Bloomberg Law Privacy & Data Security

Domestic Privacy Profile: ARIZONA

Danielle Janitch, John Blanchard, and William Furnish, of Osborn Maledon, P.A., Phoenix, provided expert review of the Arizona Profile and wrote the Risk Environment section. [Last updated March 2018. – Ed.]

TABLE OF CONTENTS

I. APPLICABLE LAWS AND REGULATIONS

A. CONSTITUTIONAL PROVISIONS

Art. II, § 8 of the Arizona Constitution provides that no person shall be disturbed in his private affairs, or his home invaded, without authority of law.

B. PERSONAL DATA PROTECTION PROVISIONS

There are several Arizona laws applicable to the privacy and security of personal information collected, used, and disclosed by businesses and governmental entities in the state. Primary among them is the law covering notifications concerning data breaches of unencrypted computerized data (Ariz. Rev. Stat. § 18-545; hereinafter, the "data breach notification law"), which is outlined below and discussed in detail at Section I.C.8. Other provisions impose restrictions on the use and disclosure of social security numbers (Ariz. Rev. Stat. § 44-1373, et seq.; see Section I.D.10.), and provide civil remedies and criminal penalties for identity theft (Ariz. Rev. Stat. § 13-2008 through Ariz. Rev. Stat. § 13-2010; see Section I.G.2.) and impermissible eavesdropping (Ariz. Rev. Stat. § 13-3005; see Section I.F.). Finally, laws related to privacy and data security applicable to specific sectors, such as health care and insurance, are set forth in the portions of this profile dedicated to those sectors.

1. Who is covered?

All individuals affected by a breach in the security system resulting in unauthorized access to the individuals' personal information must be notified in the most expedient manner possible and without unreasonable delay (Ariz. Rev. Stat. § 18-545(A)).

2. What is covered?

The data breach notification law covers the unauthorized acquisition and access to unencrypted or unredacted data that includes an individual's personal information. A person who becomes aware of such an incident must conduct an investigation to promptly determine if there has been a breach of the security system, and if such a breach has occurred, promptly notify affected individuals (Ariz. Rev. Stat. § 18-545(A)). For additional information on data breach notification requirements, see Section I.C.8.

3. Who must comply?

The data breach notification law applies to all persons conducting business in the state who own or license unencrypted computerized data that includes personal information (Ariz. Rev. Stat. § 18-545(A)). In addition, a person that maintains, but does not own, unencrypted computerized data that includes personal information must notify and cooperate with the owner or licensee of the data with respect to any breach of the security of the system following discovery of the breach without reasonable delay (Ariz. Rev. Stat. § 18-545(B)). For additional information on breach notification requirements, see Section I.C.8.

C. DATA MANAGEMENT PROVISIONS

1. Notice & Consent

The Arizona Insurance Information and Privacy Protection Act contains specific notice and consent requirements among its provisions (see Section I.E.7.). In addition, provisions governing specific

types of health care facilities and providers and health data contain requirements regarding notice and consent (see Section I.D.9.).

For information on data breach notification requirements, see Section I.C.8.

2. Collection & Use

All state agency websites must contain a privacy policy statement that, among other items, describes the information the agency obtains from individuals online and how the agency uses the information (Ariz. Rev. Stat. § 18-202(2) and (4)), and whether other entities or persons are collecting information through the website (Ariz. Rev. Stat. § 18-202(6)).

Specific provisions govern the collection and use of social security numbers by persons or entities, including state agencies and governmental subdivisions (Ariz. Rev. Stat. § 44.1373(C) -(E); see Section I.D.10.).

Specific restrictions apply to the retention and use of information concerning driver's license or state ID information by a retailer (Ariz. Rev. Stat. § 44-7701(A)); see Section I.E.8.).

The Arizona Insurance Information and Privacy Protection Act contains specific requirements regarding the collection and use of personal information among its provisions (see Section I.E.7.). In addition, provisions governing specific types of health care facilities and providers and health data contain requirements regarding the collection and use of such information (see Section I.D.9.).

3. Disclosure to Third Parties

All state agency websites must contain a privacy policy statement that, among other items, describes whether and under what circumstances the agency discloses any information obtained from individuals to other entities or persons (Ariz. Rev. Stat. § 18-202(5)).

A publicly-supported library or library system may not allow disclosure of any record or other information, including e-books, that identifies a user of library services as requesting or obtaining specific materials or services (Ariz. Rev. Stat. § 41-151.22(A)). Disclosures are permitted if necessary for reasonable operation of the library, on written consent of the user, on receipt of a court order, or if required by law (Ariz. Rev. Stat. § 41-151.22(B)). A violation of this provision is a class 3 misdemeanor (Ariz. Rev. Stat. § 41-151.22(C)).

No person may intentionally communicate or otherwise make a person's social security number available to the general public (Ariz. Rev. Stat. § 44.1373(A)(1); see Section I.D.10.).

Specific restrictions apply to the disclosure of information concerning driver's license or state ID information by a retailer (Ariz. Rev. Stat. § 44-7701(A) -(C); see Section I.E.8.).

The Arizona Insurance Information and Privacy Protection Act contains specific requirements regarding the disclosure of personal information to third parties by covered entities among its provisions (see Section I.E.7.). In addition, provisions governing specific types of health care facilities and providers and health data contain requirements regarding the disclosure of such information (see Section I.D.9.).

Arizona has adopted requirements under the federal Family Educational Rights and Privacy Act (FERPA) regarding parents' rights to give written permission before student records are disclosed to another party (Ariz. Rev. Stat. § 15-141; see Section I.E.2.).

4. Data Storage

There are no specific Arizona privacy laws governing data storage.

5. Access & Correction

While there are no general Arizona provisions governing access to and correction of personal information, the Arizona Insurance Information and Privacy Protection Act contains specific access and correction requirements with respect to entities covered by its provisions (see Section I.E.7.). In addition, Arizona has adopted requirements under the federal Family Educational Rights and Privacy Act (FERPA) regarding parents' rights to access, and request correction of, student records (Ariz. Rev. Stat. § 15-141; see Section I.E.2.). Consumer credit reporting agencies are subject to specific access and correction requirements with respect to information contained in credit reports (see Section I.D.4.). Finally, provisions governing specific types of health care facilities and providers and health data contain requirements regarding access to, and correction of, such information (see Section I.D.9.).

6. Data Security

All state agency websites must contain a privacy policy statement that includes, among other items, a general description of the security measures in place to protect a person's information without compromising the integrity of the security measures (Ariz. Rev. Stat. § 18-202(7)).

Governmental agencies must develop and establish commercially reasonable procedures to ensure that entity identifying information or personal identifying information that is collected or obtained by the agency is secure and cannot be accessed, viewed, or acquired unless authorized by law (Ariz. Rev. Stat. § 18-522)).

For information concerning breach notification requirements in the event of a breach in the security of personal information owned or licensed by an Arizona business, see Section I.C.8.

7. Data Disposal

An entity may not knowingly discard or dispose of records or documents without redacting the information or destroying the records or documents if they contain an individual's first and last name or first initial and last name in combination with corresponding complete social security number; credit or debit card number; retirement account number; savings, checking, or securities entitlement account number; or driver's license or non-operating identification license number (Ariz. Rev. Stat. § 44-7601(A)). Note, however, that these provisions apply only to paper records and paper documents (Ariz. Rev. Stat. § 44-7601(F)). In addition, the requirements do not apply to entities subject to the personal information disclosure requirements of the federal Gramm-Leach-Bliley Act, covered entities subject to the Health Insurance Portability and Accountability Act (the HIPAA Privacy Rule), or entities subject to the federal Fair Credit Reporting Act (Ariz. Rev. Stat. § 44-7601(E)). An "entity" is defined to include several forms of corporate entities, sole proprietorships, LLCs, partnerships, and governmental subdivisions or agencies, among other business types (Ariz. Rev. Stat. § 44-7601(F)).

An entity that has procedures in place for the discarding or disposing of documents that are consistent with those described above are deemed to be in compliance (Ariz. Rev. Stat. § 44-7601(D)). Enforcement procedures and civil penalties apply to violations (see Section II.C.).

8. Data Breach

Under the Arizona data breach notification law (Ariz. Rev. Stat. § 18-545)), a person conducting business in the state who owns or licenses unencrypted computerized data that includes personal information and who becomes aware of an incident of unauthorized acquisition and access to unencrypted or unredacted computerized data that includes personal information must conduct an investigation to promptly determine if there has been a breach of the security system, and if such a breach has occurred, promptly notify affected individuals. Notice must be made in the most expedient manner possible and without unreasonable delay, subject to law enforcement needs

(see below) and any measures necessary to determine the nature and scope of the breach, to identify the individuals affected, or to restore the reasonable integrity of the data system (Ariz. Rev. Stat. § 18-545(A)).

In addition, a person that maintains, but does not own, unencrypted computerized data that includes personal information must notify and cooperate with the owner or licensee of the data with respect to any breach of the security of the system following discovery of the breach without reasonable delay. Cooperation includes sharing information with the owner or licensee, and in general, it is the responsibility of the owner or licensee to provide data breach notification to affected individuals, unless there is an agreement between the owner/licensee and the person maintaining the data to the contrary (Ariz. Rev. Stat. § 18-545(B)).

Primary definitions: As used in the statute, a "breach," "breach of the security of the system," "breach of the security system," and "security breach" all mean an unauthorized acquisition of and access to unencrypted or unredacted computerized data that materially compromises the security or confidentiality of personal information maintained by the person as part of a database of personal information regarding multiple individuals and that has caused or is reasonably likely to cause substantial economic loss to an individual. Good faith acquisition by an employee or agent of a person for purposes of the person does not constitute a breach if the personal information is not used for a purpose unrelated to the person or subject to further willful unauthorized disclosure (Ariz. Rev. Stat. § 18-545(L)(1)).

"Personal information" is defined to include an individual's first name or first initial and last name in combination with the following data elements when they are not encrypted, redacted, or secured by any other method rendering the element unreadable or unusable:

- social security number;
- driver's license number or government-issued ID number; or
- account number or debit 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.

Personal information does not include publicly available information lawfully made available to the public by federal, state, or local government or widely distributed media (Ariz. Rev. Stat. § 18-545(L)(6)).

Delay in notification for law enforcement purposes: The notification requirements described above may be delayed if a law enforcement agency advises the person that the notification will impede a criminal investigation. The person must make the notification after the law enforcement agency determines that it will not compromise the investigation (Ariz. Rev. Stat. § 18-545(C)).

Proper form of notice: A person required to provide breach notification may provide written notice, electronic notice if the person's primary method of communication with the individual is by electronic means or is consistent with federal electronic records and signature requirements, telephonic notice, or substitute notice (Ariz. Rev. Stat. § 18-545(D)(1) -(4)). Substitute notice is authorized if the person required to provide notice can show that the cost of providing notice would exceed $50,000, the number of affected persons exceeds 100,000, or the person does not have sufficient contact information. On such a showing, the person may give notice via e-mail, if the person has e-mail addresses for the affected individuals; conspicuous posting of the notice on the person's website, if it maintains one; or notification to major statewide media (Ariz. Rev. Stat. § 18-545(D)(4)(a) -(c)).

Alternative compliance and exceptions: A person making notification in accordance with an information security policy that complies with the breach notification requirements described above is in compliance with these provisions if it provides notification in accordance with its policy

(Ariz. Rev. Stat. § 18-545(E)). In addition, a person in compliance with notification requirements or security breach procedures pursuant to rules and procedures of the person's primary or functional federal regulator also will be deemed to comply (Ariz. Rev. Stat. § 18-545(F)). Finally, the data breach notification requirements do not apply to entities subject to the federal Gramm-Leach-Bliley Act or to covered entities as defined under the regulations implementing the federal Health Insurance Portability and Accountability Act (the HIPAA Privacy Rule) (Ariz. Rev. Stat. § 18-545(J)).

A person is not required to disclose a breach of the security of the system if the person or a law enforcement agency, after a reasonable investigation, determines that a breach of the security of the system has not occurred or is not reasonably likely to occur (Ariz. Rev. Stat. § 18-545(G)).

Enforcement: The Attorney General has sole enforcement authority over the provisions of the data breach notification law (see Section II.C.).

