Bloomberg Law
Privacy & Data Security

Domestic Privacy Profile: TENNESSEE

Robert L. Brewer, Anthony J. McFarland, T. Stephen C. Taylor, and Elizabeth S. Warren, of Bass, Berry & Sims PLC, Nashville, provided expert review of the Tennessee Profile and wrote the Risk Environment section. [Last updated June 2018. – Ed.]

TABLE OF CONTENTS

I. APPLICABLE LAWS AND REGULATIONS

A. CONSTITUTIONAL PROVISIONS

Tenn. Const. art. I, § 8 provides that all people have the inalienable rights to life, liberty, and property, and Tenn. Const. art. I, § 7 provides that all people shall be secure in their persons, houses, papers, and possessions from unreasonable searches and seizures. Aside from these general provisions, our research has uncovered no data-specific privacy provisions in the Tennessee Constitution.

B. PERSONAL DATA PROTECTION PROVISIONS

1. Who is covered?

Tennessee's Identity Theft Deterrence Act (Tenn. Code Ann. § 47-18-2101 to Tenn. Code Ann. § 47-18-2111) is the state's overarching privacy regime. Under the statute's breach notification provisions, Tenn. Code Ann. § 47-18-2107(b), only residents of the state of Tennessee must be notified by information holders if their personal information was compromised.

Tennessee also requires the protection of "confidential information" of its "citizens" held by state agencies (Tenn. Code Ann. § 10-7-504). State agencies, municipalities, and counties are required to create safeguards and procedures to ensure the security of confidential information on laptop computers and other removable storage devices (Tenn. Code Ann. § 47-18-2901).

Other provisions of Tennessee law provide specific protections for:

- Students (Tenn. Code Ann. § 49-1-701 *et seq.*);
- Employees (Tenn. Code Ann. § 50-1-1003); and
- Medical patients (Tenn. Code Ann. § 63-2-101(b)(2)), including patient communications with heath care providers, such as social workers (Tenn. Code Ann. § 63-23-109), counselors

(Tenn. Code Ann. § 63-22-114), nurses (Tenn. Code Ann. § 63-7-125), psychologists (Tenn. Code Ann. § 63-11-213), and physical therapists (Tenn. Code Ann. § 63-13-317).

2. What is covered?

Tennessee's Identity Theft Deterrence Act defines "personal information" as a person's first name or first initial and last name, in combination with the person's (1) social security number, (2) driver's license number, or (3) "account, credit card, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account" (Tenn. Code Ann. § 47-18-2107(a)(4)(A)). Personal information however does not include "information that is lawfully made available to the general public from federal, state, or local government records or information that has been redacted, or otherwise made unusable" (Tenn. Code Ann. § 47-18-2107(a)(4)(B)).

Tennessee's identity theft laws further protect "personal identifying information," which includes an individual's social security number, driver's license identification number, savings account number, checking account number, applicable PINs or passwords, complete credit or debit card number, demand deposit account number, health insurance identification number, or unique biometric data (Tenn. Code Ann. § 39-14-150(g)(2)).

Tennessee law also provides specific protections for:

- Biometric data, including fingerprints, voice prints, retinal images, and health measurements (Tenn. Code Ann. § 39-14-150(e)(2); Tenn. Code Ann. § 49-1-706);
- Financial records, meaning documents held by a financial institution that identify a customer, not including a customer's name, address, and account number (Tenn. Code Ann. § 45-10-102(4));
- Criminal records (Tenn. Code Ann. § 40-32-101);
- Personal internet accounts (Tenn. Code Ann. § 50-1-1003); and
- Health records (Tenn. Code Ann. § 63-2-101(b)(2); Tenn. Code Ann. § 68-1-1009).

3. Who must comply?

Tennessee requirements apply to:

- Employers (Tenn. Code Ann. § 50-1-1003);
- Insurance companies (Tenn. Code Ann. § 56-7-124; Tenn. Code Ann. § 56-7-2704(a); Tenn. Code Ann. § 56-32-125);
- Entities conducting business in Tennessee (Tenn. Code Ann. § 47-18-2501);
- State boards of education and K-12 schools (Tenn. Code Ann. § 49-1-701 to Tenn. Code Ann. § 49-1-708);
- Health care providers (Tenn. Code Ann. § 63-2-101(a));
- Health care facilities (Tenn. Code Ann. § 68-11-1503; Tenn. Code Ann. § 68-11-901(13)); and
- Video tape sellers and services (Tenn. Code Ann. § 47-18-2204).

Furthermore, the Tennessee Identity Theft Deterrence Act defines an "information holder" as "any person or business that conducts business in this state, or any agency of this state or any of its political subdivisions, that owns or licenses computerized personal information of residents of this state" (Tenn. Code Ann. § 47-18-2107(a)(3)).

C. Data Management Provisions

1. Notice & Consent

Tennessee has no laws of general application addressing notice and consent, but some sector-specific provisions address the topic. (For information on notice requirements under Tennessee's general breach notification provision, see Section I.C.8.)

Identity theft: The possession, use, purchase, or sale of personal identifying information by an information holder may result in a violation of the Identity Theft Victims' Rights Act (Tenn. Code Ann. § 39-14-150) when, among other factors, the holder does not have the consent of the person identified by the information (Tenn. Code Ann. § 39-14-150(b)(1)(B); Tenn. Code Ann. § 39-14-150(c)(1)(C)).

Real estate insurance: In situations where a borrower must furnish evidence of insurance to a lender as a condition for obtaining or keeping a loan, Tenn. Code Ann. § 47-23-101 requires the lender to obtain consent from the borrower before disclosing policy information (such as an expiration date) to another person seeking to renew that policy or sell a new one.

Consumer data: Tenn. Code Ann. § 47-18-2204 prohibits video tape sellers or services from knowingly disclosing to any person personally identifiable information concerning any consumer without informed, written consent from the consumer.

Student data: The Data Accessibility, Transparency and Accountability Act (Tenn. Code Ann. § 49-1-701 to Tenn. Code Ann. § 49-1-708) requires that a state agency or educational institution obtain written consent from the student's parents, or the student if over the age of 18, before collecting individual student biometric data, such as "student data relative to analysis of facial expressions, EEG brain wave patterns, skin conductance, galvanic skin response, heart-rate variability, pulse, blood volume, posture, and eye-tracking" (Tenn. Code Ann. § 49-1-706).

Pursuant to Tenn. Op. Att'y Gen. No. 17-39 (Sept. 13, 2017), school districts that provide student directory information to charter schools (see Tenn. Code Ann. § 49-13-132) must notify parents of any change in school policy that permits such disclosure and must give parents a reasonable opportunity to opt out of the disclosure of student information. Moreover, if a school district has a policy in place that does not allow for the release of information specified in §49-13-132, the opinion requires the district to "promptly amend its policy to permit the release of [such] information . . ."

2. Collection & Use

Our research has revealed no other laws of general application addressing data collection and use in Tennessee.

3. Disclosure to Third Parties

Financial records: Under the Financial Records Privacy Act, a financial institution may not disclose to any person, except to the customer or the customer's agent, any financial records relating to that customer unless the customer has authorized disclosure to that person or the financial records are disclosed in response to a lawful subpoena (Tenn. Code Ann. § 45-10-104(a)). However, the law permits disclosure to a government authority if the financial institution "has information that . . . may be relevant to a possible violation of any statute or regulation" (Tenn. Code Ann. § 45-10-104(b)).

Insurance: The Genetic Information Nondiscrimination in Health Insurance Act prohibits insurance providers from disclosing genetic information about an individual without the individual's or a legal representative's prior written authorization, which must authorize each disclosure and identify each person to whom the disclosure would be made (Tenn. Code Ann. § 56-7-2704(b)). It is unlawful for an insurer who provides accident or health insurance to market or sell information identifying a

patient and relating to the physical or mental health or such patient without consent (Tenn. Code Ann. § 56-7-124(a)).

Medical records: Medical records are not considered public records (Tenn. Code Ann. § 63-2-101(b)(1)), and the name and address and other identifying information of a patient is prohibited from being sold or divulged (Tenn. Code Ann. § 63-2-101(b)(2)). However, the Medical Records Act of 1974, which relates to health care facilities, permits the disclosure of medical records if necessary in the course of providing care and treatment to a patient (Tenn. Code Ann. § 68-11-312(b)).

HMOs: According to the Health Maintenance Organization Act, an HMO may only disclose information "pertaining to the diagnosis, treatment, or health of any enrollee or applicant obtained from the person or from any provider" under certain limited circumstances, including "in the event of a claim or litigation between an enrollee or applicant and the HMO wherein the data or information is pertinent," "upon the express consent of the enrollee or applicant," or "when the data or information is required to be disclosed by the authority of another statute" (Tenn. Code Ann. § 56-32-125(a)).

