Bloomberg Law
Privacy & Data Security

Domestic Privacy Profile: DELAWARE

William R. Denny and Jesse L. Noa, of Potter Anderson & Corroon LLP, Wilmington, provided expert review of the Delaware Profile and wrote the Risk Environment section. [Last updated January 2018. — Ed.]

TABLE OF CONTENTS

I. APPLICABLE LAWS AND REGULATIONS

A. CONSTITUTIONAL PROVISIONS

There are no provisions in the Delaware Constitution specifically related to privacy. However, the Delaware Supreme Court has recognized that Delaware has a "commitment to protecting the privacy of its citizens." *Jones v. State*, 745 A.2d 856, 866 (Del. 1999).

B. PERSONAL DATA PROTECTION PROVISIONS

Delaware has several laws dealing generally with privacy and data protection, including the Delaware Online Privacy and Protection Act (DOPPA), Del. Code tit. 6, § 1201C through Del. Code tit. 6, § 1206C), the Student Data Privacy Protection Act (SDPPA), Del. Code tit. 14, § 8101A through Del. Code tit. 14, § 8106A, and the Computer Security Breaches Law, Del. Code tit. 6, § 12B-101 through Del. Code tit. 6, § 12B-104.

1. Who is covered?

DOPPA: The Delaware Online Privacy and Protection Act (DOPPA) prohibits operators of covered Internet websites, online or cloud computing services, or online or mobile applications directed at children from marketing or advertising certain specified products or services (see Section I.B.2., below) on their sites, services, or applications (Del. Code tit. 6, § 1204C(a)). Similar provisions apply to operators of sites, online or cloud computing services, or online or mobile applications that are not directed at children, but that have actual knowledge that a child is using the site, service, or application, and to operators who use an advertising service for marketing purposes (Del. Code tit. 6, § 1204C(b)-(e); see Section I.B.3., below). For the purposes of DOPPA, "children" are defined as Delaware residents under the age of 18 (Del. Code tit. 6, § 1202C(6)).

DOPPA further requires operators of *commercial* Internet websites, online or cloud computing services, or online or mobile applications that collect personally identifiable information about individual users residing in Delaware to make their privacy policies conspicuously available on the sites, services, or applications (Del. Code tit. 6, § 1205C). A "user" for these purposes is defined as an individual who uses the operator's site, service, or application (Del. Code tit. 6, § 1202C(17)).

DOPPA also prohibits book service providers from knowingly disclosing to a government entity, or from being compelled to disclose by any person or government entity, any book service information about a user of the provider's book service (Del. Code tit. 6, § 1206C). A "book service provider" is any commercial entity offering a book service to the public. However, an entity is not considered a book service provided if it sells a variety of consumer products and its book service sales do not exceed 2 percent of the entity's total annual gross sales of consumer products sold in the United States. A "user" for these purposes is defined as an individual who uses the provider's book service (Del. Code tit. 6, § 1202C(15)).

SDPPA: The Student Data Privacy Protection Act (SDPPA) requires that certain online operators implement and maintain reasonable security procedures to protect student data from unauthorized access, destruction, use, modification, or disclosure and to delete such data within 45 calendar days if a school district or school requests deletion of data under the district's or school's control. The law also prohibits certain online operators from knowingly engaging in targeted advertising, using information gathered by the operator to amass a profile of a student, or selling or disclosing

student data under specified circumstances (see Section I.B.2.) (Del. Code tit. 14, § 8105A). The act applies to any individual attending a school in Delaware (Del. Code tit. 14, § 8102A(15)).

Computer Security Breaches Law: The Computer Security Breaches Law currently requires any individual or commercial entity conducting business in Delaware and owning or licensing computerized data that includes personal information about a Delaware resident to conduct a good faith investigation when it becomes aware of a breach in the security of the system to determine the likelihood that personal information has been or will be misused. If such investigation determines that misuse of such information about a Delaware resident has occurred or is reasonably likely to occur, the individual or commercial entity must notify the resident as soon as possible (Del. Code tit. 6, § 12B-102(a)).

Additionally, the Computer Security Breaches Law currently requires any individual or commercial entity that maintains computerized data that includes personal information that the individual or commercial entity does not own or license (*i.e.,* a vendor) to give notice to and cooperate with the owner or licensee of the information of any breach immediately following discovery of the breach if misuse of personal information about a Delaware resident occurred or is reasonably likely to occur (Del. Code tit. 6, § 12B-102(b)).

Delaware has enacted amendments to the Computer Security Breaches Law that become effective April 14, 2018 (see Section I.B.2.).

2. What is covered?

DOPPA: The Delaware Online Privacy and Protection Act (DOPPA) prohibits operators of covered Internet websites, online or cloud computing services, or online or mobile applications directed at children, as well as operators of sites, services, or applications not directed at children who have actual knowledge that children are accessing their operations, from marketing or advertising specified products or services on their sites, services, or applications (Del. Code tit. 6, § 1204C(a)). "Children" are defined as Delaware residents under the age of 18 (Del. Code tit. 6, § 1202C(6)). An "Internet website, online or cloud computing service, or online or mobile application directed at children" means any such operation that is targeted or intended to reach an audience comprised predominantly of children. A site, service, or application will not be deemed to be "directed at children" simply because it refers or links to another site, service, or application directed at children (Del. Code tit. 6, § 1202C(11)). Similar prohibitions apply to operators of sites, services, or applications that are not directed at children but that have actual knowledge that a child is using the site, service, or application (Del. Code tit. 6, § 1204C(b)-(c)). The term "operator" does not include third parties that operate, manage, or host, but do not own, a site, service, or application (Del. Code tit. 6, § 1202C(14)).