9. Data Transfer and Cloud Computing

Our research has revealed no provisions of Arizona law specifically addressing data transfers or cloud computing. A bill that passed the Arizona legislature in 2016 (S.B. 1434) would have required the Arizona Department of Administration to identify opportunities to consolidate information technology assets through the use of cloud computing services and would have established privacy standards conforming to specified federal laws. However, the Governor vetoed the legislation on May 17, 2016.

Ethics Opinion 09-04 of the State Bar of Arizona states that lawyers providing an online data storage and retrieval system for client access of documents must take reasonable precautions to protect the security and confidentiality of client information.

10. Other Provisions

Our research has revealed no other provisions of Arizona law governing data management issues.

D. Specific Types of Data

1. Biometric Data

Pupil biometric information: A school in a school district or a charter school may not collect biometric information from a pupil unless the pupil's parent or guardian gives written permission for the collection (Ariz. Rev. Stat. § 15-109(A)). Notice must be provided at least 30 days prior to collection and include a statement, in 18-pt. boldface capital letters, that the parent or guardian must give permission (Ariz. Rev. Stat. § 15-109(B)).

Applicant fingerprint data: Certain persons applying for new or renewed teaching certificates must submit for an identity-verified fingerprint card (see Section I.E.2.).

Webpage or e-mail solicitations for fraud or theft: Biometric data is included in the definition of "identifying information" for purposes of the prohibition on using a webpage or e-mail to solicit identifying information of individuals for purposes of fraud or theft (see Section I.D.7.).

Parents' Bill of Rights: Under the Parents' Bill of Rights, parents have the right to consent in writing before a biometric scan of their minor child is made (see Section I.D.12.).

2. Consumer Data

Breach notification law: Unencrypted consumer data owned or licensed by a business in Arizona that contains personal information would be subject to the state's data breach notification law in the event that a breach is discovered (see Section I.C.8.).

Webpage or e-mail solicitations for fraud or theft: Many forms of consumer data, including names in combination with elements such as social security numbers or account numbers, contain information that would be included in the definition of "identifying information" for purposes of the prohibition on using a webpage or e-mail to solicit identifying information of individuals for purposes of fraud or theft (see Section I.D.7.).

3. Credit Card Data

Account numbers prohibited on receipts: Credit card processors are prohibited from allowing the printing of more than the last five digits of a person's credit card number or the expiration date of the card on any receipt provided to the cardholder. The prohibition applies only to electronically printed receipts and is inapplicable to transactions in which the sole means of recording the credit card number is by handwriting or an imprint of the card (Ariz. Rev. Stat. § 44-1367(A) -(B)). Violations constitute unlawful acts or practices under the state's consumer fraud law, and remedies are available under that law (see Section II.C.).

Breach notification law: Unencrypted credit or debit card data owned or licensed by a business in Arizona that contains personal information would be subject to the state's data breach notification law in the event that a breach is discovered (see Section I.C.8.).

Webpage or e-mail solicitations for fraud or theft: Credit and debit card numbers are included in the definition of "identifying information" for purposes of the prohibition on using a webpage or e-mail to solicit identifying information of individuals for purposes of fraud or theft (see Section I.D.7.).

Data disposal requirements: Specific requirements apply to the disposal or destruction of paper records or documents containing personal information of an individual, including credit and debit card numbers (see Section I.C.7.).

4. Credit Reports

Consumer access to and correction of credit report information: On receiving adequate identification credentials by a consumer, a creditor who denies credit to that consumer must disclose the name and address of any consumer reporting agency that furnished a consumer report considered by the creditor (Ariz. Rev. Stat. § 44-1693(1)). Similar requirements apply to licensing agencies who have denied a license and to employers who have denied employment, promotion, or retention of employment based on information in a credit report (Ariz. Rev. Stat. § 44-1693(2) -(3)). Finally, consumer reporting agencies must disclose the contents of the consumer's file under requirements specified by statute (Ariz. Rev. Stat. § 44-1693(4)).

In addition, consumers disputing the accuracy of their credit reports may give written notice to a consumer reporting agency specifying the inaccuracy, and the agency must investigate and document the status of the disputed information at no charge (Ariz. Rev. Stat. § 44-1694(A)). The agency must admit or deny the inaccuracy to the consumer within 30 days of receipt of notice. Any denial must include the basis for denial, a copy of the consumer's file as revised as a result of the investigation, and a notice stating that the agency will provide a description of the procedure used in the investigation if requested (Ariz. Rev. Stat. § 44-1694(B)). If the agency admits that an item is inaccurate, it must immediately correct the item and, on consumer request, must inform any person who received a report containing the incorrect information in the last six months (Ariz. Rev. Stat. § 44-1694(C)). A consumer may provide a written statement to the agency, and unless there are reasonable grounds to believe that the statement is frivolous or irrelevant, the agency must include it in the consumer's file if the statement regards an item that the agency denies is inaccurate or if the statement regards the contents of the consumer's file (Ariz. Rev. Stat. § 44-1694(D)). The agency may limit the statement to 100 words, provided it assists the consumer in writing it (Ariz. Rev. Stat. § 44-1694(E)). An agency is liable for any damages incurred by a consumer as a result of the

reporting of inaccurate information that the agency refused to correct as outlined above (Ariz. Rev. Stat. § 44-1695(B)).

Security freezes: Consumers have the right to request a consumer credit reporting agency to place a security freeze on their credit report, and an agency may not release a credit report or credit score to a third party subject to such a freeze without the consumer's prior express authorization. However, an agency may advise a specific party that a security freeze is in place (Ariz. Rev. Stat. § 44-1698(A)). The statute requires that the freeze be put in place not more than 10 business days after receipt of a written request, and provides requirements for confirming the request, periods for which the freeze remains in effect, and procedures for partial removal, temporary removal, or permanent removal (Ariz. Rev. Stat. § 44-1698(B) -(M)).

The prohibitions outlined above do not apply to uses of a credit report or credit score under statutorily prescribed circumstances, including in connection with certain financial transactions, governmental or court actions, or the provision of a credit report or score by the consumer's request, among others (Ariz. Rev. Stat. § 44-1698(N)). Violations are considered to be unlawful practices under the state's consumer fraud law and are subject to a private action (see Section I.G.1.) and action by the Attorney General (see Section II.C.) (Ariz. Rev. Stat. § 44-1698(P)).

Specific provisions apply to the placement of credit freezes on the credit report or record of a protected person. A "protected person" is defined as an individual who is under age 16 or who is an incapacitated person or a protected person for whom a guardian or conservator has been appointed. The requirements for the placement of freezes, procedures regarding the lifting of a freeze, and exceptions to the requirements are similar to those described above (Ariz. Rev. Stat. § 44-1698.02). Violations are considered to be unlawful practices under the state's consumer fraud law and are subject to a private action and action by the Attorney General (Ariz. Rev. Stat. § 44-1698.02(K)).

Identity verification requirements: Any person who does not use a consumer credit report in connection with approving an application for extension of credit must, prior to lending money or extended credit, take reasonable steps to verify the customer's identity and to confirm that the application is not the result of identity theft (see Section I.G.2.). A person who uses a consumer credit report in making such a determination must only follow these verification steps if the creditor has received a notification that a police report has been filed with a consumer reporting agency or the applicant has been a victim of identity theft, or if the creditor has received notification that the consumer has placed a fraud alert or security freeze on the consumer's credit report (Ariz. Rev. Stat. § 44-1698.01(A) -(B)).

5. Criminal Records

There are no general Arizona laws governing the privacy of criminal record information. The Civil Rights Division of the Attorney General's Office has issued guidance suggesting that an employer may make pre-employment inquiries of applicants regarding prior convictions, including when and where the convictions took place and their final disposition. However, the employer must include a statement that a conviction will not be an absolute bar to employment (Guide to Pre-Employment Inquiries Under the Arizona Civil Rights Act, Office of the Attorney General, Civil Rights Division).

State agencies are not prohibited from inquiring into information regarding the criminal record of persons seeking employment or the issuance of a license, permit, or certificate, but employment may not be denied, and a license, permit, or certificate may not be denied, based solely on a prior conviction for a felony or misdemeanor inside or outside Arizona unless the offense has a reasonable relationship to the functions of the employment or the occupation for which the person is seeking a license, permit, or certificate (Ariz. Rev. Stat. § 13-904(E)). The prohibition is inapplicable to law enforcement agencies (Ariz. Rev. Stat. § 13-904(F)).

6. Drivers' Licenses/Motor Vehicle Records

Use of driver's license information by retailers: Specific requirements apply to retailers using information from a customer's driver's license or other state issued ID (see Section I.E.8.).

Webpage or e-mail solicitations for fraud or theft: Driver's license numbers are included in the definition of "identifying information" for purposes of the prohibition on using a webpage or e-mail to solicit identifying information of individuals for purposes of fraud or theft (see Section I.D.7.).

Data disposal requirements: Specific requirements apply to the disposal or destruction of paper records or documents containing personal information of an individual, including driver's license numbers (see Section I.C.7.).

7. Electronic Communications/Social Media Accounts

A person may not, with intent to commit fraud or theft, use a webpage or an e-mail message, or otherwise use the Internet, to solicit, request, or take an action to induce a person to provide identifying information by representing, directly or by implication, that the person is an online business without the consent and approval of the online business (Ariz. Rev. Stat. § 18-542). "Identifying information" is defined as an individual's piece of information that can be used to access an individual's financial accounts or to obtain goods or services and that contains an individual's social security number, driver license number, bank account number, credit or debit card number, personal ID number, automated or electronic signature, unique biometric data, or account password (Ariz. Rev. Stat. § 18-541(2)). A private cause of action for a violation of these provisions is available (see Section I.G.1.), and the Attorney General may bring an action for injunctive relief and a civil penalty (see Section II.C.). In addition, a violation is a class 5 felony (see Section I.H.).

8. Financial Information

Social security number restrictions on government agencies: A government agency may not transmit to an individual any material that contains both the individual's social security number (SSN) and his bank, savings and loan association, or credit union account number. This prohibition does not apply to documents including such data that are sent as part of an application or enrollment process; to establish, amend, or terminate an account, contract, or policy; or to confirm the accuracy of the SSN or account number (Ariz. Rev. Stat. § 44.1373(F)). In addition, documents or records recorded and made available on an entity's public website may not contain an individual's credit card, charge card, or debit card numbers; retirement account numbers; or savings, checking, or securities entitlement account numbers (Ariz. Rev. Stat. § 44.1373(G)). Civil penalties are available for a violation of the restrictions on recording SSNs or financial information on websites (see Section II.C.).

Webpage or e-mail solicitations for fraud or theft: Information that can be used to access an individual's financial accounts and that contains specified elements such as social security numbers, credit and debit card numbers, bank account numbers, or account passwords, is included in the definition of "identifying information" for purposes of the prohibition on using a webpage or e-mail to solicit identifying information of individuals for purposes of fraud or theft (see Section I.D.7.).

Breach notification law: Unencrypted financial information owned or licensed by a business in Arizona that contains personal information would be subject to the state's data breach notification law in the event that a breach is discovered (see Section I.C.8.).

9. Health Data

In general: All medical records and payment records, and the information contained therein, are privileged and confidential. (Ariz. Rev. Stat. § 12-2292). For purposes of this requirement and those

that follow with respect to patient access and provider disclosure requirements, a "health care provider" is defined as any person licensed pursuant to the Professions and Occupations Title of the Arizona Revised Code who maintains medical records; a health care institution as defined by Ariz. Rev. Stat. § 36-401(21); an ambulance service licensed under Ariz. Rev. Stat. § 36-2201(7); and a health care service organization licensed under the Insurance Code (Ariz. Rev. Stat. § 12-2291(5)). Accordingly, the requirements apply to a host of health care institutions and providers, including hospitals, pharmacists, dentists, nurses, optometrists, pharmacists, occupational therapists, accredited health care institutions, and other medical specialists.