Motor vehicle records: Tenn. Code Ann. § 55-25-104 provides that the departments of safety and revenue and their employees or officers shall not disclose personal information about any person obtained by the department in connection with a motor vehicle record, unless written consent of the person is obtained pursuant to Tenn. Code Ann. § 55-25-106. Additional exceptions for various purposes are provided by Tenn. Code Ann. § 55-25-107(b) for matters of motor vehicle or driver safety and theft, motor vehicle emissions, motor vehicle recalls, or performance monitoring of motor vehicles and dealers by motor vehicle manufacturers, or for use in connection with matters concerning the federal selective services system. Tenn. Code Ann. § 55-25-105 also allows for disclosure of such information for safety, environmental, and federal compliance purposes.

Identity theft: The sale of personal identifying information by an information holder may result in a violation of the Identity Theft Victims' Rights Act if the holder should have known that the identifying information would be used by someone else to commit any unlawful act, including, but not limited to, obtaining or attempting to obtain credit, goods, services or medical information in the name of the other person (Tenn. Code Ann. § 39-14-150(c)(1)(B)). In addition, Tenn. Code Ann. § 47-18-2110 requires any person or entity that has obtained a federal social security number for a legitimate business or governmental purpose to make reasonable efforts to protect that social security number from disclosure to the public, unless the disclosure is for a legitimate business or governmental purpose and occurs pursuant to the terms of a business or governmental contract or other lawful legal obligation.

Student data: Under the Data Accessibility, Transparency and Accountability Act, operators of websites, online services, online applications, or mobile applications with actual knowledge that the site, service, or application is used primarily for K-12 school purposes are prohibited from selling or renting a student's information or disclosing covered information unless the disclosure is made in furtherance of a K-12 school purpose (Tenn. Code Ann. § 49-1-708(a)). Subsections (a)(4) and (d) contain other exceptions for when the operator may disclose such information.

Disclosure of student information to charter schools: In Opinion No. 17-39, the Tennessee Attorney General addressed certain questions related to the release of student information to charter schools pursuant to Tenn. Code Ann. § 49-13-132. The opinion specifies that a school district may not refuse to provide "a list of student names, ages, addresses, dates of attendance, and grade levels completed" to public charter schools on the basis of the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g). Moreover, if the school district has adopted a policy pursuant to FERPA that would otherwise bar the release directory information, the district *must* "promptly amend its policy" to permit the release of the directory information specified in Tenn. Code Ann. § 49-13-132. The school district must also notify parents of the new policy and allow them a

reasonable opportunity to opt out of the disclosure of student information. The Attorney General also clarified that Tenn. Code Ann. § 49-13-132 does not prohibit chartering authorities and public charter schools from using student contact information received from local education agencies to contact parents and provide them with additional public school options available to their children.

Tax returns: Returns and tax information are open to inspection by or disclosure to officers and employees of the Department of Revenue whose official duties require such inspection or disclosure for tax administration purposes (Tenn. Code Ann. § 67-1-1704(a)). The statute includes other instances where returns and tax information may be disclosed. See subsections (b) through (h).

4. Data Storage

Our research has revealed no laws of general application addressing data storage in Tennessee.

5. Access & Correction

Student data: The Data Accessibility, Transparency and Accountability Act gives parents and guardians the right to inspect and review educational records maintained by the school (Tenn. Code Ann. § 49-1-704(a)), as well as the right to request student data specific to their children's educational records (Tenn. Code Ann. § 49-1-704(b)). "Student data" includes, *inter alia*, state and national assessment results, transcripts, grades and GPA, attendance, demographic data, exit and drop-out information, discipline reports, date of birth, grade level, and expected graduation date (Tenn. Code Ann. § 49-1-702(15)). Unless included in a student's educational record, "student data" does not include juvenile delinquency records, criminal records, medical and health records, student social security number, and student biometric information (Tenn. Code Ann. § 49-1-702(15)(C)).

Medical records: Under Tennessee law, a health care professional must furnish a copy or summary of a patient's medical records within ten working days of a written request by the patient or the patient's authorized representative (Tenn. Code Ann. § 63-2-101(a)). Some health care facilities may have specific records access requirements, such as hospitals, which must "furnish to a patient the patient's hospital records without unreasonable delay upon request in writing," and within 30 days of the request (Tenn. Code Ann. § 68-11-304).

6. Data Security

State & local government: All state agencies and municipalities are required to create safeguards and procedures to ensure that confidential information regarding citizens is securely protected on all laptop computers and other removable storage devices used by the state agency or municipality (Tenn. Code Ann § 47-18-2901).

Educational records: The state board of education is required to develop a detailed data security plan that includes guidelines for authorizing access to teacher and student data, privacy compliance standards, data retention policies, and data breach notification procedures (Tenn. Code Ann. § 49-1-703). Operators of websites aimed at K-12 students must also "implement and maintain reasonable security procedures and practices" in order to protect personally identifiable material from unauthorized access, destruction, use, modification, or disclosure (Tenn. Code Ann. § 49-1-708(c)(1)).

7. Data Disposal

Pursuant to the Identity Theft Victims' Rights Act, any private entity that discards records containing customer personal information must either burn or shred the customer's record, erase or modify the personal identifying information to render it unreadable, or take action to destroy the customer's personal identifying information in a manner that it reasonably believes will ensure that

no unauthorized persons have access to the personal identifying information contained in the customer's record for the period of time between the record's disposal and the record's destruction (Tenn. Code Ann. § 39-14-150(g)).

8. Data Breach

General data breach notification law: Following discovery of a breach of system security, "any person or business that conducts business in this state, or any agency of this state or any of its political subdivisions, that owns or licenses computerized personal information of residents of this state" must disclose the breach of system security within 45 days to any resident of Tennessee whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person (Tenn. Code Ann. § 47-18-2107).

Primary definitions: "Breach of system security" means the acquisition of unencrypted or encrypted data, along with any necessary encryption keys, by an unauthorized person that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder. Good faith acquisition of personal information by an employee or agent of the information holder for the purposes of the information holder is not considered a breach of system security if the personal information is not used or subject to further unauthorized disclosure (Tenn. Code Ann. § 47-18-2107(a)(1)).

An "information holder" is defined as "any person or business that conducts business in this state, or any agency of this state or any of its political subdivisions, that owns or licenses computerized personal information of residents of this state" (Tenn. Code Ann. § 47-18-2107(a)(3)).

"Personal information" is an individual's first name or first initial and last name, in combination with any one or more of the following data elements:

- social security number;
- driver's license number; or
- account, credit card, or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

The term does not include "information that is lawfully made available to the general public from federal, state, or local government records or information that has been redacted, or otherwise made unusable" (Tenn. Code Ann. § 47-18-2107(a)(4)).

Form and content of notice: An information holder may provide notice of a breach of system security by written notice, electronic notice, or substitute notice. Substitute notice is permitted if the information holder demonstrates that the cost of providing notice would exceed $250,000, the affected class of subject persons to be notified exceeds 500,000 persons, or the information holder does not have sufficient contact information to provide regular notice (Tenn. Code Ann. § 47-18-2107(e)).

Notice to nationwide consumer reporting agencies: If an information holder discovers a breach of system security requiring notification of more than 1,000 persons at one time, the information holder must also notify, without unreasonable delay, all consumer reporting agencies and credit bureaus that compile and maintain files on consumers on a nationwide basis of the timing, distribution, and content of the notices (Tenn. Code Ann. § 47-18-2107(g)).

Exceptions to requirements: Tennessee's breach notification law permits information holders to maintain their own notification procedures pursuant to their own information security policies, so long as the information holders comply with their own policies and those policies conform to Tennessee's timing requirements (Tenn. Code Ann. § 47-18-2107(f)). In addition, information holders that are subject to Title V of the Gramm-Leach-Bliley Act or the Health Insurance Portability and Accountability Act are considered to be in compliance (Tenn. Code Ann. § 47-18-2107(i)).

Remedies: The breach notification law allows any customer of an information holder to bring a civil action to recover damages for or enjoin the information holder from violating breach notification requirements (Tenn. Code Ann. § 47-18-2107(h)).

9. Data Transfer & Cloud Computing

While our research has revealed no laws of general application in Tennessee addressing data transfers or cloud computing, service providers operating websites, online applications, or online services for elementary or secondary schools are subject to specific requirements regarding student personal information collected and stored on the cloud (see Section I.E.2.).

10. Other Provisions

Our research has revealed no other generally applicable data management provisions in Tennessee.

D. SPECIFIC TYPES OF DATA

1. Biometric Data

Identity theft: Unique biometric data, such as fingerprints, voice prints, and retina or iris images, are considered personal identifying information and must be protected by personal information holders under the Identity Theft Victims' Rights Act (Tenn. Code Ann. § 39-14-150(e)(2)).

Student data: The Data Accessibility, Transparency and Accountability Act (Tenn. Code Ann. § 49-1-701 to Tenn. Code Ann. § 49-1-708) requires that, unless explicitly mandated by state or federal law, a state agency or educational institution must obtain written consent from the student's parents, or the student if over the age of 18, before collecting "any individual student biometric data, student data relative to analysis of facial expressions, EEG brain wave patterns, skin conductance, galvanic skin response, heart-rate variability, pulse, blood volume, posture, and eye-tracking" (Tenn. Code Ann. § 49-1-706).