The prohibition applies to the following:

- Alcoholic liquor;
- Tobacco products, smokeless tobacco products, and moist snuff;
- Tobacco substitutes;
- Firearms;
- Electronic control devices;
- Fireworks;
- Tanning equipment or facilities;

- Dietary supplements;
- Specified lottery games;
- Salvia divinorum or derivative therefrom;
- Body piercing;
- Branding;
- Tattoos;
- Drug paraphernalia;
- Tongue-splitting; and
- Pornographic materials, as defined by the statute (Del. Code tit. 6, § 1204C(f)(1)-(16)).

For purposes of the DOPPA provision requiring operators of commercial Internet websites, online or cloud computing services, or online or mobile applications that collect personally identifiable information about individual users to make their privacy policy conspicuously available (see Section I.B.1.). "Personally identifiable information" means any personally identifiable information about a user of such services or applications that is collected and maintained by an operator in an accessible form, including first and last name, physical or e-mail address, phone number, social security number, or any other identifier that permits the physical or online contacting of the user (Del. Code tit. 6, § 1202C(15)).

For purposes of DOPPA prohibition on book service providers from providing book service information about a user (see Section I.B.1.), "book service information" is defined as: (a) any information that identifies, relates to, describes, or is associated with a particular person; (b) a unique identifier or IP address when used for such identification purposes; and (c) any information that relates to, or is capable of being associated with, a particular user's access to or use of a book service (Del. Code tit. 6, § 1202C(4)). Book service providers may disclose a user's book service information to a law enforcement agency pursuant to lawful methods or to governmental entities other than law enforcement or other persons or entities in response to a court order if specified conditions are met (Del. Code tit. 6, § 1206C(a)(1)-(3) and (5)-(6)). Book service providers may also disclose a user's book service information to law enforcement entities if (1) the law enforcement entity asserts, orally or in writing, that there is an imminent danger of death or serious physical injury requiring the immediate disclosure of the information and there is insufficient time to obtain a court order, or (2) the provider believes, in good faith, that the information is evidence directly related and relevant to a crime against the provider or that particular user. In addition, disclosure is permitted if the user has given informed, affirmative consent in writing (Del. Code tit. 6, § 1206C(a)(4)). DOPPA also requires that book service providers submit reports regarding the number of requests received for book service information. The report must be posted on the provider's website prior to March 31 each year. If the provider does not have a website, it must post the report prominently on its premises or send the report in both paper and electronic format to the Consumer Protection Unit of the Department of Justice (Del. Code tit. 6, § 1206C(e)). However, a book service provider is not required to submit a report unless it has disclosed book service information related to the access or use of a book service or book of more than 30 total users located in Delaware or users whose locations are unknown and cannot be determined.

SDPPA: The Student Data Privacy Protection Act (SDPPA) prohibits online operators from the following: (1) engaging in targeted advertising based on information including student data and state-assigned student identifiers acquired by the operator; (2) using such information to amass a

profile about a student except in furtherance of K-12 school purposes; (3) selling student data except under certain specified circumstances; (4) or disclosing student data, unless an exception applies (Del. Code tit. 14, § 8105A(1)-(4)). For the purposes of these prohibitions, "student data" is defined as personally identifiable information that: (a) is student performance information; (b) is created or provided by a student or parent to an employee or agent of the Department of Education, school district, or school; (c) is created or provided by a student or parent to an operator in the course of using the operator's site, service, or application for K-12 school purposes; (d) is created or provided by an employee or agent of the school district or school to the operator; or (e) is gathered by the operator and can be used to trace the identity of the student or is linked to information that can be used for this purpose, including a host of statutory examples, such as name, address, phone number, and educational records, among others (Del. Code tit. 14, § 8102A(16)). "Student performance information" is defined as data relating to student performance from early childhood learning programs through postsecondary education: college and career readiness; course and grade; and degree, diploma, or credential attainment. While SDPPA broadly prohibits the foregoing, an operator may disclose student data, provided that (1)-(3) above are not violated, (a) when state or federal law requires disclosure; (b) for legitimate research purposes as required or allowed by state or federal law; or (c) to a state agency, school district, or school, for K-12 school purposes, as permitted by state or federal law (Del. Code tit. 14, § 8105A(5)). There are also certain exceptions to the above prohibitions to the extent that the student data is used in the maintenance, evaluation, development, or improvement of the internet website, online or cloud computing service, or online or mobile application (Del. Code tit. 14, § 8105A(6), (7)). The law also provides certain security, maintenance and destruction requirements that operators must follow (see Section I.B.1.).

Computer Security Breaches Law: The Computer Security Breaches Law currently requires any individual or commercial entity conducting business in Delaware and owning or licensing computerized data that includes personal information about a Delaware resident to conduct a good faith investigation when it becomes aware of a breach in the security of the system to determine the likelihood that personal information has been or will be misused. If such investigation determines that misuse of such information about a Delaware resident has occurred or is reasonably likely to occur, the individual or commercial entity must notify the resident as soon as possible (Del. Code tit. 6, § 12B-102(a)).

Additionally, the Computer Security Breaches Law currently requires any individual or commercial entity that maintains computerized data that includes personal information that the individual or commercial entity does not own or license (*i.e.*, a vendor) to give notice to and cooperate with the owner or licensee of the information of any breach immediately following discovery of the breach if misuse of personal information about a Delaware resident occurred or is reasonably likely to occur (Del. Code tit. 6, § 12B-102(b)).