Patient access: On the written request of a patient or the patient's health care decision maker, a health care provider must provide access to or copies of the patient's medical and payment records (Ariz. Rev. Stat. § 12-2293(A)). Access may be denied if a health professional determines that (a) access by the patient is reasonably likely to endanger the life or safety of the patient or another person; (b) the records reference another person other than a health professional who will likely be caused substantial harm by the disclosure; (c) access by the patient's health care decision maker is reasonably likely to cause substantial harm to the patient or another person; or (d) access would reveal information obtained under a promise of confidentiality with someone other than a health professional, and access would be reasonably likely to reveal the source (Ariz. Rev. Stat. § 12-2293(B)).

Access also may be denied if the health care provider determines that the information was obtained in the course of clinical research and the patient or the patient's health care decision maker agreed to denial of access until completion of the research, or if the provider is, or is acting under the direction of, a correctional institution and access by a patient who is an inmate would jeopardize the health, safety, security, or custody of the patient, other inmates, or officers or employees at the institution (Ariz. Rev. Stat. § 12-2293(C)).

If a health care provider denies access to or copies of medical or payment records, the provider must note the determination in the patient's records and must provide a written explanation of the reasons for the denial to the patient or the patient's health care decision maker (Ariz. Rev. Stat. § 12-2293(D)).

Disclosure requirements: Health care providers may not disclose a patient's medical record or payment record, or the information contained therein, without written authorization by the patient, unless authorized by law (Ariz. Rev. Stat. § 12-2292; see also Ariz. Rev. Stat. § 12-2294(B)). Health care providers may disclose such records without written authorization when ordered by a court or tribunal (Ariz. Rev. Stat. § 12-2294(A)). In addition, such records may be disclosed without written authorization as otherwise authorized under the federal Health Insurance Portability and Accountability Act (the HIPAA Privacy Rule), or under a variety of statutory exceptions, including to health care providers who are currently providing or have previously provided treatment to the patient, to private accrediting agencies or regulatory boards, for purposes of utilization review, to persons providing services to the health care provider that have an agreement with the provider to follow HIPAA standards, to a legal representative for securing legal advice, or to a patient's third-party payor (Ariz. Rev. Stat. § 12-2294(C)). Specific requirements apply to medical or payment records of deceased patients (Ariz. Rev. Stat. § 12-2294(D)), as well as to medical or payment records subject to a subpoena (Ariz. Rev. Stat. § 12-2294.01).

A person who receives medical records or information as outlined above may not disclose them without the written authorization of the patient or the patient's health care decision maker (Ariz. Rev. Stat. § 12-2294(E)). If a health care provider releases medical records or payment records to a contractor for purposes of duplicating or disclosing them on behalf of the provider, the contractor must adhere to the disclosure restrictions described above and must return the records to the provider after the duplication or disclosure (Ariz. Rev. Stat. § 12-2294(F)).

Charges: Health care providers may charge a reasonable fee to any person requesting copies of medical records or payment records, payable in advance. No charge may be made for records provided to other providers for providing continuing care, to the patient to whom the records pertain (or to the patient's health care decision maker) for the demonstrated purpose of obtaining health care, or to state and local boards and departments (Ariz. Rev. Stat. § 12-2295).

Record retention: Medical records subject to these requirements must generally be retained for six years from the last date the patient received services from the health care provider (Ariz. Rev. Stat. § 12-2297).

Remedies: The law does not specify remedies, but does provide that a health care provider who acts in good faith is immune from liability. Accordingly, there would appear to be an implied right to a private cause of action for a violation of the requirements (Ariz. Rev. Stat. § 12-2296; see Section I.G.4).

Chronic disease surveillance system: Under the law establishing a chronic disease surveillance system in Arizona, the Department of Health Services may authorize other persons to use data from the system to study the sources of cancer, birth defects, or other diseases and to evaluate services and programs related to them (Ariz. Rev. Stat. § 36-133(D)). However, information collected on individuals by the surveillance system that can identify the individual is confidential and may only be used for specified purposes. Any person who discloses confidential information in violation of this provision is guilty of a class 3 misdemeanor (Ariz. Rev. Stat. § 36-133(F)).

Communicable disease information: A person who obtains communicable disease-related information in the course of providing a health service or who obtains that information pursuant to an authorization may not disclose or be compelled to disclose the information except under a variety of circumstances, including to the protected person, to health care providers or first responders with exposure risk, to health care facilities and providers under specified conditions, to government agencies, pursuant to court orders, or to persons authorized by the patient or the patient's health care decision maker, among others (Ariz. Rev. Stat. § 36-664(A)(1) -(18)). Additional exceptions apply to disclosures to the Department of Child Safety and disclosures by state, county, or local health departments, as well as disclosures to good Samaritans (Ariz. Rev. Stat. § 36-664(B) - (E)).

A disclosure authorization under this provision must be signed by the protected person or his health care decision maker and must specify to whom disclosure is allowed, the purpose of the disclosure, and the time period for which it is effective. A general authorization is not an authorization for release of HIV-related information unless the authorization specifically indicates as much (Ariz. Rev. Stat. § 36-664(F)). Any person to whom information is disclosed pursuant to an authorization outlined above may not disclose the information to another person in violation of the statutory requirements (Ariz. Rev. Stat. § 36-664(G)).

Court-ordered disclosures of communicable disease-related information are generally prohibited unless a statutory exception applies (Ariz. Rev. Stat. § 36-665).

A person who discloses, compels another to disclose, or procures the disclosure of communicable disease-related information in violation of the statutory requirements is guilty of a class 3 misdemeanor (Ariz. Rev. Stat. § 36-666(A)(2); see Section I.H.). In addition, the Department of Health may impose a civil penalty for a violation (see Section II.C.), and a private cause of action is available (see Section I.G.4).

Genetic testing results: Genetic testing and information derived from such testing is confidential and may be released only to specified individuals, including the person tested or that person's health care decision maker, any person specifically authorized in writing by the person tested to receive the information, or researchers or health care providers subject to delineated requirements

(Ariz. Rev. Stat. § 12-2802(A)). A person further may not disclose, or be compelled to disclose, the identity of a person on whom genetic testing is performed or the results of a genetic test that allows identification of the person, except as outlined above (Ariz. Rev. Stat. § 12-2802(B)). A person to whom genetic testing information has been disclosed may not disclose the information to any other person (Ariz. Rev. Stat. § 12-2802(F)). Health care providers and their agents and employees may be subject to civil liability for a violation (see Section I.G.4).

Mental health services: Any person undergoing evaluation or treatment pursuant to law provisions governing mental health services has the right to examine the written treatment program and the medical record, unless the attending physician or his designee determines that an examination is contraindicated or if the circumstances for refusing access under the general rules governing medical and records (see above, "Patient access") are met. A determination that examination is contraindicated must be noted in the patient's record (Ariz. Rev. Stat. § 36-507(3)).

Any records, and information contained in such records, collected under the law governing mental health services must be kept confidential, unless specified exceptions apply, including disclosures to physicians involved in a patient's care, disclosures to individuals to whom disclosure has been authorized by the patient or the patient's health care decision maker, disclosures required by court order, disclosures to government agencies under specified circumstances, or disclosures for research, utilization review, or statistical purposes, among others (Ariz. Rev. Stat. § 36-509(A)(1) -(21)). Information disclosed to a family member or close friend of the patient pursuant to the exception outlined in Ariz. Rev. Stat. § 36-509(A)(7) may include only information that is directly relevant to the person's involvement with the patient's health care or payment related to the patient's health care. A health care entity must keep a record of the name and contact information of any person to whom information is disclosed under this subsection (Ariz. Rev. Stat. § 36-509(B)). A health care entity that acts in good faith is not liable for damages in any civil action for disclosure of medical or payment records; accordingly, a private cause of action is implied in the statute (see Section I.G.4).

Breach notification law: Unencrypted health data owned or licensed by a business in Arizona that contains personal information would be subject to the state's data breach notification law in the event that a breach is discovered (see Section I.C.8.).

10. Social Security Numbers

In general: No person or entity may do any of the following:

- intentionally communicate or otherwise make an individual's social security number (SSN) available to the general public;
- print an individual's SSN on any card required for an individual to receive products or services provided by the person or entity;
- require the transmission of an individual's SSN over the Internet unless the connection is secure or the SSN is encrypted;
- require the use of an individual's SSN to access a website, unless a password or unique identification number or other authentication device is also required for access; or
- print a number that the person or entity knows to be an individual's SSN on any materials mailed to the individual, unless required by federal or state law (Ariz. Rev. Stat. § 44-1373(A)(1) -(5)).

Exceptions to prohibition: The prohibition on mailing materials including an SSN does not apply to documents sent as part of an application or enrollment process; to establish, amend, or terminate an account, contract, or policy; or to confirm the accuracy of the SSN. If a person or entity receives a number from a third party, the person or entity has no duty to inquire or otherwise determine if the number is, or contains, an individual's SSN, and may print that number on

materials mailed to the individual unless the person or entity has actual knowledge that the number is, or contains, the individual's SSN. Finally, a person or entity is not prohibited from mailing a copy or reproduction of a document that includes an SSN to an individual if the SSN was included on the original before Jan. 1, 2005 (Ariz. Rev. Stat. § 44-1373(A)(5)).

In addition to the exceptions listed above, the law does not prohibit the collection, use, or release of an SSN as required by federal or state law or for internal verification or administrative purposes (Ariz. Rev. Stat. § 44-1373(C)).

Continuous use exception: A person or entity using an individual's SSN in contravention of the above requirements prior to Jan. 1, 2005, may continue to do so after that date if the use is continuous (the post 2005 requirements apply immediately after any stoppage of use) and the person or entity provides an annual written disclosure of the individual's right to stop the use of the SSN. If the individual requests in writing, the person or entity must stop using the SSN within 30 days of the request. No fee may be charged for implementing the request, and the person or entity may not deny services to the individual because of the request (Ariz. Rev. Stat. § 44-1373(B)).

Applicability to government subdivisions and state agencies: While the prohibitions outlined above are generally applicable to state agencies and political subdivisions of Arizona, the law does not prohibit such entities from disseminating or using the last four numbers of an individual's SSN (Ariz. Rev. Stat. § 44-1373(E)). However, a government agency may not transmit to an individual any material that contains both the individual's SSN and his bank, savings and loan association, or credit union account number. This prohibition does not apply to documents including such data that are sent as part of an application or enrollment process; to establish, amend, or terminate an account, contract, or policy; or to confirm the accuracy of the SSN or account number (Ariz. Rev. Stat. § 44-1373(F)).

Information on websites: Documents or records recorded and made available on an entity's public website may not contain more than five numbers that are reasonably identifiable as being part of an individual's SSN and may not contain an individual's credit card, charge card, or debit card numbers; retirement account numbers; or savings, checking, or securities entitlement account numbers (Ariz. Rev. Stat. § 44-1373(G)).

Remedies: Civil penalties are available for a violation of the restrictions on recording SSNs or financial information on websites (see Section II.C.).

Specific requirements applicable to educational institutions: A university under the jurisdiction of the Arizona Board of Regents may not use the SSN of a faculty or staff member or student as that person's identification number. Any student who was assigned an ID number under the state's student accountability information system after June 30, 2006, must have an ID number with the university corresponding to that number. Universities may not allow the display of an individual's SSN, or any four or more consecutive numbers contained in an individual's SSN, on any Internet site maintained by the university or any other publicly available document for any purpose (Ariz. Rev. Stat. § 15-1823(A)). Similar requirements apply to community colleges, although the details vary to some degree with respect to transition requirements after the law's effective date (Ariz. Rev. Stat. § 15-1823(B) -(A)).

Data disposal requirements: Specific requirements apply to the disposal or destruction of paper records or documents containing personal information of an individual, including social security numbers (see Section I.C.7.).

Breach notification law: Unencrypted data owned or licensed by a business in Arizona that contains personal information, including social security numbers, would be subject to the state's data breach notification law in the event that a breach is discovered (see Section I.C.8.).

11. Usernames & Passwords

No person or entity may require the use of an individual's SSN to access a website, unless a password or unique identification number or other authentication device is also required for access (Ariz. Rev. Stat. § 44.1373(A)(4)).

An account number or credit or debit card number in combination with a password, when combined with an individual's first name or first initial and last name, meets the definition of "personal information" subject to data breach notification requirements (see Section I.C.8.).