2. Consumer Data

Data breach: Tennessee's breach notification law characterizes personal information as an individual's name coupled with defined data elements like social security numbers account numbers, and credit card numbers. (Tenn. Code Ann. § 47-18-2107).

Identity theft: The sale of personal identifying information by an information holder may result in a violation of the Identity Theft Victims' Rights Act–despite notice to and consent of the person identified by the information–when the holder sells the information with intent that it be used to commit an unlawful act (Tenn. Code Ann. § 39-14-150(c)(1)(A)). In addition, Tenn. Code Ann. § 47-18-2110 requires any person or entity that has obtained a federal social security number for a legitimate business or governmental purpose to make reasonable efforts to protect that social security number from disclosure to the public, unless the disclosure is for a legitimate business or governmental purpose and occurs pursuant to the terms of a business or governmental contract or other lawful legal obligation.

Video consumer privacy: Video tape sellers or services are prohibited from knowingly disclosing, to any person, personally identifiable information concerning any consumer of such provider (Tenn. Code Ann. § 47-18-2204). Violators are liable for actual damages to aggrieved customers (Tenn. Code Ann. § 47-18-2205).

3. Credit Card Data

Data breach: When used in combination with a person's name, credit or debit card numbers–together with any required security code, access code, or password allowing access to a resident's

financial accounts–are included in the definition of "personal information" subject to the provisions of the general data breach notification law (Tenn. Code Ann. § 47-18-2107(4)(A)(iii)).

Identity theft: Credit and debit card numbers are included in the definition of "personal identifying information" that, if unlawfully obtained, is subject to Tennessee's identity theft law (Tenn. Code Ann. § 39-14-150(g)(2)). For more information on identity theft, see Section I.G.2.

4. Credit Reports

Security freeze: Tennessee consumers may request that a freeze be placed on their consumer reports either by certified mail or by an electronic means provided by the credit reporting agency. A security freeze prohibits the credit reporting agency from releasing the requesting party's consumer report or credit score relating to the extension of credit without the express authorization of the Tennessee consumer (Tenn. Code Ann. § 47-18-2108(a)). The statute lists several exceptions to this prohibition. See Tenn. Code Ann. § 47-18-2108(m).

Timing and procedure: A consumer reporting agency must place a freeze on a consumer's report no later than three business days after receiving consumer's request (Tenn. Code Ann. § 47-18-2108(b)).

Temporary removal: A consumer reporting agency must temporarily lift a security freeze within 15 minutes of receipt of a request, so long as the consumer provides proper proof of authority and identification and the request is received any day between 6:00 a.m. and 9:30 p.m., as applicable to the consumer (Tenn. Code Ann. § 47-18-2108(f)).

Permanent removal: A consumer reporting agency must permanently remove a security freeze no later than two business days from the receipt of a request (Tenn. Code Ann. § 47-18-2108(j)).

Fees: Before July 1, 2018, consumer reporting agencies may charge reasonable fees for placing or permanently removing a security freeze, not exceeding $7.50 for placing a freeze or $5.00 for permanently removing one. Consumer reporting agencies may not charge any fee to temporarily lift a security freeze (Tenn. Code Ann. § 47-18-2108(l)).

2018 Tenn. Pub. Acts ch. 595, effective July 1, 2018, amends Tenn. Code Ann. § 47-18-2108(l) to prohibit a consumer reporting agency from charging a Tennessee consumer to place, temporarily lift, or permanently remove a security freeze. It further amends Tenn. Code Ann. § 47-18-2109 by amending the notice to be provided to consumers informing consumers of the right to security freezes by deleting the last paragraph of the notice, which discussed the consumer reporting agency's right to charge fees.

Violations: If a consumer reporting agency fails to comply with its legal obligations regarding security freezes, the affected consumer may recover (1) ascertainable losses sustained or damages of not less than $100 or more than $1,000, whichever is greater; (2) punitive damages that the court may allow in a private right of action; and (3) costs and reasonable attorneys' fees incurred in successful action to enforce any liability (Tenn. Code Ann. § 47-18-2108(o)).

Specific provisions for protected consumers: Separate, similar provisions apply to credit freezes placed on behalf of protected consumers (Tenn. Code Ann. § 47-18-2111). A "protected consumer" is defined as a person who is under the age of 16 at the time that a request for a security freeze is made or a person who is incapacitated or for whom a guardian has been appointed (Tenn. Code Ann. § 47-18-2111(a)(1)). A consumer reporting agency must place a security freeze for a protected consumer if it receives a request from the protected consumer's representative that is sent to the address or other point of contact specified by the agency and provides sufficient proof of identification of the protected consumer and representative, sufficient proof of the representative's authority, and any required fee (Tenn. Code Ann. § 47-18-2111(c)). Within 30 days of receiving a

request as outlined above, a consumer reporting agency must place a freeze on the protected consumer's credit report (Tenn. Code Ann. § 47-18-2111(e)).

5. Criminal Records

Dissemination of criminal history record information: The release of "confidential" criminal record information other than to law enforcement agencies for law enforcement purposes constitutes a Class A misdemeanor (Tenn. Code Ann. § 40-32-101(c)(1)). Exceptions, however, apply to the release of records to the comptroller of the treasury (or the comptroller's agent) for purposes of an audit investigation (Tenn. Code Ann. § 40-32-101(c)(2)), and to the release of arrest histories of a defendant or potential witness in a criminal proceeding to an attorney of record (Tenn. Code Ann. § 40-32-101(c)(3)).

Required background checks: Certain entities involved in health care or working with vulnerable individuals are required to conduct background checks for all job applicants. See, for example, Tenn. Code Ann. § 33-2-1202 (mental health and substance abuse facilities), Tenn. Code Ann. § 68-11-256 (licensed nursing homes), and Tenn. Code Ann. § 68-11-233 (licensed home care organizations and hospices).

6. Drivers' Licenses/Motor Vehicle Records

Identify theft: Driver's license numbers are included in the definition of "personal identifying information" that, if unlawfully obtained, is subject to Tennessee's identity theft law (Tenn. Code Ann. § 39-14-150(g)(2)). For more information on identity theft, see Section I.G.2.

Motor vehicle records: Tenn. Code Ann. § 55-25-104 provides that the departments of safety and revenue and their employees or officers shall not disclose personal information about any person obtained by the department in connection with a motor vehicle record, unless written consent of the person is obtained pursuant to Tenn. Code Ann. § 55-25-106. Additional exceptions for various purposes are provided by Tenn. Code Ann. § 55-25-107 for matters of motor vehicle or driver safety and theft, motor vehicle emissions, motor vehicle recalls, or performance monitoring of motor vehicles and dealers by motor vehicle manufacturers, or for use in connection with matters concerning the federal selective services system.

7. Electronic Communications/Social Media Accounts

Phishing: The Anti-Phishing Act (Tenn. Code Ann. § 47-18-5203) prohibits any party from representing itself to be "another person, without the authorization or permission of such other person," through the Internet, e-mail, or other means of digital communication for the purpose of soliciting a resident of the state to provide identifying information or identification documents.

Anti-spam: Tenn. Code Ann. § 47-18-2501 regulates advertising via e-mail. The law prohibits any party doing business in Tennessee from sending by e-mail any "documents consisting of unsolicited advertising material for the lease, sale, rental, gift offer, or other disposition of any realty, goods, services, or extension of credit." However, such e-mails are permissible if the party establishes a toll-free telephone number or e-mail address through which a recipient may request not to receive any further unsolicited documents.

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)).

Employer access to online usernames and passwords: Tenn. Code Ann. § 50-1-1003 (otherwise known as the Employee Online Privacy Act) prevents employers from requesting an employee or prospective employee to (1) disclose passwords to personal Internet accounts, (2) add the employer or employment agency to contacts lists on personal Internet accounts, and (3) access a personal Internet account in the presence of the employer.

8. Financial Information

Data breach: When used in combination with a person's name, credit or debit card numbers–together with any required security code, access code, or password allowing access to a resident's financial accounts–are included in the definition of "personal information" subject to the provisions of the data breach notification law (Tenn. Code Ann. § 47-18-2107(a)(4)). For more information, see Section I.C.8.

Financial records: Under the Financial Records Privacy Act, a financial institution may not disclose to any person, except to the customer or the customer's agent, any financial records relating to that customer unless the customer has authorized disclosure to that person or the financial records are disclosed in response to a lawful subpoena (Tenn. Code Ann. § 45-10-104(a)).

Identity theft: Credit and debit card numbers are included in the definition of "personal identifying information" that, if unlawfully obtained, is subject to Tennessee's identity theft law (Tenn. Code Ann. § 39-14-150(g)(2)). For more information on identity theft, see Section I.G.2.

9. Health Data

Health records privacy: Medical records are not considered public records (Tenn. Code Ann. § 63-2-101(b)(1)), and the name and address and identifying information of a patient is prohibited from being sold or divulged (Tenn. Code Ann. § 63-2-101(b)(2)). See also Tenn. Code Ann. § 50-1-306 (employers may not market or sell medical information); Tenn. Code Ann. §56-7-124 (insurers may not market or sell information that directly identifies the patient).

