginia Consumer Data Protection Act (VCDPA) protects "personal data," defined as "any information that is linked or reasonably linkable to an identified or identifiable natural person." The VCDPA clarifies that "personal data" does not include "de-identified data or publicly available information." The VCDPA defines "de-identified data," defined as "data that cannot reasonably be linked to an identified or identifiable natural person, or a device linked to such person." Data controllers in possession of "de-identified data" are required by the VCDPA to: "(1) Take reasonable measures to ensure that the data cannot be associated with a natural person; (2) Publicly commit to maintaining and using de-identified data without attempting to re-identify the data; and (3) Contractually obligate any recipients of the de-identified data to comply with all provisions of this chapter." Virginia Consumer Data Protection Act, S.B.1392 (Mar. 2, 2021) (pdf), *to be codified at* VA. CODE ANN. §§ 59.1-571 -581 (eff. Jan. 1, 2023).

Washington. The Washington Notice of Security Breaches Act (Washington Act) protects "personal information," defined as "(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) User name 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." The Washington Act does not protect "publicly available information that is lawfully made available to the general public from federal, state, or local government records." WASH. REV. CODE § 19.255.005(2)(a) (pdf).

West Virginia. The West Virginia Breach of Security of Consumer Information Act (West Virginia Act) protects "personal information," defined as "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 West Virginia Act defines "redact" as the "alteration or truncation of data such that no more than the last four digits of a social security number, driver's license number, state identification card number or account number is accessible as part of the personal information." The West Virginia Act does not protect "information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public." W.V. CODE § 46A-2A-101(6), (8) (pdf).

Wisconsin-1. The Wisconsin Notice of Unauthorized Acquisition of Personal Information Act (Wisconsin Act) protects "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 [DNA profile]. 5. The individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation." The Wisconsin Act defines "publicly available information," which is not protected, as "any information that an entity reasonably believes is one of the following: 1. Lawfully made widely available through any media. 2. Lawfully made available to the general public from federal, state, or local government records or disclosures to the general public that are required to be made by federal, state, or local law." WISC. STAT. ANN. § 134.98(1)(b) (pdf).

Wisconsin-2. The Wisconsin Disposal of Records Containing Personal Information Act (Second Wisconsin Act) protects "personal information," defined as "any of the following: 1. Personally identifiable data about an individual's medical condition, if the data are not generally considered to be public knowledge. 2. Personally identifiable data that contain an individual's account or customer number, account balance, balance owing, credit balance or credit limit, if the data relate to an individual's account or transaction with a financial institution. 3. Personally identifiable data provided by an individual to a financial institution upon opening an account or applying for a loan or credit. 4. Personally identifiable data about an individual's federal, state or local tax returns." The Second Wisconsin Act defines "personally identifiable" as "capable of being associated with a particular individual through one or more identifiers or other information or circumstances." WISC. STAT. ANN. § 134.97 (pdf).

Wyoming. The Wyoming Computer Security Breach Act (Wyoming Act) protects "personal identifying information," defined as the "first name or first initial and last name of a person in combination with one (1) or more of the [following] data elements [including Social security number; Driver's license number; 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; Tribal identification card; Federal or state government issued identification card; Shared secrets or security tokens that are known to be used for data based authentication; A username or email address, in combination with a password or security question and answer that would permit access to an online account; A birth

or marriage certificate; Medical information, meaning a person's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional; 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; Unique biometric data, meaning data generated from measurements or analysis of human body characteristics for authentication purposes; An individual taxpayer identification number] when the data elements are not redacted." The Wyoming Act defines "redact" as the "alteration or truncation of data such that no more than five (5) digits of the data elements provided in [certain subparagraphs of this subsection] are accessible as part of the personal information." WYO. STAT. § 40-12-501(a)(vii), (viii) (pdf).

FEDERAL AUTHORITIES

CCDPA. The COVID-19 Consumer Data Protection Act of 2020 (CCDPA) would protect "covered data," defined to include "precise geolocation data, proximity data, a persistent identifier, and personal health information." The CCDPA defines "precise geolocation data" as "technologically derived information capable of determining with reasonable specificity the past or present actual physical location of an individual at a specific point in time." The CCDPA defines a "persistent identifier" as "a technologically derived identifier that identifies an individual, or is linked or reasonably linkable to an individual over time and across services and platforms, which may include a customer number held in a cookie, a static Internet Protocol (IP) address, a processor or device serial number, or another unique device identifier." The CCDPA defines "personal health information" as "information relating to an individual" (including "genetic information of the individual" and "information relating to the diagnosis or treatment of past, present, or future physical, mental health, or disability of the individual") if such information "identifies, or is reasonably linkable to, the individual." The CCDPA does not apply to "aggregated data" and "de-identified data," among other types of data. The CCDPA defines "aggregated data" as "information that (A) relates to a group or category of individuals; and (B) does not identify, and is not linked or reasonably linkable to, any individual." The CCDPA defines "de-identified data" as "information held by a covered entity that—(A) does not identify and is not reasonably linkable to an individual; (B) does not contain any personal identifiers or other information that could be readily used to re-identify the