12. Information about Minors

A person may not knowingly perform an abortion on a pregnant unemancipated minor unless the attending physician has secured the written and notarized consent of one of the minor's parents or a guardian or conservator, or unless authorized by a judge of the superior court under specified circumstances (Ariz. Rev. Stat. § 36-2152).

Under provisions governing access to and disclosure of medical and payment record information (see Section I.D.9.), a "health care decision maker" is defined to include a parent of a minor authorized to make decisions on the minor's behalf under Arizona law (Ariz. Rev. Stat. § 12-2291(4)).

Under the Parents' Bill of Rights, a parent has the right to access and review all medical records of the minor child unless otherwise prohibited by law or if the parent is the subject of a criminal investigation of a crime committed against the minor and a law enforcement official requests that the information not be released (Ariz. Rev. Stat. § 1-602(6)). Parents also have the right to consent in writing before a biometric scan of their minor child is made and before any record of the child's blood or DNA is created, stored, or shared unless an exception applies (Ariz. Rev. Stat. § 1-602(7) - (8)). Finally, parents have the right to consent in writing before the state or any of its political subdivisions makes a video or voice recording of a minor child, unless the recording is made as part of a court proceeding or pursuant to other specified law enforcement activities (Ariz. Rev. Stat. § 1-602(8)).

13. Location Data

There are no laws in Arizona governing the privacy and security of location data.

14. Other Personal Data

There are no other Arizona provisions regarding data beyond those specified above.

E. SECTOR-SPECIFIC PROVISIONS

1. Advertising & Marketing

Anti-spam law: A person may not knowingly transmit commercial e-mail if the person falsifies e-mail transmission information or other routing information for unsolicited commercial e-mail, the e-mail contains false or misleading information in the subject line, or the person uses a third party's Internet address or domain name without the third party's consent for purposes of transmitting e-mail in a manner that makes it appear that the third party was the sender (Ariz. Rev. Stat. § 44-1372.01(A)). A person sending unsolicited commercial e-mail or maintaining a database for the purpose of sending such e-mails must do the following:

- use the characters "ADV:" as the first four characters in the subject line of the unsolicited commercial e-mail;
- provide a procedure allowing recipients, at no cost, to easily remove themselves from the list (after which the recipient's name must be removed within three business days), and

restrict the future sale or transfer of the recipient's e-mail address to another person or organization for the purpose of sending commercial e-mail (Ariz. Rev. Stat. § 44-1372.01(B)).

The prohibition applies to any person doing business in Arizona and to any person transmitting a commercial e-mail (a) from a computer located in the state, (b) to an e-mail address that the sender knows, or has reason to know, is held by an Arizona resident, or (c) to an interactive computer service with equipment or its principal place of business in Arizona (Ariz. Rev. Stat. § 44-1372.01(E)).

Failure to comply is an unlawful practice under the state's consumer fraud law and is subject to investigation by the Attorney General (see Section II.C.). In addition, a person injured by a violation may recover damages (see Section I.G.1.). Finally, a violation of these provisions is a class 2 misdemeanor (Ariz. Rev. Stat. § 44-1372.05).

It should be noted that the federal CAN-SPAM Act preempts state claims that are not based on traditional tort theories of falsity and deception (15 U.S.C. §7707(b)(1)).

Do-not-call and telephone solicitation: A seller or solicitor may not initiate an outbound telephone solicitation call to any number that is entered in the national Do-Not-Call Registry unless a specified exception applies (Ariz. Rev. Stat. § 44-1282(A)). A violation is deemed to be an unlawful practice under the state's consumer fraud law, and the Attorney General may investigate and take appropriate action, including a civil penalty (see Section II.C.).

In addition, under the state's telephone solicitations law, telemarketing companies must register with the state unless an exception applies (Ariz. Rev. Stat. § 44-1272 and Ariz. Rev. Stat. § 44-1273) and must disclose to consumers (a) the true name and address of the solicitor and that the purpose of the call is to sell merchandise, and (b) that the consumer has the right to cancel an order within three business days after receiving the merchandise, among other required disclosures (Ariz. Rev. Stat. § 44-1276). Specific requirements apply to sellers offering or selling business opportunities in the state (Ariz. Rev. Stat. § 44-1276.01). Unregistered sellers engaging in telephone solicitation are guilty of a class 5 felony (Ariz. Rev. Stat. § 44-1277). In addition, a consumer may rescind a sale by an unregistered seller at any time and may recover any purchase money paid, financial damages caused by the unregistered seller, and reasonable attorney fees and costs (Ariz. Rev. Stat. § 44-1279).

Right of publicity for soldiers: The right to control and to choose whether and how to use a soldier's name, portrait, or picture for commercial purposes is recognized as the soldier's right of publicity. A person is liable for using a soldier's name, portrait, or picture without obtaining prior consent from the soldier or the soldier's representative if the person uses it for advertising any goods, wares, or merchandise; soliciting patronage of a business; or receiving consideration for the sale of any goods, wares, or merchandise (Ariz. Rev. Stat. § 12-761(A) to Ariz. Rev. Stat. § 12-761(B)). Certain exceptions apply, including using a soldier's name, portrait, or picture in an artistic portrayal, for noncommercial purposes, or in an exhibit by a professional photographer, among others (Ariz. Rev. Stat. § 12-761(H)). A private cause of action is available for violations (see Section I.G.1.). In addition, the use of the name, portrait, or picture of a deceased soldier without the prior consent of the soldier or a representative is a class 1 misdemeanor (Ariz. Rev. Stat. § 13-3726).

Breach notification law: Businesses in the advertising and marketing sector who maintain unencrypted computerized data that includes "personal information" as defined in the Arizona data breach notification law are subject to the law's notification requirements if they become aware of an incident of unauthorized acquisition and access to such data (see Section I.C.8.).

SSN requirements: Requirements regarding the use and disclosure of social security numbers would apply to businesses in the advertising and marketing sector to the extent that they collect or use such information (see Section I.D.10.).

2. Education

Parental consent to collection of pupil personal information: A school district or charter school must obtain written informed consent from the parent of a pupil before administering any survey that is retained by the district, charter school, or the Department of Education for longer than one year and that solicits personal information about the pupil about a variety of topics specified by law, including critical appraisals of another person with whom a pupil has a close relationship; illegal, antisocial, or self-incriminating behavior; financial or medical information; political information; pupil biometric information; religious practices; or sexual behavior, among others (Ariz. Rev. Stat. § 15-117(A)(1) to Ariz. Rev. Stat. § 15-117(A)(14)).

Districts and charter schools must obtain the written consent described above at the beginning of the school year, although if a pupil is age 18 or older, only the pupil's consent is required. A parent may revoke consent at any time. Teachers are specifically prohibited from administering any survey without written authorization from the district or charter school (Ariz. Rev. Stat. § 15-117(B)). The law does not apply to mental health screenings, class instruction, college entrance exams, surveys that do not require a student's name or other personally identifiable information, surveys conducted by the Arizona Criminal Justice Commission, or any method of surveying based on a reasonable belief that a minor has been a victim of abuse (Ariz. Rev. Stat. § 15-117(D)).

Parents or pupils may not be subject to a penalty for failure to participate in a survey (Ariz. Rev. Stat. § 15-117(E)). District and charter schools must provide any information on a survey regarding dates, methodology, types of information collected, and reasons for conducting the survey to a parent of a pupil on request (Ariz. Rev. Stat. § 15-117(J)).

Parents having a reasonable belief that a district or charter school has violated the above provisions may file a complaint with the Attorney General or a county attorney for the county in which the alleged violation occurred, who then may initiate a suit to compel compliance and for civil penalties (see Section II.C.).

Adoption of FERPA: Arizona has requirements under the federal Family Educational Rights and Privacy Act (FERPA) regarding parents' rights regarding the release of, or access to, student records. The federal law requirements provide, among other items, that schools must provide students and pupils over the age of 18 with their rights under the law, including the right to review and inspect records; the right to request that incorrect or misleading information be fixed or that they have rights, including a hearing request, if such the request is refused; and the right to give written permission before such records are disclosed to a third party, unless an exception applies (Ariz. Rev. Stat. § 15-141(A); see also 20 U.S.C. § 1232g, et seq.).

In addition to any federal remedies available under FERPA, a superior court may grant injunctive or special action relief if an educational agency or institution or an employee or agent thereof fails to comply with FERPA requirements, without regard to whether the agency or institution actually is receiving federal funding (Ariz. Rev. Stat. § 15-141(B)). Exceptions to the requirements are provided for releases of student records related to specified juvenile corrections matters, or to law enforcement agencies and county attorneys pursuant to an intergovernmental agreement to create a juvenile justice network (Ariz. Rev. Stat. § 15-141(C) -(F)).

No pupil transcripts may be released to representatives of postsecondary institutions, the militia of Arizona, or the armed services of the U.S. without the consent of the pupil (Ariz. Rev. Stat. § 15-142(B)).

Pupil biometric information: A school in a school district or a charter school may not collect biometric information from a pupil unless the pupil's parent or guardian gives written permission for the collection (Ariz. Rev. Stat. § 15-109(A); see Section I.D.1).

Teacher fingerprint data: Specified applicants for new or renewed teaching certificates or persons required to be fingerprinted for new or continued employment in a charter school must submit for an identity-verified fingerprint card that will be used by the Department of Public Safety to process a fingerprint clearance card as required by law (Ariz. Rev. Stat. § 15-106). The statute sets the requirements for application (Ariz. Rev. Stat. § 15-106(1) -(10)). An entity contracted by the Department to collect the information must comply with all information privacy and security measures established by the Department, as well as the Department's information technology security policy (Ariz. Rev. Stat. § 15-106(6)).

Breach notification law: Businesses in the education sector who maintain unencrypted computerized data that includes "personal information" as defined in the Arizona data breach notification law are subject to the law's notification requirements if they become aware of an incident of unauthorized acquisition and access to such data (see Section I.C.8.).

Social security numbers: Universities under the jurisdiction of the Arizona Board of Regents and community colleges may not use the social security number of a faculty or staff member or student as that person's identification number (Ariz. Rev. Stat. § 15-1823). In addition, the requirements regarding the use and disclosure of social security numbers apply to the education sector to the extent that they collect or use such information. For a discussion of both requirements, see Section I.D.10.

Student Data: Ariz. Rev. Stat. § 15-1046 prohibits operators of web sites and mobile apps primarily used and designed for school purposes from selling or renting a student's information or from knowingly disclosing a student's information under certain circumstances. It also requires operators to implement and maintain reasonable security procedures and practices.

3. Electronic Commerce

Breach notification law: Businesses in the electronic commerce sector who maintain unencrypted computerized data that includes "personal information" as defined in the Arizona data breach notification law are subject to the law's notification requirements if they become aware of an incident of unauthorized acquisition and access to such data (see Section I.C.8.).

SSN requirements: Requirements regarding the use and disclosure of social security numbers would apply to businesses in the economic services sector to the extent that they collect or use such information (see Section I.D.10.).

4. Financial Services

Breach notification law: Businesses in the financial services sector who maintain unencrypted computerized data that includes "personal information" as defined in the Arizona data breach notification law are subject to the law's notification requirements if they become aware of an incident of unauthorized acquisition and access to such data (see Section I.C.8.).

SSN requirements: Requirements regarding the use and disclosure of social security numbers would apply to businesses in the financial services sector to the extent that they collect or use such information (see Section I.D.10.).

Data disposal requirements: Specific requirements apply to the disposal or destruction of paper records or documents containing personal information of an individual, including retirement account numbers and savings, checking, or securities entitlement account numbers (see Section I.C.7.).

Insurance provisions: For information on insurance code provisions governing the collection, use, and disclosure of personal information, including information regarding an individual's finances, see Section I.E.7.

5. Health Care

Medical and payment record information: General access and disclosure requirements applicable to medical and payment records and information apply to hospitals, physicians, and other health care facilities and practitioners. In addition, the law contains requirements applicable to specific providers and facilities. For information on these requirements, see Section I.D.9.

Breach notification law: Businesses in the health care sector who maintain unencrypted computerized data that includes "personal information" as defined in the Arizona data breach notification law are subject to the law's notification requirements if they become aware of an incident of unauthorized acquisition and access to such data (see Section I.C.8.).