Access: Health care professionals must furnish to a patient or a patient's authorized representative a copy or summary of such patient's medical records within 10 working days of the patient's or representative's request (Tenn. Code Ann. § 63-2-101(a)). Some health care facilities may have specific records access requirements, such as hospitals, which must "furnish to a patient the patient's hospital records without unreasonable delay upon request in writing" (Tenn. Code Ann. § 68-11-304).

Cancer registry: Tennessee maintains a cancer registry to provide appropriate cancer-related data to "members of the medical, scientific, and academic research communities for purposes of authorized institutional research" (Tenn. Code Ann. § 68-1-1003(a)). All information in the registry is kept confidential (Tenn. Code Ann. § 68-1-1006). Any person who receives information containing the personal identity of any patient and who willfully divulges that identity to persons not authorized by the registry commits a Class C misdemeanor (Tenn. Code Ann. § 68-1-1009).

Communicable and other diseases required to be reported: Whenever any physician, surgeon, or practitioner of medicine knows or suspects that any patient is infected with any communicable disease, except venereal disease, such physician, surgeon, or practitioner of medicine must immediately notify the health authorities of the patient's town or county (Tenn. Code Ann. § 68-5-102).

Health data held by insurance companies: Tenn. Code Ann. § 56-32-125 requires health maintenance organizations (HMOs) to keep confidential any information they maintain relating to the diagnosis, treatment, or health of an enrollee or applicant. Insurance providers are prohibited from requesting or requiring from a current or prospective customer genetic information about the customer or any customer's family member, or disclose genetic information about an individuals without the prior written authorization of the individual or their legal representative (Tenn. Code Ann. § 56-7-2704).

Mental health records: Health providers must keep confidential all "applications, certificates, records, reports, legal documents, and pleadings made," along with information provided or

received in connection with the provision of mental health services (Tenn. Code Ann. § 33-3-103). Violations of confidentiality constitute a Class C misdemeanor (Tenn. Code Ann. § 33-3-116).

Trauma registry: Tennessee maintains a registry of persons who are treated at designated trauma centers or comprehensive regional pediatric centers (CRPCs). All information in the registry is kept confidential (Tenn. Code Ann. § 68-11-259).

Brain trauma registry: Tennessee maintains a central registry of persons who sustain traumatic brain injury. The information provided to the registry is kept confidential (Tenn. Code Ann. § 68-55-204).

Birth defects registry: Tennessee maintains on ongoing program that monitors birth defects statewide. The information collected and analyzed pursuant to this registry is kept confidential (Tenn. Code Ann. § 68-5-506).

Alcohol and drug treatment: The registration and other records of treatment facilities shall remain confidential and are privileged (Tenn. Code Ann. § 33-10-408).

10. Social Security Numbers

Data breach: Social security numbers are included in the definition of "personal information" subject to the provisions of the general data breach notification law (Tenn. Code Ann. § 47-18-2107(a)(4)).

Identity theft: Social security numbers are included in the definition of "personal identifying information" that, if unlawfully obtained, is subject to Tennessee's identity theft law (Tenn. Code Ann. § 39-14-150(g)(2)). For more information on identity theft, see Section I.G.2. In addition, Tenn. Code Ann. § 47-18-2110 requires any person or entity that has obtained a federal social security number for a legitimate business or governmental purpose to make reasonable efforts to protect that social security number from disclosure to the public, unless the disclosure is for a legitimate business or governmental purpose and occurs pursuant to the terms of a business or governmental contract or other lawful legal obligation.

11. Usernames & Passwords

Employer access to online usernames and passwords: Tenn. Code Ann. § 50-1-1003 (otherwise known as the Employee Online Privacy Act) prevents employers from requesting an employee or prospective employee to (1) disclose passwords to personal Internet accounts, (2) add the employer or employment agency to contacts lists on personal Internet accounts, and (3) access a personal Internet account in the presence of the employer. Taking adverse action against an employee or prospective employee for failure to disclose such information is also prohibited.

Data breach: When used in combination with a person's name, account information–combined with a password that permits access to an individual's financial account–is included in the definition of "personal information" subject to the provisions of the general data breach notification law (Tenn. Code Ann. § 47-18-2107).

Identity theft: Personal ID numbers, electronic ID codes, and passwords are included in the definition of "personal identifying information" that, if unlawfully obtained, is subject to Tennessee's identity theft law (Tenn. Code Ann. § 39-14-150(g)(2)). For more information on identity theft, see Section I.G.2.

12. Information about Minors

Information collected by school service providers: Service providers operating websites, online applications, or online services aimed at K-12 students are prohibited from using student data they gather in order to amass a profile about a student or from or selling, renting, or disclosing a

student's information except in certain circumstances (Tenn. Code Ann. § 49-1-708). For more on educational institutions, see Section I.E.2.

Minor victims of crime: Tenn. Code Ann. § 10-7-504(t) makes the identifying information of the minor victim of a criminal offense confidential and not open to inspection by members of the public, unless a court waives the confidentiality at the request of the minor's custodial parent or legal guardian and upon the court's finding of good cause shown; creates certain exceptions.

13. Location Data

Law enforcement activities: Tenn. Code Ann. § 38-1-602 provides that "[u]pon request of a law enforcement agency, a wireless telecommunications service provider shall provide call location information concerning the telecommunications device of the user in order for the requesting law enforcement agency to respond to a call for emergency services or an emergency situation that involves the risk of death or serious physical harm."

14. Other Personal Data

Tenn. Code Ann. § 10-8-102 prohibits libraries from disclosing "any library record that identifies a person as having requested or obtained specific materials, information, or services or as having otherwise used such library."

E. SECTOR-SPECIFIC PROVISIONS

1. Advertising & Marketing

Anti-spam: Tenn. Code Ann. § 47-18-2501 prohibits any party doing business in Tennessee from sending by e-mail any "documents consisting of unsolicited advertising material for the lease, sale, rental, gift offer, or other disposition of any realty, goods, services, or extension of credit." However, such e-mails are permissible if the party establishes a toll-free telephone number or e-mail address through which a recipient may request not to receive any further unsolicited documents. If the sending of unsolicited bulk e-mail results in damage to property, criminal penalties ranging from a Class A misdemeanor (if damage to property is less than $1,000) to a Class A felony (if damage to property exceeds $250,000) may be applicable (Tenn. Code Ann. § 39-14-603; Tenn. Code Ann. § 39-14-105). Persons who incur injuries from the transmission of unsolicited bulk e-mail may file suit to recover actual damages, attorney's fees, and, in lieu of actual damages, the lesser of $10 per e-mail transmitted or $1,000 per day (Tenn. Code Ann. § 39-14-604).

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)).

Phishing: The Anti-Phishing Act (Tenn. Code Ann. § 47-18-5203) prohibits any party from representing itself to be "another person, without the authorization or permission of such other person" through the Internet, e-mail, or other means of digital communication for the purpose of soliciting a resident of this state to provide identifying information or identification documents.

Right of publicity: Tennessee law provides every individual with a property right in the use of his or her "name, photograph, or likeness" in any medium in any manner (Tenn. Code Ann. § 47-25-1103(a)). This right is freely assignable and does not expire upon the death of the individual (Tenn. Code Ann. § 47-25-1103(b)). Knowingly using another individual's name, photograph, or likeness without prior consent constitutes a Class A misdemeanor and gives rise to civil liability (Tenn. Code Ann. § 47-25-1105).

Telemarketing: The Consumer Telemarketing Protection Act (Tenn. Code Ann. § 47-18-1501 to Tenn. Code Ann. § 47-18-1527) prohibits the use of automatic-dialing equipment to transmit recordings for the purpose of advertising goods, services, or property for personal, family, or

household use, or for the purpose of conducting polls or soliciting information, unless consent is received and the call is made between the hours of 8:00 a.m. and 9:00 p.m. (Tenn. Code Ann. § 47-18-1502). Violations constitute Class A misdemeanors and carry fines of $1,000 per call.

Data breach: Businesses engaged in the advertising and marketing sector that own or license data that includes "personal identifying information" as defined under Tennessee's general data breach notification law are subject to the law's provisions regarding required notices of a breach in the security of a system (Tenn. Code Ann. § 47-18-2107). For more information on breach notification requirements, see Section I.C.8.

2. Education

At the state level, the Data Accessibility, Transparency and Accountability Act (Tenn. Code Ann. § 49-1-701 to Tenn. Code Ann. § 49-1-708) controls the release of student records.

Prohibited data collection: Schools are prohibited from collecting individual student data on (1) political affiliation, (2) religion, (3) voting history, and (4) firearms ownership. (Tenn. Code Ann. § 49-1-705).

Access to student records: The law guarantees the right of parents and guardians to access their children's educational records (Tenn. Code Ann. § 49-1-704). A student's educational records can include various types of student data such as state and national assessment results, transcripts, grades and GPA, attendance, demographic data, exit and drop-out information, discipline reports, date of birth, grade level, and expected graduation date. However, the term "student data" explicitly does not include juvenile delinquency records, criminal records, medical and health records, student social security numbers, and student biometric information unless such information is included in a student's educational record (Tenn. Code Ann. § 49-1-702).