The law defines "personal information" as a Delaware resident's first name or first initial and last name in combination with any of the following elements, when either the name or the data elements are not encrypted: (a) social security number; (b) driver's license number or Delaware ID card number; or (c) account number or credit or debit card number, in combination with any code or password that would allow access to the resident's financial account (Del. Code tit. 6, § 12B-101(4)). The definition excludes publicly available information that is lawfully made available by a governmental entity (Del. Code tit. 6, § 12B-101(4)). "Notice" includes written notice, telephone notice, or electronic notice (provided it is consistent with the requirements of federal law governing electronic signatures (15 U.S.C. § 7001)). Substitute notice is permitted if the individual or commercial entity shows that the cost of notice will exceed $75,000, the affected class of residents

to be notified exceeds 100,000, or the individual or commercial entity does not have sufficient contact information available. Substitute notice must include e-mail notice if the individual or commercial entity has e-mail addresses for the affected residents, conspicuous posting on the individual's or commercial entity's website, and notice to major statewide media (Del. Code tit. 6, § 12B-101(3)). Individuals or commercial entities that maintain their own notice procedures as part of an information security policy for the treatment of personal information whose procedures are otherwise consistent with the above described provisions are deemed to meet the requirements of the Computer Security Breaches Law, as are individuals and commercial entities regulated by state or federal law that maintain procedures required by the regulator (Del. Code tit. 6, § 12B-103). Notice may be delayed if a law enforcement agency determines that the notice would impede a criminal investigation, but notice must be made as soon as possible after the agency determines that an investigation is no longer impeded (Del. Code tit. 6, § 12B-102(c)).

Effective April 14, 2018, the amended Computer Security Breaches Law will require persons conducting business in the state and owning, licensing, or maintaining personal information of Delaware residents to implement and maintain reasonable procedures and practices to prevent the unauthorized acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business (Del. Code tit. 6, § 12B-100 (effective 4/14/2018)). The amended law has expanded the definition of "personal information" now to include, in addition to the items listed above, (1) passport number, (2) a username or e-mail address in combination with a password or security question that would permit access to the account, (3) medical history, medical treatment by a healthcare professional, or diagnosis of mental or physical condition by a healthcare professional, (4) health insurance policy number, subscriber identification number, or any other unique identifier used by a health insurer to identify the person, (5) DNA profile, (6) biometric data used for authentication purposes, and (7) an individual taxpayer identification number. The revised law continues to exclude from personal information any information that is lawfully available to the general public from government records, and expands this exclusion to include information lawfully available from widely distributed media (Del. Code tit. 6, § 12B-101(7)(b) (effective 4/14/2018)).

The law's notice requirements have also been amended. Under the revised law, the person suffering a data breach will have a 60-day period after determination of the security breach within which to provide notice, unless, during that time, the person reasonably determines after an appropriate investigation that the breach of security is "unlikely to result in harm." "Determination of the breach of security" is defined as the point in time at which the person suffering the breach has sufficient evidence to conclude that a breach of security has taken place (Del. Code tit. 6, § 12B-101(2) (effective 4/14/2018)). This language appears intended to indicate a time later than the actual discovery of an event that later turns out to be a breach of security. The amended law still excludes the notice requirement if the breached data is encrypted; however, this safe harbor will not apply if encrypted data *and* the encryption key are breached. Also new is the requirement that the Delaware Attorney General must be notified if the affected number of Delaware residents to be notified exceeds 500 (Del. Code tit. 6, § 12B-102(d) (effective 4/14/2018)).

The revised law also amends the obligation of vendors to notify their customers of data breaches. Under the revised law, "a person that maintains computerized data that includes personal information that the person does not own or license" (*i.e.,* a vendor) must give immediate notice to "the owner or licensee of the information" (*i.e.,* its customer) upon its determination that there has been a breach of security. As discussed above, under the current version of the law, a vendor is only required to notify its customer of a data breach when the vendor determines that misuse of the information had "occurred or is reasonably likely to occur." The revised law requires that the

vendor must provide immediate notice without any consideration of whether there is a risk of harm. It is up to the customer, the one who owns or licenses the information, to conduct the risk of harm analysis with the cooperation of the vendor.

Additionally, the revised law requires that Delaware residents be offered credit monitoring services, at no cost, for a period of one year if the breach of security includes Social Security numbers.

3. Who must comply?

DOPPA: The Delaware Online Privacy and Protection Act (DOPPA) provisions applicable to online marketing to children described above (see Section I.B.1. and Section I.B.2.) apply to "operators," defined as a person owning an Internet website, online or cloud computing service, or online or mobile application. The term "operator" does not include third parties that operate, manage, or host, but do not own, a site, service, or application (Del. Code tit. 6, § 1202C(14)). The statute also provides that an "Internet website, online or cloud computing service, or online or mobile application directed at children" means any such operation that is targeted or intended to reach an audience comprised predominantly of children. A site, service, or application will not be deemed to be "directed at children" simply because it refers or links to another site, service, or application directed at children (Del. Code tit. 6, § 1202C(11)).

An operator directing its offerings at children that is using an advertising service is not required to comply with Section 1204C(a) of DOPPA (see Section I.B.1. and Section I.B.2.), but must inform the advertising service that its operations are directed at children. In turn, the advertising service must comply with DOPPA provisions (Del. Code tit. 6, § 1204C(d)-(e)). The statute defines "advertising service" as a person who provides, creates, plans, or handles marketing or advertising for another person (Del. Code tit. 6, § 1202C(1)).

The DOPPA provisions applicable to the conspicuous posting of privacy policies apply to any commercial Internet website, online or cloud computing service, or online or mobile application (Del. Code tit. 6, § 1205C(a)). While the statute does not specifically define the term "commercial," it is likely that the provision would be construed to apply to any operator operating a site, service, or application for profit.