individual to whom the information pertains; (C) is subject to a public commitment by the covered entity: (i) to refrain from attempting to use such information to identify any individual; and (ii) to adopt technical and organizational measures to ensure that such information is not linked to any individual; and (D) is not disclosed by the covered entity to any other party unless the disclosure is subject to a contractually or other legally binding requirement that: (i) the recipient of the information shall not use the information to identify any individual; and (ii) all onward disclosures of the information shall be subject to the requirement described in clause (i)." The COVID-19 Consumer Data Protection Act of 2020, S.3663, 116th Cong., 2nd Sess. (May 7, 2020) (pdf).

DCA. The Data Care Act of 2018 (DCA) would establish duties for online service providers with respect to "individual identifying data," defined in relevant part as data that are "linked, or reasonably linkable" to certain end users and computer devices. The DCA would establish additional duties for online service providers with respect to "sensitive data," defined to include a social security number; personal information (as defined in the Children's Online Privacy Protection Act of 1998); a driver's license number, passport number, military identification number, or any other similar number issued on a government document used to verify identity; a financial account number, credit or debit card number, or any required security code, access code, or password that is necessary to permit access to a financial account of an individual; unique biometric data such as a finger print, voice print, a retina or iris image, or any other unique physical representation; information sufficient to access an account of an individual, such as user name and password or email address and password; the first and last name of an individual, or first initial and last name, or other unique identifier in combination with—(i) the month, day, and year of birth of the individual; (ii) the maiden name of the mother of the individual; or (iii) the past or present precise geolocation of the individual; information that relates to—(i) the past, present, or future physical or mental health or condition of an individual; or (ii) the provision of health care to an individual; and the nonpublic communications or other nonpublic user-created content of an individual. Data Care Act of 2018, S.3744, 115th Cong., 2nd Sess., § 3 (Dec. 12, 2018) (pdf).

ENPA. The Exposure Notification Privacy Act (ENPA) would impose certain data privacy and security standards on operators of automated infectious disease exposure notification services with respect to "covered data." The ENPA defines "covered data" in relevant part as "information that

is: (A) linked or reasonably linkable to any individual or device linked or reasonably linkable to an individual; (B) not aggregate data; and (C) collected, processed, or transferred in connection with an automated exposure notification service." The Exposure Notification Privacy Act, S.3861, 116th Cong., 2nd Sess., § 2(6) (June 1, 2020) (pdf).

HIPAA. The Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule protects "protected health information" (PHI), defined in relevant part as "individually identifiable health information" (IIHI). The HIPAA Privacy Rule defines IIHI in relevant part as information "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." The HIPAA Privacy Rule does not apply to de-identified information. Information has been de-identified under the HIPAA Privacy Rule if the Expert Determination standard or the Safe Harbor has been satisfied. The Expert Determination provides: "A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable: (i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and (ii) Documents the methods and results of the analysis that justify such determination." The Safe Harbor provides: "The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed: (A) Names; (B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000. (C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older; (D) Telephone numbers; (E) Fax numbers; (F) Electronic mail addresses; (G) Social security numbers; (H) Medical record numbers; (I) Health plan beneficiary numbers; (J) Account numbers; (K) Certificate/license numbers; (L) Vehicle identifiers and serial numbers, including license plate numbers; (M) Device identifiers and serial numbers;

(N) Web Universal Resource Locators (URLs); (O) Internet Protocol (IP) address numbers; (P) Biometric identifiers, including finger and voice prints; (Q) Full face photographic images and any comparable images; and (R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; [and] The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information." The HIPAA Privacy Rule, codified in relevant part at 45 C.F.R. §§ 160.103, 164.514 (pdf).