Biometric data: In addition, the law requires that a state agency or educational institution obtain written consent from the student's parents, or the student if over the age of 18, before collecting individual student biometric data, such as "student data relative to analysis of facial expressions, EEG brain wave patterns, skin conductance, galvanic skin response, heart-rate variability, pulse, blood volume, posture, and eye-tracking" (Tenn. Code Ann. § 49-1-706).

Online school service providers: Operators of websites, online services, online applications, or mobile applications with actual knowledge that the site, service, or application is used primarily for K-12 school purposes and is designed and marketed for K-12 school purposes (see Tenn. Code Ann. § 49-1-702(11)) are prohibited from knowingly (1) engaging in targeted advertising based on information acquired because of use of the operator's site, service, or application for K-12 school purposes, (2) using information, including persistent unique identifiers, created or gathered by the operator to amass a profile about a student except in furtherance of K-12 school purposes, (3) selling or renting a student's information, and (4) disclosing covered information unless the disclosure is made pursuant to several exceptions (Tenn. Code Ann. § 49-1-708(a)). Operators are required to (1) maintain reasonable security procedures and practices to protect covered information from unauthorized uses, and (2) delete students' covered information upon request of the K-12 school (Tenn. Code Ann. § 49-1-708(c)). Violation of these provisions may give rise to civil liability under the Tennessee Consumer Protection Act (Tenn. Code Ann. § 49-1-708(g)).

Disclosure of student information to charter schools: In Opinion No. 17-39, the Tennessee Attorney General addressed certain questions related to the release of student information to charter schools as required by Tenn. Code Ann. § 49-13-132. The opinion specifies that a school district may not refuse to provide "a list of student names, ages, addresses, dates of attendance, and grade levels completed" to public charter schools on the basis of the Family Educational Rights and Privacy Act (20 U.S.C. § 1232g). Moreover, if the school district has adopted a policy pursuant to FERPA that would otherwise bar the release directory information, the district must "promptly

amend its policy" to permit the release of the directory information specified in Tenn. Code Ann. § 49-13-132. The school district must also notify parents of the new policy and allow them a reasonable opportunity to opt out of the disclosure of student information. The Attorney General also opined that Tenn. Code Ann. § 49-13-132 does not prohibit chartering authorities and public charter schools from using student contact information received from local education agencies to contact parents and provide them with additional public school options available to their children.

Data breach: Businesses engaged in the education sector that own or license data that includes "personal information" as defined under Tennessee's general data breach notification law are subject to the law's provisions regarding required notices of a breach in the security of a system (Tenn. Code Ann. § 47-18-2107). For more information on breach notification requirements, see Section I.C.8.

3. Electronic Commerce

Anti-spam: Tenn. Code Ann. § 39-14-603 prohibits persons from forging e-mail transmission information for the purpose of transmitting unsolicited bulk electronic mail through or into the computer network of an e-mail service provider or its subscribers.

Data breach: Businesses engaged in the electronic commerce sector that own or license data that includes "personal information" as defined under Tennessee's general data breach notification law are subject to the law's provisions regarding required notices of a breach in the security of a system (Tenn. Code Ann. § 47-18-2107). For more information on breach notification requirements, see Section I.C.8.

Identity theft: The sale of personal identifying information by an information holder may result in a violation of the Identity Theft Victims' Rights Act–despite notice to and consent of the person identified by the information–when the holder sells the information with intent that it be used to commit an unlawful act (Tenn. Code Ann. § 39-14-150(c)(1)(A)).

4. Financial Services

Data breach: Credit card numbers and bank account information are considered protected personal information pursuant to Tenn. Code Ann. § 47-18-2107(a)(4). Businesses engaged in the financial sector that own or license data that includes "personal information" as defined under the Commonwealth's general data breach notification law may be subject to the law's provisions regarding required notices in a breach of the security of a system (see Section I.C.8.). However, the law specifically provides that entities subject to the privacy provisions of the federal Gramm-Leach-Bliley Act that maintain procedures for breach notification in accordance with that law are deemed to be in compliance (Tenn. Code Ann. § 47-18-2107(i).

5. Health Care

Access and disclosure requirements: Under Tennessee law, a health care professional must furnish a copy or summary of a patient's medical records within ten working days of a written request by the patient or the patient's authorized representative (Tenn. Code Ann. § 63-2-101(a)). Some health care facilities may have specific records access requirements, such as hospitals, which must "furnish to a patient the patient's hospital records without unreasonable delay upon request in writing" (Tenn. Code Ann. 68-11-304).

Data breach: Businesses engaged in the health care sector that own or license data that includes "personal information" as defined under Tennessee's general data breach notification law are subject to the law's provisions regarding required notices of a breach in the security of a system (Tenn. Code Ann. § 47-18-2107). For more information on breach notification requirements, see Section I.C.8.

Nursing homes: Every nursing home resident or patient has the right to have his records kept confidential (Tenn. Code Ann. § 68-11-901(13)).

Pharmacists: Where necessary, pharmacists may disclose patient information to a person authorized to prescribe drugs or devices, or to communicate a prescription order (Tenn. Code Ann. § 63-10-212(a)).

Health care facilities: Health care facilities are prohibited from divulging the name and address or other identifying information of a patient except for: (1) any statutorily required reporting to health or government authorities; (2) access by an interested third-party payer or designee, for the purpose of utilization reviews, case management, peer reviews, or other administrative functions; (3) access by health care providers from whom the patient receives or seeks care; (4) directory information (if the patient does not object); and any request by OIG or the Medicaid fraud control unit with respect to an ongoing investigation. (Tenn. Code Ann. §68-11-1503).

Communicable and other diseases required to be reported: Whenever any physician, surgeon or practitioner of medicine knows or suspects that any patient is infected with any communicable disease, such physician surgeon, or other practitioner of medicine must immediately notify the health authorities of the patient's town or county (Tenn. Code Ann. § 68-5-102).

Mental health records: Health providers must keep confidential all "applications, certificates, records, reports, legal documents, and pleadings made," along with information provided or received in connection with the provision of mental health services (Tenn. Code Ann. § 33-3-103).

Trauma registry: Tennessee maintains a registry of persons who are treated at designated trauma centers or comprehensive regional pediatric centers (CRPCs). All information in the registry is kept confidential (Tenn. Code Ann. § 68-11-259).

Brain trauma registry: Tennessee maintains a central registry of persons who sustain traumatic brain injury. The information provided to the registry is kept confidential (Tenn. Code Ann. § 68-55-204).

Birth defects registry: Tennessee maintains on ongoing program that monitors birth defects statewide. The information collected and analyzed pursuant to this registry is kept confidential (Tenn. Code Ann. § 68-5-506).

Alcohol and drug treatment: The registration and other records of treatment facilities shall remain confidential and are privileged (Tenn. Code Ann. § 33-10-408).

Cancer registry: Tennessee maintains a cancer registry to provide appropriate cancer-related data to "members of the medical, scientific, and academic research communities for purposes of authorized institutional research" (Tenn. Code Ann. §68-1-1003(a)). All information in the registry is kept confidential (Tenn. Code Ann. § 68-1-1006). Any person who receives information containing the personal identity of any patient and who willfully divulges that identity to persons not authorized by the registry commits a Class C misdemeanor (Tenn. Code Ann. § 68-1-1009).

6. HR & Employment

Access to employee online accounts: The Employee Online Privacy Act (Tenn. Code Ann. § 50-1-1001 to Tenn. Code Ann. § 50-1-1004) prevents employers from requiring or compelling an employee or prospective employee to (1) disclose passwords to personal Internet accounts, (2) add the employer or employment agency to contacts lists on personal Internet accounts, and (3) access a personal Internet account in the presence of the employer. Employers are further prohibited from even requesting that employees disclose passwords to personal email accounts. Taking adverse action against an employee or prospective employee for failure to disclose such information is also prohibited.

Data breach: Employers that own or license data that includes "personal information" as defined under Tennessee's general data breach notification law are subject to the law's provisions regarding required notices of a breach in the security of a system (Tenn. Code Ann. § 47-18-2107). For more information on breach notification requirements, see Section I.C.8.

7. Insurance

Health insurance providers/HMOs: Any information obtained by a health maintenance organization (HMO) relating to the diagnosis, treatment, or health of an enrollee must be held in confidence by the HMO (Tenn. Code Ann. § 56-32-125).

Insurance providers are prohibited from requesting or requiring from a current or prospective customer genetic information about the customer or any customer's family member, or disclose genetic information about an individuals without the prior written authorization of the individual or their legal representative (Tenn. Code Ann. § 56-7-2704).

Real estate insurance: In situations where a borrower must furnish evidence of insurance to a lender as a condition for obtaining or keeping a loan, Tenn. Code Ann. § 47-23-101 prohibits lenders, mortgagees, assignees, or creditors from disclosing, without written consent, insurance policy information to another person or party so as to enable the solicitation or renewal of a policy.