The DOPPA provisions protecting the privacy of book service information apply to book services offered by book service providers. A "book service" is defined as a service whereby an entity, as its primary purpose, provides individuals with the opportunity to rent, purchase, borrow, browse, or view books electronically or via the Internet (Del. Code tit. 6, § 1202C(3)). A "book service provider" is any commercial entity offering a book service to the public, except that a commercial entity that offers a variety of consumer products to the public will not qualify as a book service provider if its book service sales do not exceed 2% of the entity's total annual gross consumer sales in the U.S. (Del. Code tit. 6, § 1202C(5)).

SDPPA: The Student Data Privacy Protection Act (SDPPA) applies to "operators," defined as any person other than the Department of Education, school districts, or schools, to the extent that they: (a) operate an Internet website, online or cloud computing service, or online or mobile application with actual knowledge that the foregoing is used primarily for K-12 purposes and was designed and marketed for K-12 school purposes; or (b) collect, maintain, or use student data in a digital or electronic format for K-12 school purposes (Del. Code tit. 14, § 8102A(10)). The Act does not apply to general audience internet websites, online or cloud computing services or online or mobile applications, even if login credentials created for services or applications covered by SDPPA may be used to access those general audience services or applications (Del. Code tit. 14, § 8106A(1)).

Computer Security Breaches Law: The Computer Security Breaches Law's investigation and notice requirements apply to individuals and commercial entities that own or license computerized data that includes personal information about Delaware residents (Del. Code tit. 6, § 12B-102(a)). "Commercial entities" include corporations, business trusts, partnerships, and other delineated business entities (Del Code tit. 6, § 12B-101(2)). The law also creates certain notice and cooperation requirements for vendors, *i.e.,* individuals or commercial entities that maintains computerized information containing personal information that the individual or entity does not own or license (see Section I.B.2.).

The revised Computer Security Data Breach Law, effective April 14, 2018, applies to persons conducting business in the state—including individuals, business entities, and governmental entities—that own, license, or maintain personal information of Delaware residents.

C. Data Management Provisions

1. Notice & Consent

Delaware has no general provisions governing notice and consent regarding personal data, but some sector-specific provisions address the topic. For example, under the Delaware Online Privacy and Protection Act (DOPPA), book service providers may disclose a user's book service information if the user has given informed, affirmative consent in writing (Del. Code tit. 6, § 1206C(a)(4)). For more information on the general prohibition against disclosure by book service providers, see Section I.D.13.

In addition, for purposes of the general prohibition on the interception of wire, oral, or electronic communications, such an interception is permissible if the person is a party to the communication or if one of the parties to the communication has given consent to the interception (Del. Code tit. 11, § 2402(c)(4)). However, Del. Code tit. 11, § 1335 prohibits the installation of any hearing, recording, amplifying, or broadcasting device without the consent of the persons entitled to privacy at the place of installation. In addition, the law makes it a violation of privacy to intercept a telephone communication without the consent of all parties (Del. Code tit. 11, § 1335(a)(4)). For more information on these provisions, see Section I.F.

The Employee/Applicant Protection for Social Medial Act prohibits employers from demanding access to employee's or applicant's personal social media accounts or requiring employees or applicants to access such accounts in the presence of the employer (Del. Code tit. 19, § 709A).

2. Collection & Use

Delaware has no general provisions governing collection and use of personal data, but many of the sector-specific provisions discussed throughout this profile place restrictions on the use of such data. See, for example, Section I.E.2. (regarding prohibiting the use of personal information by an online operator to amass a profile about a student except in furtherance of K-12 school purposes), Section I.D.12. (prohibiting online operators from knowingly using personal information of minors for marketing or advertising services), and Section I.D.2. (regarding the requirement that commercial Internet service providers that collect personal information must conspicuously post their privacy policy), among many others.

3. Disclosure to Third Parties

Delaware has no general provisions governing the disclosure of personal data to third parties, but many of the sector-specific provisions discussed throughout this profile place restrictions on the disclosure of such data. See, for example, Section I.D.13. (regarding restrictions on disclosure of

book service information by book service providers), Section I.E.2. (regarding disclosures of student information by online operators of online sites or services used for K-12 purposes), and Section I.F. (regarding disclosures related to electronic surveillance activities), among many others.

The Victim Online Privacy Act, Del. Code tit. 11, § 9616A, prohibits any person from posting or displaying on the internet the actual address, telephone number or image of any participant in the witness and crime victim protection program, if the intent of posting the information is to incite violence or threaten the program participant, or if the program participant is a minor.

4. Data Storage

There are no general provisions in Delaware law governing the storage of personal data. However, a person or entity providing an electronic communications service or a remote computing service may not knowingly divulge to any other person or entity the contents of an electronic communication while it is in the service's electronic storage (Del. Code tit. 11, § 2422(a); see Section I.D.7.). Additionally, Delaware does regulate the disposal and destruction of records under certain circumstances (see Section I.C.7.).

5. Access & Correction

The Right to Inspect Personnel Files Act (Del. Code tit. 19, § 732) mandates that employers permit an employee, upon request, to inspect the employee's personnel files used to determine his qualifications for employment, promotion, additional compensation, termination, or disciplinary action. Employers must make such records available during regular business hours, although they may require employees to inspect them during their own free time. Employers may, at their discretion, require employees to file a written form requesting access and indicating either the purpose of the inspection or the particular parts of the record requested.

On receiving a record pursuant to the above requirements, an employee may make notes, but employers are not required to allow employees to remove the record from the employer's premises. The employer may require the inspection to take place in the presence of a designated official. The employee must be given sufficient time for inspection commensurate with the volume of the file. Inspections may be limited to once a year, except for reasonable cause (Del. Code tit. 19, § 733).