SSN requirements: Requirements regarding the use and disclosure of social security numbers would apply to businesses in the health care sector to the extent that they collect or use such information (see Section I.D.10.).

Insurance provisions: For information on insurance code provisions governing the collection, use, and disclosure of personal information, including medical record and health information, see Section I.E.7.

6. HR & Employment

The primary Arizona laws governing privacy requirements applicable to employers govern electronic surveillance and drug testing. For information on electronic surveillance, see Section I.F. The drug testing law, and other privacy laws applicable to employers, are outlined in detail below.

Drug testing provisions: Employers are permitted to test employees for the presence of drugs or alcohol, provided that statutory requirements are met (Ariz. Rev. Stat. § 23-493.01). Testing of current employees must take place during, or immediately before or after, an employee's normal working hours. Employers must pay for tests on current employees and may pay for tests on prospective employees if they choose. If a test is conducted at a location other than the employee's normal worksite, the employee is entitled to reasonable transportation costs (Ariz. Rev. Stat. § 23-493.02). The law specifies testing procedure and policy requirements, together with permissible disciplinary actions resulting from positive tests (Ariz. Rev. Stat. § 23-493.03 through Ariz. Rev. Stat. § 23-493.05).

Any communications received by an employer relevant to drug or alcohol test results received pursuant to tests conducted under the employer's testing policy are confidential and may not be disclosed in any public or private proceeding, except in an action brought by the employer against the employee, or to (a) the employee, prospective employee, or a designate, (b) an individual designated by the employer to receive and evaluate test results or hear the explanation of an employee or prospective employee, or (c) an arbitrator or mediator, or court or governmental agency (Ariz. Rev. Stat. § 23-493.09(A)). Employees have the right to access test results, subject to the maintenance of confidentiality of other individuals (Ariz. Rev. Stat. § 23-493.09(B)).

Criminal records inquiries: Although there are no Arizona laws governing inquiries by employers into the criminal records of employees or applicants, the Civil Rights Division of the Attorney General's Office has issued guidance suggesting that an employer may make pre-employment inquiries of applicants regarding prior convictions, including when and where the convictions took place and their final disposition. However, the employer must include a statement that a conviction will not be an absolute bar to employment (Guide to Pre-Employment Inquiries Under the Arizona Civil Rights Act, Office of the Attorney General, Civil Rights Division).

State agencies are not prohibited from inquiring into information regarding the criminal record of persons seeking employment, but employment may not be denied based solely on a prior conviction for a felony or misdemeanor inside or outside Arizona unless the offense has a

reasonable relationship to the functions of the employment (Ariz. Rev. Stat. § 13-904(E)). The prohibition is inapplicable to law enforcement agencies (Ariz. Rev. Stat. § 13-904(F)).

Payroll records: Employers must permit an employee or a designated representative to inspect and copy payroll records pertaining to the employee (Ariz. Rev. Stat. § 23-364(D)).

Medical examinations and inquiries: Under the Arizona Civil Rights Act, no employer may conduct a medical examination or make an inquiry of a job applicant as to whether the applicant is an individual with a disability or with respect to the nature or severity of the disability (Ariz. Rev. Stat. § 41-1466(A)). However, an employer may make pre-employment inquiries into the ability of an applicant to perform job functions, and may require a medical examination after an offer of employment is made under specified circumstances. All entering employees must be subject to the examination regardless of disability, and information obtained as a result of such testing must be collected and maintained on separate forms in a separate medical file. Such information must be treated as a confidential medical record, except that the employer may inform supervisors of necessary duty restrictions, may inform first aid personnel as appropriate if an employee may require emergency treatment, and may provide information to government officials examining the employer's compliance with the requirements outlined above (Ariz. Rev. Stat. § 41-1466(B)).

With respect to current employees, medical examinations and inquiries with respect to disability are not permitted unless the examination or inquiry is shown to be job related and consistent with business necessity (Ariz. Rev. Stat. § 41-1466(C)). However, employers may conduct voluntary medical examinations as part of an employee health program and may inquire into an employee's ability to perform job functions (Ariz. Rev. Stat. § 41-1466(D)). The disclosure restrictions described above with respect to prospective employees are similarly applicable to information obtained from current employees (Ariz. Rev. Stat. § 41-1466(E)).

References: It is permissible for a former employer to provide a requesting employer information concerning a person's education, training, experience qualifications, and job performance to be used in evaluating a person for employment. In addition, it is lawful for school districts to provide fingerprint check information to another school district if requested to do so by the subject of the fingerprinting. A copy of any such communication must be sent by the former employer to the former employee's last known address (Ariz. Rev. Stat. § 23-1361(B)). Specific requirements apply to references made or requested by banks and other financial entities (Ariz. Rev. Stat. § 23-1361(G) to Ariz. Rev. Stat. § 23-1361(H)).

A private cause of action is available for violations, but employers sending reference information as described above are immune from liability if they act in good faith. For more information on potential liabilities, see Section I.G.4

Breach notification law: Employers who maintain unencrypted computerized data that includes "personal information" as defined in the Arizona data breach notification law are subject to the law's notification requirements if they become aware of an incident of unauthorized acquisition and access to such data (see Section I.C.8.).

SSN requirements: Requirements regarding the use and disclosure of social security numbers apply to employers to the extent that they collect or use such information (see Section I.D.10.).

7. Insurance

Insurance Information and Privacy Protection Act: The Arizona Insurance Information and Privacy Protection Act (IIPPA; Ariz. Rev. Stat. § 20-2101, et seq.) governs requirements that insurers must follow with respect to the collection, use, and disclosure of personal information, including access and correction requirements. The provisions of the law are outlined in detail below.

Primary definitions: The IIPPA applies to insurance institutions, insurance producers, and insurance support organizations that collect, receive, or maintain information from Arizona residents (for purposes of life, health, or disability insurance), or that collect, receive, or maintain information in connection with policies, contracts, or certificates of insurance issued in the state (for purposes of property or casualty insurance) (Ariz. Rev. Stat. § 20-2101(A)). Each of these insurers is defined by law (Ariz. Rev. Stat. § 20-2102(10), (11) and (13)). A partial exemption from the law is applicable to insurance institutions subject to the requirements of the federal Health Insurance Portability and Accountability Act (the HIPAA Privacy Rule), provided they are in compliance with federal requirements (Ariz. Rev. Stat. § 20-2122).

"Personal information" is defined as any individually identifiable information gathered in connection with an insurance transaction and from which a judgment may be made about an individual's character, habits, avocations, finances, occupation, general reputation, credit, health, or other personal characteristics. It specifically includes a person's name and address and medical record information but not privileged information (Ariz. Rev. Stat. § 20-2102(19)). "Medical record information" means personal information relating to an individual's physical or mental condition, medical history, or medical treatment and that is obtained from a medical professional or medical care institution, from the individual, or from the individual's spouse, parent, or legal guardian (Ariz. Rev. Stat. § 20-2102(18)).

Notice of information practices: Insurance institutions and producers must provide a notice of information practices to applicants and policyholders in connection with covered insurance transactions (Ariz. Rev. Stat. § 20-2104(B)(1)). The notice must be provided, in the case of an application, no later than when the insurer delivers the insurance policy or certificate, if the information was collected solely from the applicant or from public records, and when the insurer first collects information from a source other than the applicant or a public record (Ariz. Rev. Stat. § 20-2104(B)(1)). In case of a policy renewal, the insurer must provide the notice at least annually, and in the case of a policy reinstatement or change, not later than the time the insurer receives a request for a reinstatement or change unless a notice was already given within the previous 12 months (Ariz. Rev. Stat. § 20-2104(B)(2) to Ariz. Rev. Stat. § 20-2104(B)(3)).

The notice must be in writing or, if agreed to by the parties, in electronic form and must meet either deferral Gramm-Leach-Bliley Act requirements or requirements outlined in the IIPPA, including whether information may be collected from persons other than the individual, the types of information that may be collected, the types of permissible disclosures, a description of the individual's rights, and a statement that information obtained from an insurance support organization report may be retained by that organization and disclosed to other persons (Ariz. Rev. Stat. § 20-2104(C)). Abbreviated notice is permitted under specific conditions (Ariz. Rev. Stat. § 20-2104(D)), and notice to individual participants or beneficiaries in employee benefit plans, group insurance policies, or workers' compensation plans is not required if notice was provided to the plans themselves (Ariz. Rev. Stat. § 20-2104(F)). Finally notice is not required to lapsed policyholders or to policyholders whose last known address is invalid, as outlined in the IIPPA (Ariz. Rev. Stat. § 20-2104(G) to Ariz. Rev. Stat. § 20-2104(H)).

Disclosure requirements: In general, an insurance institution, producer, or support organization may not disclose any personal or privileged information about an individual collected or received in connection with an insurance transaction unless the disclosure is with the written authorization of the individual (Ariz. Rev. Stat. § 20-2113(1)). The IIPPA specifies, among other items, the elements that must be included in a written authorization form, including that it be written in plain language, that it be dated, the types of persons authorized to make a disclosure and the nature of the information authorized, and the time period for which it is valid, which varies depending on the purpose for which the authorization is sought, but may not exceed 30 months when signed in

support of an application for health insurance and for the term of the policy signed for purposes of a benefit claim (Ariz. Rev. Stat. § 20-2106).

An authorization submitted by another insurance institution, producer, or support organization must meet the written authorization requirements of the IIPPA, and an authorization submitted by a person other than these insurers must be dated, signed by the individual, and obtained one year or less before the date disclosure is sought (Ariz. Rev. Stat. § 20-2113(1)(a) to Ariz. Rev. Stat. § 20-2113(1)(b)).

Exceptions apply to disclosures to a person other than an insurance institution, producer, or support organization that are reasonably necessary to enable the person to perform a business function for the disclosing insurer and if the person agrees not to further disclose unless specified circumstances apply (Ariz. Rev. Stat. § 20-2113(2)(a)), or to enable the person to provide information to the disclosing insurer for purposes of determining eligibility for benefits or detecting criminal activity or fraud (Ariz. Rev. Stat. § 20-2113(2)(b)). In addition, disclosures to insurance organizations, producers, support organizations, and self-insurers are permitted if the information disclosed is limited to an amount reasonably necessary to detect criminal activity or fraud or for the disclosing or receiving insurer to perform its function in an insurance transaction (Ariz. Rev. Stat. § 20-2113(3)). A list of additional exceptions apply, including disclosures to medical care institutions, regulatory authorities, and law enforcement agencies, among others (Ariz. Rev. Stat. § 20-2113(4) to Ariz. Rev. Stat. § 20-2113(17)).

Of particular note, disclosure is authorized to a person whose only use of the information will be in connection with the marketing of a product or service if no medical information, privileged information, or personal information relating to an individual's character or personal habits is disclosed, the individual has been given the opportunity to indicate that he does not want personal information to be disclosed for marketing purposes and has not done so, and the person receiving the information agrees to use it strictly for marketing purposes (Ariz. Rev. Stat. § 20-2113(11)). In addition, an affiliate whose only use of personal information will be for audit or marketing purposes may use such information if it agrees not to disclose the information to an unaffiliated person for any other purpose, but no medical record information may be disclosed for marketing purposes without the written consent of the individual (Ariz. Rev. Stat. § 20-2113(12)).

Access requirements: If any individual, after providing proper identification, submits a written request to an insurance institution, producer, or support organization for access to recorded personal information reasonably described by the individual that can be reasonably located by the insurer, the insurer, within 30 business days of receipt of the request, must:

- inform the individual of the nature and substance of the information in writing or by telephone or oral communication, at its election;
- permit the individual to see and copy, in person, the information or to obtain a copy of the information by mail, at the individual's election, unless the information is encoded, in which case the insurer must provide an accurate translation in plain language;
- disclose to the individual the identity of any person to whom the insurer has disclosed the information within the two years preceding the request, if recorded, and if not recorded, the names of those institutions or persons to whom the information is normally disclosed; and
- provide the individual with a summary of procedures by which the individual may request correction, amendment, or deletion of the information (Ariz. Rev. Stat. § 20-2108(A)).

If medical record information that was originally supplied to the insurer by a medical care institution or a medical provider is requested, the insurer may provide access to the information directly to the individual requesting it or to a medical provider designated by the individual, at the

insurer's election. If disclosure is made to a medical professional, the insurer must notify the individual at the time of disclosure that it has done so (Ariz. Rev. Stat. § 20-2108(C)).