Data breach: Insurers that own or license data that includes "personal information" as defined under Tennessee's general data breach notification law are subject to the law's provisions regarding required notices of a breach in the security of a system (Tenn. Code Ann. § 47-18-2107). For more information on breach notification requirements, see Section I.C.8.

8. Retail & Consumer Products

Consumer data: As information holders, merchants are not prohibited under the Identity Theft Victims' Rights Act from selling personal identifying information of their customers, so long as they notify and secure the consent of the customers identified by the information (Tenn. Code Ann. § 39-14-150(c)(1)(C)). In addition, Tenn. Code Ann. § 47-18-2204 prohibits video tape sellers or services from knowingly disclosing to any person personally identifiable information concerning any consumer without informed, written consent. Per Tenn. Code Ann. § 47-18-2205, violators are liable for actual damages to aggrieved customers.

Right of publicity: A person aggrieved by the unlawful use of the person's name, portrait, or picture for advertising or trade purposes has a private right of action to enjoin the violation and recover damages, and any person committing such a violation is guilty of a misdemeanor (Tenn. Code Ann. § 47-25-1103; Tenn. Code Ann. § 47-25-1105). For more information on the right of publicity, see Section I.E.1.

Data breach: Businesses engaged in the retail and consumer products sector that own or license data that includes "personal information" as defined under Tennessee's general data breach notification law are subject to the law's provisions regarding required notices of a breach in the security of a system (Tenn. Code Ann. § 47-18-2107). For more information on breach notification requirements, see Section I.C.8.

9. Tech & Telecom

Anti-spam: Tenn. Code Ann. § 47-18-2501 prohibits any party doing business in Tennessee from sending by e-mail any "documents consisting of unsolicited advertising material for the lease, sale, rental, gift offer, or other disposition of any realty, goods, services, or extension of credit." However, such e-mails are permissible if the party establishes a toll-free telephone number or e-mail address through which a recipient may request not to receive any further unsolicited documents.

Phishing: The Anti-Phishing Act (Tenn. Code Ann. § 47-18-5203) prohibits any party from representing itself to be "another person, without the authorization or permission of such other person" through the Internet, e-mail, or other means of digital communication for the purpose of soliciting a resident of the state to provide identifying information or identification documents.

Employer access to online usernames and passwords: Tenn. Code Ann. § 50-1-1003 (otherwise known as the Employee Online Privacy Act) prevents employers from requesting an employee or prospective employee to (1) disclose passwords to personal Internet accounts, (2) add the employer or employment agency to contacts lists on personal Internet accounts, and (3) access a personal Internet account in the presence of the employer. Taking adverse action against an employee or prospective employee for failure to disclose such information is also prohibited.

Online school service providers: Operators of websites, online services, online applications, or mobile applications with actual knowledge that the site, service, or application is used primarily for K-12 school purposes and is designed and marketed for K-12 school purposes are prohibited from knowingly (1) engaging in targeted advertising, (2) using information, including persistent unique identifiers, created or gathered by the operator to amass a profile about a student except in furtherance of K-12 school purposes, (3) selling or renting a student's information, and (4) disclosing covered information unless the disclosure is made in furtherance of a K-12 school purpose (Tenn. Code Ann. § 49-1-708).

10. Other Sectors

Our research has revealed no specific Tennessee law provisions applicable to other business sectors.

F. ELECTRONIC SURVEILLANCE

Tennessee's Freedom from Unwanted Surveillance Act (Tenn. Code Ann. § 39-13-609), as redrafted by 2018 Tenn. Pub. Acts ch. 970 (effective July 1, 2018), clarifies that the use of the drone by law enforcement to gather evidence or other information constitutes a search. A drone may be used without a search warrant if used in compliance with applicable FAA rules, exemptions, or other authorizations and it is used (1) to counter a high risk of a terrorist attack, (2) to prevent imminent danger to life, (3) to provide continuous aerial coverage when searching for fugitives or monitoring a hostage situation; (4) to provide expansive aerial coverage when searching for missing persons; (5) to investigate certain motor vehicle accidents, (6) where a criminal offense has occurred on publicly owned property or where the law enforcement agency has reasonable suspicion that a criminal offense has occurred on such property; or (7) at the scene of a fire investigation. The 2018 amendment expands on the present law creating a cause of action for persons who are aggrieved by misuse of a drone by law enforcement by specifying that any such person may seek all appropriate relief, including injunctive relief, destruction of the evidence, information or other data obtained, damages, and reasonable attorney fees (Tenn. Code Ann. § 39-13-609(f)).

Tennessee's wiretapping and electronic surveillance law, Tenn. Code Ann. § 39-13-601, *inter alia*, prohibits one who "[i]ntentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication" or who uses "any electronic, mechanical, or other device to intercept any oral communication" (Tenn. Code Ann. § 39-13-601(a)). However, it is lawful for "a provider of wire or electronic communications service, or a telecommunications company, whose facilities are used in the transmission of a wire communication, to intercept, disclose or use that communication in the normal course of employment while engaged in any activity that is necessary to the rendition of service or to the protection of the rights or property of the provider of that service" (Tenn. Code Ann. § 39-13-601(b)(1)). Furthermore, it is lawful "for a person acting under the color of law to intercept a wire,

oral or electronic communication, where the person is a party to the communication or one of the parties to the communication has given prior consent to such interception" (Tenn. Code Ann. § 39-13-601(b)(4)), and it is lawful for a person not acting under color of law to the same under the same conditions "unless the communication is intercepted for the purpose of committing any criminal or tortious act in violation of the constitution or laws of the state of Tennessee" (Tenn. Code Ann. § 39-13-601(b)(5)).

A person who violates Tenn. Code Ann. § 39-13-601(a) commits a Class D felony (Tenn. Code Ann. §39-13-602). Moreover, Tenn. Code Ann. § 39-13-603 provides for a private cause of action.

G. PRIVATE CAUSES OF ACTION

1. Consumer Protection

In general: The Tennessee Consumer Protection Act of 1977 (Tenn. Code Ann. § 47-18-101 to Tenn. Code Ann. § 47-18-131) provides that any person who suffers an ascertainable loss of money, property, or other thing of value as a result of any unfair or deceptive act or practice specified in Tenn. Code Ann. § 47-18-104(b)–except Tenn. Code Ann. § 47-18-104(b)(27)–may seek actual damages. Enforcement with respect to unspecified deceptive acts is vested "exclusively in the office of the attorney general" (Tenn. Code Ann. § 47-18-104(b)(27)).

General data notification breach law: Any customer of an information holder who is a person or business entity and who is injured by a violation of the data breach notification requirement may sue to recover damages and to enjoin the information holder from further violations (Tenn. Code Ann. § 47-18-2107(h)).

Security freezes: If a consumer reporting agency fails to comply with its legal obligations regarding security freezes, the affected Tennessee consumer may recover actual damages or statutory damages of not less than $100 or more than $1,000, whichever is greater, as well as punitive damages and any other remedies available at law. Successful plaintiffs are also entitled to reasonable costs and fees as determined by the court (Tenn. Code Ann. § 47-18-2108(o)).

2. Identity Theft

Tenn. Code Ann. § 47-18-2104(c) permits private actions for violations of identity theft laws to be brought within two years from the date that the liability arises, or from the date that the injured party discovers the liability in cases where a defendant has concealed it. If a person engages in identity theft willfully or knowingly, the court may award the injured party treble damages, along with other relief it considers necessary and proper (Tenn. Code Ann. § 47-18-2104(d)). Persons affected by a violation of the identity theft laws may bring an action for declaratory and injunctive relief even absent any actual damages. (Tenn. Code Ann. § 47-18-2104(f)). The court may also award plaintiffs reasonable attorneys' fees and costs upon a showing of a violation of the identity theft laws (Tenn. Code Ann. § 47-18-2104(g)).

For purposes of the identity theft laws, "personal identifying information" includes a customer's social security number, driver's license identification number, savings account number, checking account number, applicable PINs or passwords, complete credit or debit card number, demand deposit account number, health insurance identification number, or unique biometric data (Tenn. Code Ann. § 39-14-150(g)(2); see also Tenn. Code Ann. § 47-18-2102).

3. Invasion of Privacy

Patient privacy: Tenn. Code Ann. § 68-11-1501 to Tenn. Code Ann. § 68-11-1505, also known as the Patient's Privacy Protection Act, allows injured parties to seek civil actions for damages for invasion of privacy (Tenn. Code Ann. § 68-11-1504). Divulging identifying information belonging to a patient

for a purpose not permitted by law, or selling such information for any purpose, also constitutes an invasion of the patient's right to privacy (Tenn. Code Ann. § 63-2-101(b)(2)).

Anti-spam: Tenn. Code Ann. § 47-18-2501 regulates advertising via e-mail. The law prohibits any party doing business in Tennessee from sending by e-mail any "documents consisting of unsolicited advertising material for the lease, sale, rental, gift offer, or other disposition of any realty, goods, services, or extension of credit." However, such e-mails are permissible if the party establishes a toll-free telephone number or e-mail address through which a recipient may request not to receive any further unsolicited documents. 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)).