An employee who disagrees with any information contained in his personnel files may reach an agreement with the employer concerning the removal or correction of the information. If an agreement cannot be reached, the employee has the right to submit a written statement explaining his position that must be attached to the file and must accompany any transmittal or disclosure of the records to a third party (Del. Code tit. 19, § 734).

An employer who refuses an employee access to personnel files in violation of Labor Law requirements is subject to a civil penalty of from $1,000 to $5,000 per violation. The same civil penalties apply to an employer who discharges or discriminates against an employee because the employee has made a complaint, given information to the Department of Education, caused a proceeding to be instituted, or testified in such a proceeding (Del. Code tit. 19, § 735).

6. Data Security

There are currently no general provisions in Delaware law governing the security of personal data, but many of the sector-specific provisions discussed throughout this profile contain data security requirements, including the Student Data Privacy Protection Act (SDPPA) (see Section I.E.2.), among others. However, effective April 14, 2018, Delaware's amended Computer Security Breaches

Law (see Section I.B.2. and Section I.C.8.) will require covered persons to implement and maintain reasonable procedures and practices to prevent the unauthorized acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business.

7. Data Disposal

Del. Code tit. 6, § 5001C through Del. Code tit. 6, § 5004C establish requirements for the safe destruction of records containing personal identifying information by commercial entities. To the extent that a commercial entity seeks to permanently dispose of records containing such information, it must take reasonable steps to destroy or arrange for the destruction of the records by shredding, erasing, or otherwise destroying or modifying the personal identifying information in the records to make it unreadable or indecipherable (Del. Code tit. 6, § 5002C). The law defines "commercial entities" subject to the requirements (Del. Code tit. 6, § 5001C(1)), but provides exemptions for certain businesses such as banks or other financial institutions subject to the federal Gramm-Leach-Bliley Act, health insurers and health care facilities subject to federal HIPAA requirements, consumer reporting agencies subject to the Federal Credit Reporting Act, and governmental subdivisions, agencies, or instrumentalities (Del. Code tit. 6, § 5004C). The law defines "personal identifying information" as a consumer's first name or first initial and last name in combination with any one of the enumerated elements in the statute that relate to the consumer, when either the name or the data elements are not encrypted, including: Social Security number; passport number; driver's license or state identification card number, insurance policy number, financial services account number, bank account number, credit or debit card number, tax or payroll information, confidential health care information, diagnosis, condition or treatment, or evaluation from a health care provider who has treated the patient (Del. Code tit. 6, § 5001C(3)). The law defines "records" as non-public information that is inscribed on a tangible medium, or that is stored in an electronic or other medium and is retrievable in perceivable form on which personal identifying information is recorded or preserved (Del. Code tit. 6, § 5001C(3)-(4)). Consumers damaged by a violation of these provisions may bring a civil action against the commercial entity (Del. Code tit. 6, § 5003C).

Del. Code tit. 19, § 736, entitled "safe destruction of records containing personal identifying information," requires employers seeking to permanently dispose of records containing an employee's personal identifying information to take all reasonable steps to destroy or arrange for the destruction of the records by shredding, erasing, or otherwise destroying or modifying the personal identifying information in the records to make it unreadable or indecipherable. Employees are entitled to bring a civil action against an employer for intentional or reckless violations of this requirement.

Under the Student Data Privacy Protection Act (SDPPA) (see Section I.E.2.), operators in possession of student data must delete such data within a reasonable time (not to exceed 45 days) on the request of a school district or school having control of the data (Del. Code tit. 14, § 8104A(2)).

8. Data Breach

The Computer Security Breaches Law requires any individual or commercial entity conducting business in Delaware and owning or licensing computerized data including personal information about a Delaware resident to conduct "in good faith a reasonable and prompt investigation" when it becomes aware of a breach in the security of the system to determine whether the information has been or will be misused and, if so, to notify the resident as soon as possible (Del. Code tit. 6, § 12B-102(a)). While the law does not define what constitutes a "good faith . . . reasonable and

prompt investigation," it does contain specific provisions related to the notice required if such an investigation reveals that misuse has occurred or is reasonably likely to occur, as outlined below.

The current law defines "personal information" as a Delaware resident's first name or first initial and last name in combination with any of the following elements, when either the name or the data elements are not encrypted: (a) social security number; (b) driver's license number or Delaware ID card number; or (c) account number or credit or debit card number, in combination with any code or password that would allow access to the resident's financial account (Del. Code tit. 6, § 12B-101(4)). However, "personal information" does not include publicly available information lawfully made available to the general public from a government source (Del. Code tit. 6, § 12B-101(4)). "Notice" includes written notice, telephone notice, or electronic notice (provided it is consistent with the requirements of federal law governing electronic signatures (15 U.S.C. § 7001). Substitute notice is permitted if the individual or commercial entity shows that the cost of notice will exceed $75,000, the affected class of residents to be notified exceeds 100,000, or the individual or commercial entity does not have sufficient contact information available. Substitute notice must include e-mail notice if the individual or commercial entity has e-mail addresses for the affected residents, conspicuous posting on the individual's or commercial entity's website, and notice to major statewide media (Del. Code tit. 6, § 12B-101(3)). Individuals or commercial entities that maintain their own notice procedures as part of an information security policy for the treatment of personal information whose procedures are otherwise consistent with the above described provisions are deemed to meet the requirements of the Computer Security Breaches Law if they comply with the notice provisions of their own procedures, as are individuals and commercial entities regulated by state or federal law that maintain procedures required by the regulator and comply with those procedures (Del. Code tit. 6, § 12B-103).