Insurers providing access to personal information as outlined above may charge a reasonable fee for costs incurred in providing copies (Ariz. Rev. Stat. § 20-2108(D)). The access obligations described above may be met by another insurance institution, producer, or support organization acting on the insurer's behalf (Ariz. Rev. Stat. § 20-2108(E)).

Correction, amendment, or deletion: Within 30 business days of receipt of a written request to correct, amend, or delete recorded personal information in its possession, an insurance institution, producer, or support organization must either correct, amend, or delete the information or notify the individual of its refusal to correct, amend, or delete, the reasons for its refusal, and the individual's right to file a statement (see below) (Ariz. Rev. Stat. § 20-2109(A)).

If an insurer corrects, amends, or deletes personal information, it must notify the requesting individual and must provide the corrected information to any person specified by the individual who may have received the recorded information in the previous two years, to any insurance support organization if it has systematically received recorded personal information from the insurer in the past seven years (unless the support organization no longer maintains personal information about the individual), and to any insurance support organization that furnished the subject personal information (Ariz. Rev. Stat. § 20-2109(B)).

Any individual disagreeing with an insurer's refusal to correct, amend, or delete disputed health information may file a statement setting forth what the individual thinks is the correct information and the reasons why the individual disagrees with the refusal. The insurer must file the statement with the individual's disputed information, provide the statement in any subsequent disclosure of the disputed personal information, and furnish the statement in the same manner as required when the insurer provides corrected information as outlined above (Ariz. Rev. Stat. § 20-2109(C) -(D)). In addition, on request of the individual, the insurance institution must reconsider its underwriting decision based on corrected information or an individual's statement with respect to a refusal to correct, amend, or delete (Ariz. Rev. Stat. § 20-2109(E)).

Remedies: The Director of Insurance is authorized to impose a cease-and-desist order and civil penalties for violations of the above provisions (see Section II.C.). In addition, a private right of action is available (see Section I.G.1.).

Specific requirements related to HIV information: No person may require the performance of an HIV-related test without first obtaining the written consent of the subject or an authorized person. In addition, no person who obtains confidential HIV-related information in the process of processing insurance information or insurance applications may disclose the information except to the protected person or a representative, a person to whom disclosure is authorized in writing, a government agency specifically authorized to receive the information, a person to whom disclosure is ordered by a court or administrative body, or the Industrial Commission under specified circumstances (Ariz. Rev. Stat. § 20-448.01(A) to Ariz. Rev. Stat. § 20-448.01(C)). Disclosure is permitted to underwriting departments and personnel involved in underwriting decisions, as well as claims personnel reviewing claims, if the disclosure is reasonably necessary for execution of the underwriting decision or claim (Ariz. Rev. Stat. § 20-448.01(D)).

An authorized release must be signed by the protected person or a representative, must be dated, and must describe to whom disclosure is authorized, the purpose of disclosure, and the time period for which it is valid. A general authorization for the release of medical or other information is not adequate to serve as a release for HIV information unless the general release specifies as much in writing and complies with the preceding requirements (Ariz. Rev. Stat. § 20-448.01(E)).

A person to whom confidential HIV information is released (other than the protected person or the protected person's representative) may not further disclose it except as authorized by the law (Ariz. Rev. Stat. § 20-448.01(F)). A disclosure made pursuant to a written release must be accompanied by a statement warning that further disclosure is prohibited without the specific written consent of the subject or as otherwise permitted by law. The person making such a disclosure must keep a record of all disclosures and must provide access to the record to the protected person or a representative (Ariz. Rev. Stat. § 20-448.01(G) to Ariz. Rev. Stat. § 20-448.01(H)). Finally, no person may be compelled by a subpoena, court order, or search warrant to disclose confidential HIV information unless specified conditions are met (Ariz. Rev. Stat. § 20-448.01(I)).

A protected person whose rights have been violated has the same remedies available to persons whose rights have been violated under provisions of the Insurance Information and Privacy Protection Act (see above and Section I.G.1.).

Specific requirements related to genetic testing information: Under a specific provision of the insurance law, a person may not order or require the performance of a genetic test without first receiving the written consent of the subject or the subject's representative. In addition, the results of a genetic test are confidential and may not be released to any party without the express consent of the subject or representative (Ariz. Rev. Stat. § 20-448.02).

Breach notification law: Businesses in the insurance sector who maintain unencrypted computerized data that includes "personal information" as defined in the Arizona data breach notification law are subject to the law's notification requirements if they become aware of an incident of unauthorized acquisition and access to such data (see Section I.C.8.).

SSN requirements: Requirements regarding the use and disclosure of social security numbers would apply to businesses in the insurance sector to the extent that they collect or use such information (see Section I.D.10.).

8. Retail & Consumer Products

Permissible use of driver's license and state ID information: A retailer may retain and use information from a customer's driver's license or other state-issued ID only for the purpose of (a) verifying the customer's age, (b) establishing the customer's identity, (c) confirming that the customer is properly licensed to operate a motor vehicle, recreational vehicle, truck, or motorcycle on a public road, or (d) disclosing the information to the Department of Transportation, a person licensed under insurance law, a notary public, or a business for specified purposes such as check verification, creditworthiness, fraud detection, or account collection, among others (Ariz. Rev. Stat. § 44-7701(A)). The retailer may not transmit this information to a third party for any purpose other than those specified above or for purposes of a law enforcement investigation (Ariz. Rev. Stat. § 44-7701(B)). The law does not prohibit the use of this information in a court or administrative proceeding (Ariz. Rev. Stat. § 44-7701(C)). Enforcement actions and civil penalties are available for a violation (see Section II.C.).

Breach notification law: Businesses in the retail and consumer products sector who maintain unencrypted computerized data that includes "personal information" as defined in the Arizona data breach notification law are subject to the law's notification requirements if they become aware of an incident of unauthorized acquisition and access to such data (see Section I.C.8.).

SSN requirements: Requirements regarding the use and disclosure of social security numbers would apply to businesses in the retail and consumer products sector to the extent that they collect or use such information (see Section I.D.10.).

Anti-spam and do-not-call provisions: See Section I.E.1

9. Social Media

Breach notification law: Businesses in the social media sector who maintain unencrypted computerized data that includes "personal information" as defined in the Arizona data breach notification law are subject to the law's notification requirements if they become aware of an incident of unauthorized acquisition and access to such data (see Section I.C.8.).

SSN requirements: Requirements regarding the use and disclosure of social security numbers would apply to businesses in the social media sector to the extent that they collect or use such information (see Section I.D.10.).

10. Tech & Telecom

Breach notification law: Businesses in the tech and telecommunications sector who maintain unencrypted computerized data that includes "personal information" as defined in the Arizona data breach notification law are subject to the law's notification requirements if they become aware of an incident of unauthorized acquisition and access to such data (see Section I.C.8.).

SSN requirements: Requirements regarding the use and disclosure of social security numbers would apply to businesses in the tech and telecommunications sector to the extent that they collect or use such information (see Section I.D.10.).

Divulging communication service information: A person who intentionally and without lawful authority obtains knowledge of the contents of a wire or electronic communication in connivance with a communications service provider, or a communications service provider who intentionally divulges the contents of a wire or electronic communication entrusted to the provider for transmission or delivery to any person other than the person for whom it was intended without permission of the intended recipient or pursuant to a statutory exception, is guilty of a class 6 felony (Ariz. Rev. Stat. § 13-3006; for more information on Arizona's eavesdropping law, see Section I.F.).

11. Other Sectors

There are no Arizona provisions regarding privacy and data security related to other business sectors.

F. ELECTRONIC SURVEILLANCE

Eavesdropping law: A person is guilty of a class 5 felony if he intentionally intercepts a wire or electronic communication to which the person is not a party, or aids or authorizes another person to do so, without the consent of either a sender or receiver of a communication (Ariz. Rev. Stat. § 13-3005(A)(1)). In addition, a person who intentionally and without lawful authority obtains knowledge of the contents of a wire or electronic communication in connivance with a communications service provider, or a communications service provider who intentionally divulges the contents of a wire or electronic communication entrusted to the provider for transmission or delivery to any person other than the person for whom it was intended without permission of the intended recipient or pursuant to a statutory exception, is guilty of a class 6 felony (Ariz. Rev. Stat. § 13-3006). It is a defense to a criminal action brought under the law that a person relied in good faith on a subpoena or ex parte order in disclosing the information or divulged the information pursuant to specified statutory requirements (Ariz. Rev. Stat. § 13-3013).

An exception is provided where the interception is effected with the consent of a party to the communication or a person present during the communication (thus making Arizona a "one-party consent" state). Additional exceptions are provided for interceptions made pursuant to a subpoena or ex parte order granted under the statute, as well as for specified activities by communications

service providers, interceptions of certain radio communications, transmissions causing harmful interference, and the divulging of contents of wire or electronic communications inadvertently obtained that appear to pertain to a crime, among others (Ariz. Rev. Stat. § 13-3012).

A separate provision of the eavesdropping law makes it unlawful for a person to knowingly photograph, videotape, film, digitally record, or otherwise secretly view another person without their consent in a restroom, bathroom, locker room, bedroom, or other location where the person has a reasonable expectation of privacy and the person is engaged in specified activities (Ariz. Rev. Stat. § 13-3019(A)). It is also unlawful for a person to disclose, display, distribute, or publish a photograph, video tape, film, or digital recording obtained as outlined above (Ariz. Rev. Stat. § 13-3019(B)). A violation of either of these requirements is a class 5 felony, except that a violation of the provisions without the use of a device is a class 6 felony for a first offense (Ariz. Rev. Stat. § 13-3019(C) -(D)). The offense is augmented to a class 4 felony if the person depicted is recognizable (Ariz. Rev. Stat. § 13-3019(E)).

A civil cause of action is available for violations of the eavesdropping law (see Section I.G.4).

Video recordings of minors: Under the Parents' Bill of Rights, parents have the right to consent in writing before the state or any of its political subdivisions makes a video or voice recording of a minor child, unless an exception applies (see Section I.D.12.).

G. PRIVATE CAUSES OF ACTION

1. Consumer Protection

Failure to comply with security freeze requirements: Any consumer reporting agency that is grossly negligent or that acts willfully and maliciously with intent to harm a consumer is liable to a consumer for actual damages, if any, attorney fees, and court costs if it fails to implement a security freeze, releases a credit report or credit score if a security freeze is in place, or fails to remove a security freeze at the customer's request (Ariz. Rev. Stat. § 44-1695(D); see Section I.D.4.).

[NOTE: Another statutory provision (Ariz. Rev. Stat. § 44-1698(P)) provides that an act in violation of the security freeze provisions is an unlawful practice under the state's consumer fraud law and is subject to enforcement through a private action. Presumably, the provisions of Ariz. Rev. Stat. § 44-1695(D) above are designed to establish the damages available. A corollary provision governing the placement of security freezes on the credit reports or records of protected persons (also discussed at Section I.D.4.) contains an identical provision specifying that an act in violation of law is an unlawful practice subject to a private action (Ariz. Rev. Stat. § 44-1698.02(K)). However, Ariz. Rev. Stat. § 44-1695(D) does not reference the law governing security freezes placed on behalf of protected persons, so the private enforcement mechanism for that provision is unclear.]

Disclosure of inaccurate credit report information after correction request: An agency that refuses to correct a consumer credit report in response to a consumer's allegation of inaccuracy (see Section I.D.4.) is liable for any damages incurred by the consumer as a result of the reporting of the inaccurate information (Ariz. Rev. Stat. § 44-1695(B)).

IIPPA: A person whose rights are violated as the result of a violation of provisions of the Insurance Information and Privacy Protection Act (IIPPA) governing access to personal information (see Section I.E.7.) may apply to a superior court for appropriate equitable relief (Ariz. Rev. Stat. § 20-2118(A)). An insurance institution, producer, or support organization responsible for a violation of the IIPPA related to improper disclosure of personal information is liable for damages caused to the individual, but no monetary award in excess of actual damages may be awarded (Ariz. Rev. Stat. § 20-2118(B)). In either type of action, the court may award costs and attorney fees to the prevailing party (Ariz. Rev. Stat. § 20-2118(C)). An action must be brought within two years from the date the

alleged violation was or should have been discovered (Ariz. Rev. Stat. § 20-2118(D)). No claim for defamation, invasion of privacy, or "negligency" [sic] may be brought under the IIPPA unless a disclosure or furnishing of false information was done with malice or willful intent to injure (Ariz. Rev. Stat. § 20-2119).