ITPDCA. Information Transparency & Personal Data Control Act (ITPDCA) would direct the Federal Trade Commission (FTC) to promulgate regulations obligating certain data controllers, processors, and third parties to make available to the public information involving the collection, transmission, storage, processing, sale, sharing of sensitive personal information, or other use of sensitive personal information from persons operating in or persons located in the United States when the public's sensitive personal information is collected, transmitted, stored, processed, sold or shared. The ITPDCA would protect "sensitive personal information," defined to exclude "de-identified data." The ITPDCA defines "de-identified data" as information held that: (A) does not identify, and is not linked or reasonably linkable to, and individual or device; (B) does not contain a persistent identifier or other information that could readily be used to de-identify the individual to whom, or the device to which, the identifier or information pertains; (C) is subject to a public commitment by the entity to refrain from attempting to use such information to identify any individual or device and to adopt technical and organizational measures to ensure that such information is not linked to any individual or device; and (D) is not disclosed by the covered entity to any other party unless the disclosure is subject to a contractually or other legally binding requirement. Information Transparency & Personal Data Control Act, H.R. 1816, 117th Cong., 1st Sess. (Mar. 11, 2021) (pdf).

MYOBA. The Mind Your Own Business Act of 2019 (MYOBA) would direct the Federal Trade Commission (FTC) to promulgate regulations obligating certain entities to implement reasonable cybersecurity and privacy policies, practices, and procedures to protect "personal information." MYOBA defines "personal information" as "any information, regardless of how the information is collected, inferred, or obtained, that is reasonably linkable to a specific consumer or consumer device." Mind Your Own

Business Act of 2019, S.2637, 116th Cong., 1st Sess., § 2(12) (Oct. 17, 2019) (pdf).

PHEPA. The Public Health Emergency Privacy Act establishes certain privacy and security protects for "emergency health data," defined as "data linked or reasonably linkable to an individual or device, including data inferred or derived about the individual or device from other collected data provided such data is still linked or reasonably linkable to the individual or device, that concerns the public COVID–19 health emergency." The PHEPA specifies that such data includes: "(A) information that reveals the past, present, or future physical or behavioral health or condition of, or provision of healthcare to, an individual, including—(i) geolocation data, when such term means data capable of determining the past or present precise physical location of an individual at a specific point in time, taking account of population densities, including cell-site location information, triangulation data derived from nearby wireless or radio frequency networks, and glob- al positioning system data; (ii) proximity data, when such term means information that identifies or estimates the past or present physical proximity of one individual or device to another, including information derived from mate of the likelihood that a particular in-dividual may contract, such disease or disorder; and (iii) genetic data, biological samples, and biometrics; and (B) other data collected in conjunction with other emergency health data or for the purpose of tracking, screening, monitoring, con- tact tracing, or mitigation, or otherwise responding to the COVID–19 public health emergency, including—Bluetooth, audio signatures, nearby wireless networks, and near-field communications; (iii) demographic data; (iv) contact information for identifiable individuals or a history of the individual's contacts over a period of time, such as an address book or call log; and (v) any other data collected from a personal device." Public Health Emergency Privacy Act, S.3749, 116th Cong., 2nd Sess., § 2(8) (May 14, 2020) (pdf).

PPHDA. The Protecting Personal Health Data Act (PPHDA) would direct the Secretary of the federal Department of Health and Human Services (HHS) to promulgate regulations that would strengthen privacy and security protections for "personal health data" that are collected, processed, analyzed, or used by consumer devices, services, applications, or software. The PPHDA would define "personal health data" as "any information, including genetic information, whether oral or recorded in any form or medium, that relates to the past, present, or future physical or mental health or condition of an individual and that identifies the individual or with respect to which

there is a reasonable basis to believe that the information can be used to identify the individual. The PPHDA requires the Secretary of HHS to "consider appropriate standards for the de-identification of personal health data." The PPHDA would also create a task force responsible for studying "the long-term effectiveness of de-identification methodologies for genetic data and biometric data." S.1842, 116th Cong., 1st Sess. (June 13, 2019) (pdf).

SMARTWATCH Data Act. The Stop Marketing and Revealing the Wearables and Trackers Consumer Health (SMARTWATCH) Data Act would prohibit certain entities that collect consumer health information (CHI) from transferring or selling CHI to information brokers who collect or analyze CHI for profit. The SMARTWATCH Data Act defines CHI as "any information about the health status, personal biometric information, or personal kinesthetic information about a specific individual that is created or collected by a personal consumer device, whether detected from sensors or input manually." The SMARTWATCH Data Act clarifies that its transfer and sale prohibitions do not apply to CHI that has been "aggregated or anonymized," defining "aggregated" as "the removal of individual consumer identities so that the information is not linked or reasonably linkable to any consumer, including a personal consumer device and does not include [one] or more individual consumer records that have not been deidentified." The SMARTWATCH Data Act further defines "deidentified" information as "information that cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, computer, or other device." Stop Marketing and Revealing the Wearables and Trackers Consumer Health (SMARTWATCH) Data Act, S.2885, 116th Cong., 1st Sess. (Nov. 18, 2019) (pdf).