The Computer Security Breaches Law's investigation and notice requirements apply to individuals and commercial entities that own or license computerized data that includes personal information about Delaware residents (Del. Code tit. 6, § 12B-102(a)). "Commercial entities" include corporations, business trusts, partnerships, and other delineated business entities (Del Code tit. 6, § 12B-101(2)). An individual or commercial entity that maintains computerized information containing personal information that the individual or entity does not own or license (*i.e.*, a vendor) must provide notice to the owner or licensee of the information of any breach immediately upon discovery, if misuse occurred or is likely to occur, and must cooperate with the owner by supplying all information relevant to the breach (Del. Code tit. 6, § 12B-102(b)). Notice may be delayed if a law enforcement agency determines that it will impede a criminal investigation, but notice must be made as soon as possible after the agency determines that an investigation is no longer impeded (Del Code tit. 6, § 12B-102(c)).

The recent amendment to the Computer Security Breaches Law, which will become effective April 14, 2018, has made substantial revisions to the law. The amended Computer Security Breaches Law will now require persons conducting business in the state and owning, licensing, or maintaining personal information of Delaware residents to implement and maintain reasonable procedures and practices to prevent the unauthorized acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business.

The amended law has expanded the definition of "personal information," now to include (1) passport number, (2) a username or e-mail address in combination with a password or security question that would permit access to the account, (3) medical information, (4) health insurance information, (5) DNA profile, (6) biometric data used for authentication purposes, and (7) an individual taxpayer identification number. Notwithstanding this expansion, the revised law

continues to exclude from personal information any information that is considered publicly available from a government source, and adds to this exclusion to exclude information publicly available through widely-distributed media.

The law's notice requirements have also been amended. Under the revised law, the owner or licensee of information suffering a data breach will have a 60-day period following determination of the breach within which to provide notice, unless, during that time, the person reasonably determines after an appropriate investigation that the breach of security is "unlikely to result in harm." The amended law still excludes the notice requirement if the breached data is encrypted; however, this safe harbor will not apply if encrypted data and the encryption key are breached, and there is a likelihood that the key could be used to unencrypt the data. Also new is the requirement that the Delaware Attorney General must be notified if the affected number of Delaware residents to be notified exceeds 500.

The revised law also amends the obligation of vendors to notify their customers of data breaches. Under the revised law, "a person that maintains computerized data that includes personal information that the person does not own or license" (*i.e.,* a vendor) must give immediate notice to "the owner or licensee of the information" (*i.e.,* its customer) upon its determination that there has been a breach of security. Under the current version of the law, a vendor is only required to notify its customer of a data breach when the vendor determines that misuse of the information had "occurred or is reasonably likely to occur." The revised law, in contrast, requires that the vendor must provide immediate notice without any consideration of whether there is a risk of harm. It is up to the customer, the one who owns or licenses the information, to conduct the risk of harm analysis with the cooperation of the vendor.

Additionally, the revised law requires that the owner or licensee of data suffering a breach that includes Social Security numbers to offer credit monitoring services, at no cost, to Delaware residents whose data was breached for a period of one year.

9. Data Transfer & Cloud Computing

There are no provisions of Delaware law specifically addressing data transfers.

The provisions of Delaware Online Privacy and Protection Act (DOPPA) that generally prohibit marketing or advertising specified products or services to children (see Section I.D.12.) and that require a conspicuous posting of a privacy policy by certain operators (see Section I.D.2.) are applicable to cloud computing services.

10. Other Provisions

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

D. Specific Types of Data

1. Biometric Data

For purposes of the Student Data Privacy Protection Act (SDPPA) (see Section I.E.2.), biometric data is considered to be "student data" subject to the SDPPA's requirements regarding the use, disclosure, or sale of such data by online operators (Del. Code tit. 14, § 8102A(16)(e)).

The recent amendment to the Computer Security Breaches Law, effective April 14, 2018, modifies the definition of "personal information" to include, among other things, biometric data (discussed in Section I.B.2. and Section I.C.8.; see also Section IV., below).

2. Consumer Data

Conspicuous display of privacy policy: The Delaware Online Privacy and Protection Act (DOPPA) requires certain online operators that collect personally identifiable information about individual users to make their privacy policies conspicuously available on their sites, services or applications (Del. Code tit. 6, § 1205C). The requirement applies to any commercial Internet website, online or cloud computing service, or online or mobile application (Del. Code tit. 6, § 1205C(a)). While the statute does not specifically define the term "commercial," the provision appears to be applicable to any operator operating a site, service, or application for profit. A "user" in this context is defined as an individual who uses the operator's site, service, or application (Del. Code tit. 6, § 1202C(17)).

Under DOPPA, "personally identifiable information" means any personally identifiable information about a user that is collected by an operator, including first and last name, physical or e-mail address, phone number, social security number, or any other identifier that permits the physical or online contacting of the user (Del. Code tit. 6, § 1202C(15)).

The law specifies the elements that must be contained in the privacy policy, including the categories of personally identifiable information collected and the categories of third parties with whom the operator may share the information, the process for reviewing and requesting changes to a user's personally identifiable information, the process by which the operator notifies users of material changes to the policy, and the effective date of the policy. The policy also must disclose how the operator responds to web browser "Do No Track" signals or similar mechanisms and whether other parties may collect personally identifiable information about a user's activities over time and across different websites, services, or applications (Del. Code tit. 6, § 1205C(b)(1)-(7)).

An operator's privacy policy is considered to be "conspicuously available" when the operator makes it available via the Internet through the following means:

- A webpage on which the actual privacy policy is posted if the webpage is the home page or first significant page after entering the website;
- An icon that hyperlinks to a webpage on which the actual privacy policy is posted, if the icon is located on the first significant page after entering the website, contains the word "privacy," and uses a distinct color contrasting with the background color of the webpage;
- A text link meeting the requirements directly above, if the word "privacy" is written in capital letters equal to or greater in size than the surrounding text, or in larger or contrasting type than the surrounding text, or is otherwise set off; or
- Any other functional hyperlink displayed so that a reasonable individual would notice it (Del. Code tit. 6, § 1202C(7)(a)-(d)).