The same remedies outlined above are available to protected persons whose rights have been violated pursuant to specific provisions governing the disclosure of confidential HIV information by insurers (Ariz. Rev. Stat. § 20-448.01(L); for a discussion of the specific prohibitions, see Section I.E.7.).

Webpage or e-mail solicitations for fraud or theft: A person who is in the business of providing Internet access service to the public or who owns a webpage or trademark and is adversely affected by a violation of provisions prohibiting the use of a webpage or e-mail communications for purposes of theft or fraud (see Section I.D.7.) may bring an action to enjoin further violations and to recover the greater of actual damages or $2,500 for each violation (Ariz. Rev. Stat. § 18-543(A)). Any person other than the persons described above who are adversely affected by a violation (essentially, persons who reveal identifying information due to another person's impermissible webpage or e-mail solicitation) may bring an action to enjoin further violations and to recover the greater of actual damages or $5,000 for each violation (Ariz. Rev. Stat. § 18-543(B)). Multiple violations resulting from any single action or act constitute one violation (Ariz. Rev. Stat. § 18-543(G)). Treble damages are available if the court determines that a person has engaged in a pattern or practice of violation (Ariz. Rev. Stat. § 18-543(E)). Any action must be brought within three years of the date the violation was, or through the exercise of diligence reasonably should have been, discovered (Ariz. Rev. Stat. § 18-543(D)).

Anti-spam law: A person whose property or person is injured because of a violation of the state's anti-spam law is entitled to recover any damages sustained, including loss of profits, and costs incurred from a suit (Ariz. Rev. Stat. § 44-1372.02(A)). If an injury results from the intentional transmission of unsolicited commercial e-mail, the injured person may recover attorney fees and costs and may choose, in lieu of actual damages, to recover the lesser of $10 for each unsolicited commercial e-mail impermissibly transmitted or $25,000 (Ariz. Rev. Stat. § 44-1372.02(B)). If such an injury is sustained by an e-mail service provider, that provider may recover attorney fees and costs and, in lieu of actual damages, the greater of $10 per e-mail in violation or $25,000 (Ariz. Rev. Stat. § 44-1372.02(D)). There is no cause of action available against an e-mail service provider for transmitting unsolicited commercial e-mail over the computer network (Ariz. Rev. Stat. § 44-1372.02(C)).

Telephone solicitations: Under the state's telephone solicitations law (see Section I.E.1), a consumer may rescind a sale by an unregistered seller at any time and may recover any purchase money paid, financial damages caused by the unregistered seller, and reasonable attorney fees and costs (Ariz. Rev. Stat. § 44-1279).

Soldier's right of publicity: A person who uses the name, portrait, or picture of a soldier in violation of the soldier's right of publicity (see Section I.E.1) is subject to injunctive relief to prevent the unauthorized use, treble damages, punitive or exemplary damages, and attorney fees and costs (Ariz. Rev. Stat. § 12-761(C)). Any profits from an unauthorized use must be taken into account in calculating damages (Ariz. Rev. Stat. § 12-761(D)). A claim must be brought within five years after the unauthorized publication (Ariz. Rev. Stat. § 12-761(F)).

2. Identity Theft

In general: Taking the identity of another person or entity is a class 4 felony (Ariz. Rev. Stat. § 13-2008(E)). For purposes of this provision, a person takes the identity of another person or entity if the person knowingly takes, purchases, manufactures, records, possesses, or uses any personal

identifying or entity identifying information of another person or entity, without consent, with the intent to obtain or use that identity for an unlawful purpose or to cause loss to the person or entity whose identity was stolen without regard to whether they actually suffer economic loss, or with the intent to obtain or continue employment (Ariz. Rev. Stat. § 13-2008(A)). Prosecutors may combine multiple violations in a complaint under circumstances outlined in the law (Ariz. Rev. Stat. § 13-2008(C)).

Aggravated identity theft and knowingly accepting identity: A person commits aggravated identity theft when he knowingly takes personal or entity identifying information as described above of three or more persons, when the theft causes another person or entity to suffer a loss of $1,000 or more, or when the theft is committed with the intent to obtain employment (Ariz. Rev. Stat. § 13-2009(A)). In addition, an offense is committed by an employer who knowingly accepts the identity of another person, knowing the individual is not the actual person identified by the information and using the information for purposes of determining whether the person has legal authorization to work in the U.S. under federal laws prohibiting unlawful aliens from working in the U.S. (Ariz. Rev. Stat. § 13-2009(B)). Each of these violations is a class 3 felony (Ariz. Rev. Stat. § 13-2009(E)).

Trafficking: A separate offense is provided for trafficking in the identity of another person or entity. A person commits such an offense if the person knowingly sells, transfers, or transmits any personal or entity identifying information without the consent of the victim for any unlawful purpose or to cause loss to the person or entity whether or not the person actually suffers any economic loss, or to allow another person to obtain or continue employment (Ariz. Rev. Stat. § 13-2010(A)). Trafficking is a class 2 felony (Ariz. Rev. Stat. § 13-2010(C)).

Exceptions for minors: An exception applies in each classification of identity theft for persons under the age of 21 who use forged identification to purchase alcohol or to access age-restricted venues (Ariz. Rev. Stat. § 13-2008(D); Ariz. Rev. Stat. § 13-2009(D); Ariz. Rev. Stat. § 13-2010(B)).

Consumer reporting agencies: For information on requirements applicable to consumer reporting agencies regarding prevention of identity theft, see Section I.D.4.

3. Invasion of Privacy

In general, invasion of privacy claims in Arizona are governed by common law doctrine. The Arizona Court of Appeals has held that invasion of privacy claims are governed by the two-year limitations period prescribed by Ariz. Rev. Stat. § 15-542 (*Hansen v. Stoll*, 130 Ariz. 454 (App. Div. 1 1981).

4. Other Causes of Action

Access to and disclosure of patient medical and payment records: The law governing the requirements applicable to health care providers with respect to access to, and disclosure of, patient records (see Section I.D.9.) does not specify procedures for a private cause of action, but does provide that a health care provider who acts in good faith is not liable for damages in a civil action for the disclosure of records. Accordingly, there would appear to be an implied right to a private cause of action for a violation of the requirements. A health care provider is presumed to have acted in good faith, but the presumption may be rebutted by clear and convincing evidence (Ariz. Rev. Stat. § 12-2296).

Unlawful disclosure of communicable disease-related information: A protected person may bring an action in Superior Court for legal and equitable relief on his own behalf against a person who violates provisions prohibiting the disclosure of communicable disease-related information (Ariz. Rev. Stat. § 36-668; see Section I.D.9.).

Unlawful disclosure of genetic testing results: Health care providers and their agents and employees who disclose information related to the genetic testing of an individual (see Section I.D.9.) may be subject to civil liability for a violation. Such a person is presumed to have acted in good faith, but the presumption may be rebutted by a preponderance of the evidence (Ariz. Rev. Stat. § 12-2802(G)).

Unlawful disclosure of mental health service records: A health care entity that discloses medical or payment record information in contravention of restrictions on such disclosures in the mental health services law (see Section I.D.9.) and that does so acting in good faith is not liable for damages in a civil action brought for a violation. The entity is presumed to have acted in good faith, but the presumption may be overcome by clear and convincing evidence (Ariz. Rev. Stat. § 36-509(E)).

Improper employment references: A private cause of action is available for violation of the provisions governing employment references (see Section I.E.6). Employers sending reference information pursuant to these provisions are immune from liability if they act in good faith. A presumption of good faith exists if the employer has fewer than 100 employees and only provides the information in the manner described by the law, or if the employer employs 100 or more employees and has a regular practice of providing reference information about the reason for termination of a former employee or about the job performance, professional conduct, or evaluation of a current or former employee (Ariz. Rev. Stat. § 23-1361(C)). The presumption is rebuttable by a showing that the employer disclosed the information with actual malice or intent to mislead (Ariz. Rev. Stat. § 23-1361(D)). Courts may award court costs, attorney fees, and other related expenses to a prevailing party (Ariz. Rev. Stat. § 23-1361(I)).

Eavesdropping law: Any person whose oral, wire, or electronic communication is intentionally intercepted or disclosed in violation of the state's eavesdropping law (see Section Section I.F.) may bring a civil action against the person committing the violation. The victim may receive preliminary and other equitable or declaratory relief as appropriate, as well as damages equal to the greater of the sum of actual damages and any profits made by the violator, statutory damages of $100 per day for each violation, or statutory damages of $10,000 (Ariz. Rev. Stat. § 12-731(A)(1) to Ariz. Rev. Stat. § 12-731(A)(2)). The victim may also recover punitive damages in appropriate cases and reasonable attorney fees and other costs (Ariz. Rev. Stat. § 12-731(A)(3) -(4)). An action must be brought within one year after the date that the victim had a reasonable opportunity to discover the violation (Ariz. Rev. Stat. § 12-731(B)). It is a defense to a civil action brought under the eavesdropping law that a person relied in good faith on a subpoena or ex parte order in disclosing the information or divulged the information pursuant to specified statutory requirements (Ariz. Rev. Stat. § 13-3013).

H. CRIMINAL LIABILITY

A violation of provisions prohibiting the use of a webpage or e-mail communications for purposes of fraud or theft (see Section I.D.7.) is a class 5 felony (Ariz. Rev. Stat. § 18-544).

Any person who knowingly discloses any record or other information, including e-books, that identifies a user of library services as requesting or obtaining specific materials or services in violation of provisions applicable to publicly-supported libraries (see Section I.C.3) is guilty of a class 3 misdemeanor (Ariz. Rev. Stat. § 41-151.22(C)).

Information collected on individuals by the state chronic disease surveillance system (see Section I.D.9.) that can identify the individual is confidential and may only be used for specified purposes. Any person who discloses confidential information in violation of this provision is guilty of a class 3 misdemeanor (Ariz. Rev. Stat. § 36-133(F)).

A person who discloses, compels another to disclose, or procures the disclosure of communicable disease-related information in violation of statutory requirements (see Section I.D.9.) is guilty of a class 3 misdemeanor (Ariz. Rev. Stat. § 36-666(A)(2)). Immunity is available if the person, health facility, or health care provider acted in good faith. Good faith is presumed unless overcome by clear and convincing evidence (Ariz. Rev. Stat. § 36-666(B) -(D)).

Anti-spam law: A violation of the state's anti-spam law (see Section I.E.1) is a class 2 misdemeanor (Ariz. Rev. Stat. § 44-1372.05).

Telephone solicitation by unregistered seller: Unregistered sellers engaging in telephone solicitation are guilty of a class 5 felony (Ariz. Rev. Stat. § 44-1277).

Use of image of deceased soldier: The use of the name, portrait, or picture of a deceased soldier without the prior consent of the soldier or a representative in violation of the soldier's right of publicity (see Section I.E.1) is a class 1 misdemeanor (Ariz. Rev. Stat. § 13-3726).

Eavesdropping: See Section I.F.

Identity theft: See Section I.G.2.

II. REGULATORY AUTHORITIES AND ENFORCEMENT

A. ATTORNEY GENERAL

The Arizona Attorney General has enforcement authority over most Arizona privacy laws, including the data breach notification law (see Section I.C.8.), provisions related to the use and disclosure of social security numbers (see Section I.D.10.), security freeze requirements (see Section I.D.4.), and anti-spam and do-not-call provisions (see Section I.E.1).

B. OTHER REGULATORS

The Arizona Department of Health Services is responsible for administering penalties regarding the unlawful disclosure of communicable disease-related information (see Section I.D.9.).

The Arizona Department of Insurance has enforcement authority over the provisions of the Insurance Information and Privacy Protection Act (IIPPA) governing access to and disclosure of personal information (see Section I.E.7.).