4. Other Causes of Action

Anti-spam: If a person incurs an injury from the transmission of unsolicited bulk e-mail, the person may file suit to recover actual damages, attorney's fees, and, in lieu of actual damages, the lesser of $10 per e-mail transmitted or $1,000 per day (Tenn. Code Ann. § 39-14-604).

Electronic surveillance: The 2018 amendment to Tennessee's Freedom from Unwanted Surveillance Act provides for a cause of action for persons who are aggrieved by misuse of a drone by law enforcement by specifying that any such person may seek all appropriate relief, including injunctive relief, destruction of the evidence, information or other data obtained, damages, and reasonable attorney fees (Tenn. Code Ann. § 39-13-609(f)).

Tenn. Code Ann. § 39-13-603 permits a private cause of action for violations of Tennessee's wiretapping and electronic surveillance law.

Right of publicity: Knowingly using another individual's name, photograph, or likeness without the individual's prior consent gives rise to civil liability (Tenn. Code Ann. § 47-25-1105(a)).

Video consumer privacy: Video tape sellers or services are prohibited from knowingly disclosing, to any person, personally identifiable information concerning any consumer of such provider (Tenn. Code Ann. § 47-18-2204). Violators are liable for actual damages to aggrieved customers (Tenn. Code Ann. § 47-18-2205).

H. CRIMINAL LIABILITY

1. Criminal Records

The release of "confidential" records other than to law enforcement agencies for law enforcement purposes is punishable as a Class A misdemeanor (Tenn. Code Ann. § 40-32-101(c)(1)). However, any such records may be disclosed to the comptroller of the treasury for purposes of audit investigation, and the arrest histories of a defendant or potential witness in a criminal proceeding may be released to an attorney of record in the proceeding (Tenn. Code Ann. § 40-32-101(c)(2)).

2. Offenses Against Property

Under the Tennessee Personal and Commercial Computer Act, knowingly accessing computer or telecommunications systems for the purpose of obtaining money, services, or products, or falsifying computer data or financial instruments, is punishable at minimum as a Class A misdemeanor up to a Class A felony depending on the value of the property or services obtained (Tenn. Code Ann. § 39-14-602(a); Tenn. Code Ann. § 39-14-105). Knowingly accessing, altering, or damaging a computer system, software, or data is subject to similar penalties (Tenn. Code Ann. § 39-14-602(b)). Misrepresenting a person's identity in order to gain access to personal information in motor vehicle records constitutes a Class C misdemeanor (Tenn. Code Ann. § 55-25-112).

3. Invasion of Privacy

Tennessee imposes criminal penalties for multiple types of invasion of privacy violations. Wiretapping and electronic surveillance constitutes a Class D felony under Tenn. Code Ann. § 39-13-602. Intentionally recording or disseminating cellphone or cordless phone transmissions constitutes a Class A misdemeanor under Tenn. Code Ann. § 39-13-604(c). The offense is a Class E felony if the defendant knowingly publishes, distributes, or otherwise disseminates to another (Tenn. Code Ann. § 29-13-604(c)(2)).

4. Identity Theft

Under the Identity Theft Victims' Rights Act, identity theft constitutes a Class D felony, and identity theft trafficking constitutes a Class C felony (Tenn. Code Ann. § 39-14-150(i)).

5. Right of Publicity

Knowingly using another individual's name, photograph, or likeness in any medium, without the individual's prior consent, constitutes a Class A misdemeanor (Tenn. Code Ann. § 47-25-1105(b)).

6. Unlawful Photographing

Knowingly photographing a person when the person has a reasonable expectation of privacy without the person's consent is a Class A misdemeanor if the photograph "would offend or embarrass an ordinary person if such person appeared in the photograph" and "was taken for the purpose of sexual arousal or gratification." (Tenn. Code Ann. § 39-13-605(d)(1)). The offense is elevated to a class E felony if (1) the defendant disseminates such photographs or (2) the victim is under 13 years of age at the time of the offense (Tenn. Code Ann. § 39-13-605(d)(2)). If (1) the photographs are disseminated and (2) the victim is under 13 years of age, the violation constitutes a Class D felony (Tenn. Code Ann. § 39-13-605(d)(3)). Similarly, knowingly spying upon or otherwise viewing a person without the person's consent in a place where the person has a reasonable expectation of privacy is a Class A misdemeanor if the viewing "would offend or embarrass an ordinary person" and "was for the purpose of sexual arousal or gratification of the defendant" (Tenn. Code Ann. § 39-13-607(d)(1)). The offense is elevated to a Class E felony if the subject is under 13 years of age (Tenn. Code Ann. § 39-13-607(d)(2)).

7. Social Security Numbers

Unlawfully disclosing social security numbers constitutes a Class B misdemeanor, subject to statutory exceptions listed at Tenn. Code Ann. § 47-18-2110(b). Each violation is punishable as a separate offense (Tenn. Code § 47-18-2110(c)).

8. Phishing

The Anti-Phishing Act (Tenn. Code Ann. § 47-18-5203) prohibits any party from representing itself to be "another person, without the authorization or permission of such other person," through the Internet, e-mail, or other means of digital communication for the purpose of soliciting a Tennessee resident to provide identifying information or identification documents. Violations of the Anti-Phishing Act constitute Class A misdemeanors, while attempts constitute Class B misdemeanors (Tenn. Code Ann. § 47-18-5203(e)).

9. Anti-spam

If the falsification or forgery of transmission information in connection with the transmission of unsolicited bulk e-mail as prohibited by Tenn. Code Ann. § 39-14-603 results in damage to property, criminal penalties ranging from a Class A misdemeanor (if damage to property is less than $1,000) to a Class A felony (if damage to property exceeds $250,000) may be applicable (Tenn. Code Ann. § 39-14-105; see also Tenn. Code Ann. § 39-14-603(f)).

10. Telemarketing

The use of automatic-dialing equipment to transmit recordings in violation of the Consumer Telemarketing Protection Act constitutes a Class A misdemeanor (Tenn. Code Ann. § 47-18-1508).

11. Real Estate Insurance

Willful failure to keep real estate insurance information confidential in violation of Tenn. Code Ann. § 47-23-101 is a Class A misdemeanor.

12. Electronic Tracking

Knowingly installing an electronic tracking device in or on any vehicle for the purpose of monitoring or following an occupant of the vehicle without all owners' consent constitutes a Class A misdemeanor (Tenn. Code Ann. § 39-13-606(d)). Similarly, it is a Class A misdemeanor to knowingly intercept a radio transmission made by certain law enforcement and public safety officials for the purpose of committing or aiding in the flight from a criminal offense (Tenn. Code Ann. § 39-13-608(c)).

13. Surveillance

The use of a drone by a person with the intent to surveil a person or property or to capture an image of an individual at an open-air event venue, without the person's or owner's consent, constitutes a Class C misdemeanor (Tenn. Code Ann. § 39-13-903).

14. Physical or Mental Health Information

Patient records: It is a Class C misdemeanor for certain entities including accident or health insurers and hospitals to market or sell information identifying a patient relating to their physical or mental health without consent (Tenn. Code § 56-7-124(a)(3)).

Mental health records: Any person who discloses or fails to keep confidential any mental health applications, certificates, records, reports, legal documents, and pleadings made and information provided or received in connection with services under the Mental Health and Substance Abuse and Intellectual and Developmental Disabilities Title of the Tennessee Code commits a Class C misdemeanor (Tenn. Code Ann. § 33-3-116).

Cancer registry: Any person who receives information containing the personal identity of any patient listed in a cancer registry and who willfully divulges that identity to persons not authorized by the cancer registry commits a Class C misdemeanor (Tenn. Code Ann. § 68-1-1009(a)).

Sexually transmitted disease records: All records and information held by the department of health or a local health department relating to known or suspected cases of STDs is strictly confidential. Any person who releases such records without authorization is guilty of a Class C misdemeanor (Tenn. Code Ann. § 68-10-111).

Birth defects registry: A willful disclosure of individually identifiable information contained in the Tennessee birth defects registry is a Class A misdemeanor, and negligent disclosure is a class B misdemeanor (Tenn. Code Ann. § 68-5-506).

Employee health records: An employer may not market or sell medical information that directly identifies an employee without authorization. Such disclosure is a Class C misdemeanor (Tenn. Code Ann. § 50-1-306).

II. REGULATORY AUTHORITIES AND ENFORCEMENT

A. Attorney General

The Attorney General is responsible for the administration of most of Tennessee's privacy and consumer protection laws, including the Identity Theft Deterrence Act (Tenn. Code Ann. § 47-18-2101 to Tenn. Code Ann. § 47-18-2111), Consumer Protection Act (Tenn. Code Ann. § 47-18-101 to Tenn. Code Ann. § 47-18-131), and the Anti-Phishing Act (Tenn. Code Ann. § 47-18-5201 to Tenn. Code Ann. § 47-18-5205).

B. Other Regulators

The State Board of Education is tasked with managing student data pursuant to the Data Accessibility, Transparency and Accountability Act (Tenn. Code Ann. § 49-1-701 to Tenn. Code Ann. § 49-1-708).