If the Internet website, online or cloud computing service, or online or mobile application is not a website, an operator may use any other reasonably accessible means of making the privacy policy available to users (Del. Code tit. 6, § 1202C(7)(e)).

Destruction of consumer records: Del. Code tit. 6, § 5001C through Del. Code tit. 6, § 5004C establish requirements for the safe destruction of records containing personal identifying information by commercial entities. For more information, see Section I.C.7.

3. Credit Card Data

Credit card numbers are included in the definition of "personal information" subject to the requirements of the Computer Data Breaches Law (Del. Code tit. 6, § 12B-101(4); see Section I.C.8.).

Credit card numbers are included in the definition of "personal identifying information" subject to requirements imposed on specified commercial entities with respect to the destruction of records containing such information (Del. Code tit. 6, § 5001C(3); see Section I.C.7.).

Credit card numbers are included in the definition of "personal identifying information" subject to the requirements imposed on employers with respect to the destruction of records containing such information (Del. Code tit. 19, § 736(a)(1); see Section I.E.6.).

4. Credit Reports

Del. Code tit. 19, § 711(g) makes it an unlawful employment practice for an employer to inquire into or consider the credit history or credit score of an applicant during the initial application process, up to and including the first interview. If an applicant is otherwise qualified, employers may inquire into or consider these items after the first interview. The prohibition does not apply to police jobs or any other position where federal or state law requires or permits a consideration of criminal history.

The provisions of Del. Code tit. 6, § 5001C through Del. Code tit. 6, § 5004C establishing requirements for the safe destruction of records containing personal identifying information by commercial entities do not apply to consumer reporting agencies subject to the Federal Credit Reporting Act (Del. Code tit. 6, § 5004C(3)).

Consumers may place a freeze on their credit reports under the Delaware Clean Credit and Identity Theft Protection Act (Del. Code tit. 6, § 2201 through Del. Code tit. 6, § 2205; see Section I.G.2. for details).

5. Criminal Records

Del. Code tit. 19, § 711(g) makes it an unlawful employment practice for an employer to inquire into or consider the criminal record or criminal history of an applicant during the initial application process, up to and including the first interview. If an applicant is otherwise qualified, employers may inquire into or consider these items after the first interview. Public employers may disqualify an applicant based on criminal history where the exclusion is related to the position in question and consistent with business necessity. In making such a disqualification, the public employer must consider the nature of the offense or conduct, the time that has passed since the incident or the completion of a sentence, and the nature of the job being sought. The prohibition does not apply to police jobs or any other position where federal or state law requires or permits a consideration of criminal history.

The Delaware Bureau of Identification may furnish information pertaining to identification and conviction data about a person to an individual or agency requesting the information for purpose of employment of the person, provided that the requesting individual or agency pays a reasonable fee and the use of the data is limited to the purpose for which it was given (Del. Code tit. 11, § 8513(c)(1)). Further dissemination of this information by the individual or agency requesting it is prohibited (Del. Code tit. 11, § 8513(d)).

Del. Code tit. 16, § 1141 requires licensed nursing facilities—including assisted living facilities, family care homes, retirement homes, and other similar facilities—to conduct a criminal background check

on an applicant prior to employing the applicant in a facility. In addition, the criminal history of any person not directly employed by the facility must be provided to the facility upon that person's commencement of work (Del. Code tit. 16, § 1141(c)). A facility may make a conditional hire and suspend the background check requirement for 60 days, but only if the facility has received verification that the applicant has been fingerprinted by the Bureau of Identification (Del. Code tit. 16, § 1141(d)). The criminal history information is confidential, may only be used in determining if the applicant is suitable for employment, and must be stored in a manner that maintains its confidentiality (Del. Code tit. 16, § 1141(g)). Applicants must provide accurate information sufficient for the facility to secure a criminal history and must execute a release to allow the facility to obtain the history and to provide the history to the facility in which work is to be performed if it is a facility other than the hiring facility (Del. Code tit. 16, § 1141(i)). Other than conditional employment, no applicant may be employed in a facility until the background check has been obtained (Del. Code tit. 16, § 1141(h)). The law provides for civil penalties for both facilities and applicants that violate its requirements (Del. Code tit. 16, § 1141(f) and (j); see Section II.C.). Regulations by the Delaware Department of Health and Social Services specify that disqualifying convictions include any conviction within the prior 15 years for abusing, neglecting, or mistreating a resident of a facility or an impaired adult (Del. Admin. Code tit. 16, § 3105-8.2).

Provisions substantially similar to those described above apply to background checks of applicants for employment in home health agencies and private residences (Del. Code tit. 16, § 1145; Del. Admin. Code tit. 16, § 3110-1.0, et seq.). In addition, drug testing is required for applicants to nursing and similar facilities (Del. Code tit. 16, § 1142) and home health agencies and private residences (Del. Code tit. 16, § 1146).

6. Drivers' Licenses/Motor Vehicle Records

Del. Code tit. 21, § 305 generally prohibits the disclosure of personal information obtained as part of a motor vehicle record. However, such information may be released under certain circumstances, including to a legitimate business to verify the accuracy of personal information submitted by an individual to a business or to obtain correct information for purposes of preventing fraud if information submitted by the individual is incorrect (Del. Code tit. 21, § 305(b)(3)). In addition, such information may be released to an employer or insurer to obtain or verify information relating to a holder of a commercial driver's license required under federal law (Del. Code tit. 21, § 305(b)(9)). Information also may be released if the requestor provides a notarized, written consent from the individual whose information is sought (Del. Code tit. 21, § 305(e)).