C. SANCTIONS & FINES

Breach notification: The Attorney General has the sole enforcement authority over violation of the state's data breach notification law (see Section I.C.8.). The Attorney General may bring an action to obtain actual damages for a willful and knowing violation and a civil penalty not to exceed $10,000 per breach of the security of the system or series of breaches of a similar nature discovered in a single investigation (Ariz. Rev. Stat. § 18-545(H)).

Improper recording of SSNs on websites: The Attorney General, a county attorney, or both may commence an action for a violation of restrictions on the recording of social security numbers or financial account information on a public website (see Section I.D.8. and Section I.D.10.) (Ariz. Rev. Stat. § 44-1373(H)). A person or entity in violation is subject to a civil penalty of up to $500 for each act of impermissible recording, but such a penalty is not applicable to a person or entity who transmits the document for recording but has no authority for the creation of the document (Ariz.

Rev. Stat. § 44-1373(I)). In addition, a county agency is not subject to civil liability (Ariz. Rev. Stat. § 44-1373(J)).

IIPPA: An insurer that violates the provisions of the Insurance Information and Privacy Protection Act (IIPPA) governing access to and disclosure of personal information (see Section I.E.7.) is subject to imposition of a cease-and-desist order by the Director of Insurance after a hearing (Ariz. Rev. Stat. § 20-2116). In addition, the Director may impose a civil penalty of not more than $500 for each violation, not to exceed $10,000 in the aggregate, for violations of the IIPPA (Ariz. Rev. Stat. § 20-2117(A)). A person violating a cease-and-desist order is subject to a civil penalty of not more than $10,000 for each violation or not more than $50,000 per violation if the Director finds that violations constitute a general business practice, as well as suspension or revocation of the insurer's license (Ariz. Rev. Stat. § 20-2117(B)).

Illegal use of webpage or e-mail for fraud or theft: With respect to provisions prohibiting the use of a webpage or e-mail communications for purposes of fraud or theft (see Section I.D.7.), the Attorney General may bring an action to enjoin further violations and to recover the greater of actual damages or $2,500 for each violation (Ariz. Rev. Stat. § 18-543(A)). Multiple violations resulting from any single action or act constitute one violation (Ariz. Rev. Stat. § 18-543(G)). Treble damages are available if the court determines that a person has engaged in a pattern or practice of violation (Ariz. Rev. Stat. § 18-543(E)). Any action must be brought within three years of the date the violation was, or through the exercise of diligence reasonably should have been, discovered (Ariz. Rev. Stat. § 18-543(D)). The Attorney General may also recover reasonable attorney fees and costs (Ariz. Rev. Stat. § 18-543(F)).

Parental consent to collection of pupil personal information: Parents having a reasonable belief that a school district or charter school has violated provisions requiring parental consent prior to the collection of personal information about a pupil for survey purposes (see Section I.E.2.) may file a complaint with the Attorney General or a county attorney for the county in which the alleged violation occurred, who then may initiate a suit to compel compliance and for civil penalties. On receiving written notice of a failure to comply, a district or charter school may avoid the cause of action or a penalty if it destroys any information gathered in violation of the requirements and provides written instruction to the individual conducting the survey, which must be kept on file for one year (Ariz. Rev. Stat. § 15-117(K)).

For each violation as described above, the court may impose a civil penalty not to exceed $500 (Ariz. Rev. Stat. § 15-117(L)). The penalty is payable to the Attorney General's office or county treasurer, as appropriate, for the use and reimbursement of costs of prosecution (Ariz. Rev. Stat. § 15-117(M)).

Violations of FERPA requirements: With respect to requirements under the federal Family Educational Rights and Privacy Act (FERPA) adopted by Arizona regarding parents' rights regarding the release of, or access to, student records (see Section I.E.2.), in addition to any federal remedies available under FERPA, a superior court may grant injunctive or special action relief if an educational agency or institution or an employee or agent thereof fails to comply with FERPA requirements, without regard to whether the agency or institution actually is receiving federal funding (Ariz. Rev. Stat. § 15-141(B)).

Data disposal requirements: Entities that violate requirements regarding the disposal or destruction of paper records or documents containing personal information (see Section I.C.7.) are subject to enforcement action by either the county attorney for the county in which the records or documents were wrongfully discarded or disposed, or by the Attorney General. Procedures are specified for instances in which a violation concerning the same entity occurs in multiple counties (Ariz. Rev. Stat. § 44-7601(B)). For each violation arising out of one incident, a civil penalty will be

imposed that may not exceed $500 for a first violation, $1,000 for a second violation, or $5,000 for a third or subsequent violation (Ariz. Rev. Stat. § 44-7601(C)).

Use of driver's license information by retailers: Retailers who violate specified restrictions on the use of driver's license or state ID information (see Section I.E.8.) are subject to an enforcement action by the county attorney for the county in which the violation occurred. The law specifies the procedure for cases in which a violation by the same retailer occurs in multiple counties (Ariz. Rev. Stat. § 44-7701(D)(1)). In addition, an enforcement action may be brought by the Attorney General. While a violation of the restriction of driver's license information is deemed to constitute an unlawful practice under the state's consumer fraud law, the civil penalties applicable to a violation (see below) are in lieu of any penalties prescribed by the consumer fraud law (Ariz. Rev. Stat. § 44-7701(D)(1)).

For each violation, a civil penalty will be imposed that may not exceed $500 for a first violation, $1,000 for a second violation, or $5,000 for a third or subsequent violation (Ariz. Rev. Stat. § 44-7701(E)).

Unlawful printing of credit card account number or expiration date: The Attorney General may investigate violations of the law prohibiting the printing of more than the last five digits of a credit card number or the card's expiration date on customer receipts (see Section I.D.3.). A violation is an unlawful act or practice under the state's consumer protection law, and the Attorney General may take appropriate action under that law, including bringing an action to impose a civil penalty of not more than $10,000 for a willful violation (Ariz. Rev. Stat. § 44-1367; see also Ariz. Rev. Stat. § 44-1531).

Security freeze provisions: A violation of provisions governing restrictions on the disclosure of credit report information of consumers and protected persons subject to a security freeze (see Section I.D.4.) is subject to enforcement by the Attorney General. In the case of a security freeze concerning a consumer that is not a protected person, the Attorney General may seek injunctive relief to prevent future violations (Ariz. Rev. Stat. § 44-1698(P)). In the case of a security freeze concerning a protected person, the Attorney General may investigate and take appropriate action as prescribed by the state's consumer fraud law (Ariz. Rev. Stat. § 44-1698.02(K)).

Unlawful disclosure of communicable disease-related information: The Department of Health Services may impose a civil penalty of not more than $5,000 for a violation of provisions prohibiting the disclosure of communicable disease-related information (Ariz. Rev. Stat. § 36-667(A)(2); see Section I.D.9.).

Anti-spam law: A violation of the state's anti-spam law (see Section I.E.1) is considered to be an unlawful practice under the consumer protection law, and the Attorney General may investigate and take any appropriate action prescribed under that law (Ariz. Rev. Stat. § 1372.01(D)).

Do-not-call violations: A violation of the state's do-not-call requirements (see Section I.E.1) is an unlawful practice under the consumer fraud law. The Attorney General may investigate and take appropriate action under that law, but a civil penalty imposed for a violation may not exceed $1,000 per violation (Ariz. Rev. Stat. § 44-1282(B)).

D. REPRESENTATIVE ENFORCEMENT ACTIONS

The Arizona Attorney General has written an opinion specifying that text messages and social media activity of public officials constitute public records to the extent that the information is related to their official roles (Opinion No. I17-004 (R15-026), July 7, 2017).

E. STATE RESOURCES

The Attorney General provides information for consumers and businesses regarding credit reporting and credit repair, telemarketing scams, identity theft, and security freezes, among other items. Although the Attorney General does not endorse any particular set of guidelines regarding data security, consumers can find resources for maintaining their privacy and preventing or limiting instances of identity theft on the Attorney General's website , the FTC's website , and at https://www.identitytheft.gov/.

The Attorney General's Civil Rights Division has issued a Guide to Pre-Employment Inquiries that outlines information on specific inquiries in the context of the state's Civil Rights Act.

III. RISK ENVIRONMENT

Arizona State Attorney General, Mark Brnovich has identified data privacy and security for businesses and consumers as a priority of his administration. Although companies are often the victims of cybersecurity incidents, Arizona law requires that they take steps to prevent and limit such incidents and keep consumers informed as to:

- the nature and scope of data that is being collected and maintained;
- the ways in which the data is to be used or shared; the parties, if any, with whom the data may be shared; and
- any incidents in which the data may have been compromised.

In the event that such information is concealed or misrepresented from consumers, the Attorney General may investigate or commence other proceedings under Arizona's data breach notification law (Ariz. Rev. Stat. § 18-545(H)) or the Arizona Consumer Fraud Act (Ariz. Rev. Stat. § 44-1524).

Non-criminal data privacy and security laws are enforced by the Consumer Protection and Advocacy Section of the Civil Litigation Division, including the laws requiring notification of data breaches under Ariz. Rev. Stat. § 18-545. The Consumer Protection division has a staff of 30 employees, eight of whom are attorneys. The Consumer Protection Division also has a unit devoted to addressing consumer complaints, which can be filed online.

In addition to individual consumer protection, the Attorney General has participated in several high-profile enforcement actions regarding data breaches, including those involving Target Corporation, PHH Mortgage Corporation, and Nationwide Insurance. The Attorney General has also participated in the consumer fraud action against Lenovo Corporation regarding vulnerable computer software. The Attorney General has also joined a multi-state investigation of the Equifax data breach.

As part of the 2018 Arizona legislative session, the Attorney General has also sponsored HB 2154, which proposes to amend and update Arizona's data breach statute in several ways. This bill expands the definition of personal information to include biometric data, electronic signatures, e-mail addresses and passwords, medical information, and tax information. In the event of a data breach compromising this information, consumers will be notified and better able to take speedy action to minimize potential harm. The bill also promotes Attorney General enforcement by requiring any breaches be reported to the Attorney General and the major credit reporting agencies. A breach of this notification requirement is a breach of Arizona's Consumer Fraud Act.

IV. EMERGING ISSUES AND OUTLOOK

A. Recent Legislation

1. Student Data

2017 Arizona Session Laws, Chapter 180, added a new provision to Title 15 (Education) that prohibits operators of web sites and mobile apps primarily used and designed for school purposes from selling or renting a student's information or from knowingly disclosing a student's information under certain circumstances. It also requires operators to implement and maintain reasonable security procedures and practices. The law came into effect on Aug. 9, 2017. See Ariz. Rev. Stat. § 15-1046.

B. Proposed Legislation

1. Data Breach Notification

HB 2154, introduced Jan. 17, 2018, proposes to expand the definition of personal information and imposes more detailed notification requirements in the event of a data breach, such as the requirement to notify the Attorney General and the individuals affected within 45 days. The bill passed the House on Mar. 7, 2017, and was sent to the Senate.

2. Workplace Privacy

SB 1417, introduced Jan. 29, 2018, would prohibit an employer from discharging or refusing to hire, promote, or retain an individual because of that individual's consumer report or credit history.

SB 1242, introduced Jan. 18, 2018, would prohibit employers from seeking salary history information, whether orally or in writing or whether personally or through an agent, about an applicant for employment.

HB 2312, introduced in January 2017, would prohibit employers from inquiring about, considering, or requiring disclosure of the criminal conviction record of an employment applicant unless the inquiry takes place after a conditional offer and is only for the period of five years prior to the date of the offer, and unless the conviction record has a direct relationship to the employment position. The bill was referred to the House Commerce and House Rules Committees.

3. Student Biometric Data

SB 1373, also introduced in January 2017, would prohibit schools or school service providers from collecting or possessing student biometric information without first developing a written policy for the collection, retention, disclosure, and destruction of biometric information and then obtaining a written release for the collection of such information. The bill was held in committee and was not enacted.

C. Other Issues

1. Equifax Breach

In September 2017, Arizona Attorney General Mark Brnovich joined 31 other attorneys general in an investigation into the Equifax data breach. In a letter sent to Equifax Sept. 15, the attorneys general called for Equifax to disable links for enrollment in fee-based credit monitoring service in the wake of the massive data breach.