The Department of Health administers the Vital Records Act (Tenn. Code Ann. § 68-3-101 to Tenn. Code Ann. § 68-3-106) and reports any violations to the district attorney general (Tenn. Code Ann. § 68-3-105(a)(2)).

C. Sanctions & Fines

Identity theft: Violators of the Identity Theft Deterrence Act (Tenn. Code Ann. § 47-18-2101 to Tenn. Code Ann. § 47-18-2111) are subject to fines of up to $5,000 per day that a person's identity was assumed and can also be subject to injunctions, temporary restraining orders, and asset freezes (Tenn. Code Ann. § 47-18-2105(d)).

Motor vehicle records: Misrepresenting a person's identity in order to gain access to personal information in motor vehicle records is punishable by a criminal fine not to exceed $1,000 (Tenn. Code Ann. § 55-25-112).

Telemarketing: The district attorney general may seek injunctive relief and recover statutory damages and attorney's fees following unlawful use of an automatic dialing equipment for commercial purposes (Tenn. Code Ann. § 47-18-1509). In addition, any individual or corporation found to be in violation of the Consumer Telemarketing Protection Act in a civil action will be liable for a civil penalty in the amount of $1,000 for each call made in violation of the law (Tenn. Code Ann. § 47-18-1510(a)).

D. Representative Enforcement Actions

On May 24, 2017, Tennessee joined 46 other states and the District of Columbia in an $18.5 million settlement with Target Corporation to resolve the states' investigation into the company's 2013 credit card data breach.

E. State Resources

The Tennessee Attorney General has information on its website for consumers regarding envelope stuffing schemes, natural disasters, Internet auction fraud, and vacation claims and offers.

III. RISK ENVIRONMENT

The Tennessee legislature typically is not viewed as activist on privacy and data security issues. As noted above, in 2017 Tennessee updated its breach notification statutes to bring them more in line with those of other states, including providing an encrypted data exemption to the notice obligations. The sponsors of that bill, however, are retiring from the legislature. Relatedly, one-third of the members of the next legislature will be new to the House or the Senate, injecting a great deal of uncertainty about the priorities of the next legislative body. There is no indication privacy or data security matters are front and center for either legislative branch.

In addition, Tennessee will be electing a new governor in 2018. None of the leading gubernatorial candidates have expressed publicly any anticipated or desired privacy or data security initiatives. However, the Tennessee Department of Commerce and Insurance (TDCI) may eventually request that the new governor include as part of the Administration's legislative package the National Association of Insurance Commissioners (NAIC) Model Law on Insurance Data Security, which establishes minimum standards for data security and standards for the investigation of and notification of data breaches for all entities licensed by or registered with TDCI (*e.g.*, insurance companies, producers, third party administrators, utilization review agents).

Tennessee is a business-friendly state, and a number of business organizations take a prominent role in pending legislation considered to affect business operations and other issues. For example, these organizations took an active role to amend the initial version of the recent breach notification statutes so the resulting requirements would more closely align with the realities and practicalities of a company's ability to provide breach notification.

IV. EMERGING ISSUES AND OUTLOOK

A. RECENT LEGISLATION

1. Consumer Report Security Freeze

2018 Tenn. Pub. Acts ch. 595, effective July 1, 2018, amends Tenn. Code Ann. § 47-18-2108(l) to prohibit a consumer reporting agency from charging a Tennessee consumer to place, temporarily lift, or permanently remove a security freeze. It further amends Tenn. Code Ann. § 47-18-2109 by amending the notice to be provided to consumers by deleting the last paragraph of the notice, which discussed the consumer reporting agency's right to charge fees.

2. Electronic Surveillance

The Freedom from Unwanted Surveillance Act redrafts Tenn. Code Ann. § 39-13-609 by specifying that all use of drones by law enforcement must comply with applicable FAA rules, exemptions, or other authorizations. Creates a general requirement that, in order to use a drone to search for and collect evidence or obtain information or other data, law enforcement must first obtain a search warrant or there must be a judicially recognized exception to the warrant requirement at the time of use. Also requires that any evidence, information, or other data collected or obtained by use of a drone (1) be deleted within three business days of collection unless it is directly relevant to an ongoing investigation or criminal prosecution, (2) not be admissible as evidence if it was collected in a manner that does not comply with FAA requirements, (3) not be used as probable cause if unrelated to the purpose of the collection. 2018 Tenn. Pub. Acts ch. 970. Effective July 1, 2018. This statutory regime is consistent with the increasingly important role of state governments in protecting privacy rights in the context of drone operations after the D.C. Circuit's recent decision

in *Electronic Privacy Information Center v. FAA*, No. 16-1297, 2018 BL 215985 (D.C. Cir. June 19, 2018) (rejecting a challenge to the FAA's refusal to address privacy issues in its rulemaking on small drone use on standing grounds).

3. Student Data

The Student Due Process Protection Act makes information reasonably likely to a identify a student accused of committing an alleged sexual offense or alleged violent sexual offense and information reasonably likely to identify the victim of such an offense confidential and not open to inspection by members of the public under the Public Records Act. This confidential information may be redacted from public records. 2018 Tenn. Pub. Acts Ch. 980. Effective July 1, 2018.

4. Data Breach Notification

2017 Tenn. Pub. Acts, ch. 91, effective April 4, 2017, amended the state's data breach notice law to clarify that companies need not give notice of an encrypted data breach, unless the encryption key is also breached. The law rectified confusion created by a 2016 amendment.

Tennessee had adopted a breach notification law in 2005 that specifically exempted providing notice if the breached data was encrypted. But in 2016, the law was amended (2016 Tenn. Pub. Acts ch. 692) to remove the exemption. The law as amended, however, still mentioned in another section that encryption was a means of protecting data. This created confusion for companies about whether they could still avoid providing notice if data was encrypted.

The 2016 law also set a 45-day deadline for data breach notification, which remains unchanged.

5. Minors; Victims' Rights

2017 Tenn. Pub. Acts, ch. 308, effective July 1, 2017, makes the identifying information of the minor victim of a criminal offense confidential and not open to inspection by members of the public under the Public Records Act, unless a court waives the confidentiality with respect only to the minor's name at the request of the minor's custodial parent or legal guardian; creates certain exceptions.

6. Consumer Protection; Telecommunications

2017 Tenn. Pub. Acts, ch. 257, effective July 1, 2017, creates a Class A misdemeanor, civil penalties enforceable by the attorney general and reporter, and a private right of action related to "spoofing" of caller identification, facsimile, and text messaging services. Codified at Tenn. Code Ann. § 47-18-2302.

7. State Vendors

2017 Tenn. Pub. Acts, ch. 114, effective April 19, 2017, makes confidential the identities of vendors providing the state with goods and services used to protect certain electronic, communication, and data storage systems for the purposes of the Public Records Act; authorizes a governmental entity receiving such goods and services to vote to make the identities of such vendors confidential; revises exception as to who may receive such confidential information under the Public Records Act. Amends Tenn. Code § 10-7-504.

8. Digital Assets

2016 Tenn. Pub. Acts Ch. 570, effective July 1, 2016, creates the Revised Uniform Fiduciary Access to Digital Assets Act, which grants the personal representative of a decedent the right to access any digital asset in which at death the decedent had a right or interest.

B. Proposed Legislation

1. Education

SB 1761, introduced Jan. 23, 2018, would require a director of schools to report a breach of security in the administration of the Tennessee Comprehensive Assessment Program (TCAP) test, or any successor test, and the local education agency's response to the breach of security to the commissioner of education and the state board of education within five days of discovering the breach. A related bill, HB 1723, was introduced in the House.

2. Election Hacking

HB 1519, introduced Jan. 10, 2018, would require the coordinator of elections to engage a cybersecurity firm to perform a study of the voter data system in this state and produce a report that details the risk to voter data posed by hacking. A related bill, SB 1681, was introduced in the Senate.

C. Other Issues

1. Equifax Breach

In a press release issued Sept. 19, 2017, Tennessee Attorney General Herbert H. Slatery III announced that he had sent a letter to Equifax expressing his concern about the vulnerability Tennessee residents to identity theft and financial loss as a result of the data breach. The Attorney General did not subsequently announce, however, whether Equifax responded to the letter.

2. Facebook/Cambridge Analytica

In March 2018, Tennessee Attorney General Herbert H. Slatery III joined other attorneys general in a letter sent to Facebook CEO Mark Zuckerberg, asking questions about data-sharing procedures that led to the alleged use of 50 million users' data without their consent by Cambridge Analytica. The National Association of Attorneys General seeks information about how the company will make privacy policies and terms of service clearer and more understandable; what controls the company has over data given to developers; what safeguards are in place to police these activities; and what kinds of user data the social media giant knew Cambridge Analytica was accessing and using, and when.

Facebook sent a detailed response to the National Association of Attorneys General on May 7, 2018, that outlines the company's policies and practices regarding user data, the facts related to the misuse of data, and the steps Facebook is taking to address the incident and prevent any recurrence.