7. Electronic Communications/Social Media Accounts

A person or entity providing an electronic communications service or a remote computing service may not knowingly divulge to any other person or entity the contents of an electronic communication while it is in the service's electronic storage (Del. Code tit. 11, § 2422(a)). Exceptions apply for disclosure to addressees or intended recipients of the communication, disclosure with the consent of the originator or an addressee or intended recipient, or other specified circumstances (Del. Code tit. 11, § 2422(b)). Law enforcement officials may also require disclosure under specified circumstances (Del. Code tit. 11, § 2423). Consumers aggrieved by a violation of these requirements may bring a civil action (Del. Code tit. 11, § 2427).

Del. Code tit. 19, § 709A provides that an employer may not require or request an applicant or employee to provide access to personal social media unless an exception applies. For a comprehensive explanation of these provisions, see Section I.E.6.

8. Financial Information

Financial information is included in the definition of "personal identifying information" subject to the requirements of Del. Code tit. 6, § 5001C through Del. Code tit. 6, § 5004C, which establish requirements for the safe destruction of records containing personal identifying information by commercial entities (see Section I.C.7.). Note, however, that the requirements of these laws do not apply to financial institutions subject to the provisions of the federal Gramm-Leach-Bliley Act (see Section I.E.4.).

The Delaware Online Privacy and Protection Act (DOPPA) defines "personally identifiable information" as any personally identifiable information about a user that is collected by an operator, including first and last name, physical or e-mail address, phone number, social security number, or any other identifier that permits the physical or online contacting of the user (Del. Code tit. 6, § 1202C(15)). Accordingly, to the extent that an online operator of a commercial Internet service collects such information, it would be subject to DOPPA requirements that it conspicuously post its privacy policy (see Section I.D.2.).

Insurers subject to the Delaware Insurance Code are prohibited from disclosing non-public personal financial information in violation of the federal Gramm-Leach-Bliley Act. For a comprehensive discussion of this prohibition, see Section I.E.7.

9. Health Data

Document destruction requirements: Confidential health information is included in the definition of "personal identifying information" subject to the requirements of Del. Code tit. 6, § 5001C through Del. Code tit. 6, § 5004C, which establish requirements for the safe destruction of records containing personal identifying information by commercial entities (see Section I.C.7.).

Genetic information: No person may collect genetic information about an individual without first obtaining the individual's informed consent. Exceptions apply for genetic information obtained by law enforcement to establish identity in the course of a criminal investigation, to determine paternity, or to determine the identity of deceased individuals, among others (Del. Code tit. 16, § 1202). Retention of genetic information is prohibited without the informed consent of the individual, and a genetic sample must be destroyed promptly, although there are specified exceptions to both of these requirements (Del. Code tit. 16, § 1203). The law defines the elements required for an individual to give informed consent, which requires signing a consent form including a description of the information to be collected and/or retained and its purpose and potential uses (Del. Code tit. 16, § 1201(4)). Subjects may inspect, request correction of, and obtain genetic information from their records (Del. Code tit. 16, § 1204). Persons may not disclose, or be compelled to disclose, the identity of an individual on whom genetic testing has been conducted or disclose the information in a manner that allows identification of the individual, unless a statutory exception applies (Del. Code tit. 16, § 1205). Violations for unlawfully obtaining, retaining, or disclosing genetic information is punishable by fines, and violators are liable to the victim of a violation (Del. Code tit. 16, § 1208).

Employers may not intentionally collect, directly or indirectly, any genetic information concerning an employee or applicant, or a member of the family of such employee or applicant, unless it can be demonstrated that the information is job-related and consistent with business necessity or that the information is sought in connection with the retirement system of the employer or the underwriting or administration of an employee benefit plan (Del. Code tit. 19, § 711(d)). Violations of this prohibition fall under the general enforcement provisions governing unfair labor practices (Del. Code tit. 19, § 712 and Del. Code tit. 19, § 713), as well as the provisions governing civil

actions by an aggrieved employee (Del. Code tit. 19, § 714 and Del. Code tit. 19, § 715; see Section I.G.4.).

The amended Computer Security Breaches Law includes DNA profile in the expanded definition of personal information, thereby triggering notice requirements for qualifying security breaches (see Section I.B.2.).

HIV testing information: No person may disclose, or be compelled to disclose, the identity of an individual on whom an HIV test is performed or disclose the results of the test in a manner that allows identification of the individual, except to the test subject or a legal guardian, a person who secures a legally effective release, or specified health care facilities or providers, among other exceptions (Del. Code tit. 16, § 717(a)). Persons to whom such information has been lawfully disclosed under the above referenced exceptions may not disclose the results to another person (Del. Code tit. 16, § 717(b)). Persons aggrieved by a violation of these provisions have a private cause of action (Del. Code tit. 16, § 718).

Miscellaneous requirements: Delaware law contains a variety of specific provisions regarding certain types of personal information, records, or data collected and retained by certain health care facilities, including nursing facilities, dental plan organizations, managed care organizations, substance abuse treatment facilities, and mental health hospitals and residential centers. For more information on these requirements, see Section I.E.5.

10. Social Security Numbers

Social security numbers are included in the definition of "personally identifiable information" under the Delaware Online Privacy and Protection Act (DOPPA). Under that law, certain online operators that collect such information about individual users must make their privacy policy conspicuously available on their site, service, or application (Del. Code tit. 6, § 1205C; see Section I.D.2.).

Social security numbers are defined as "personal information" under the Delaware Computer Security Breaches Law. Any individual or commercial entity conducting business in Delaware and owning or licensing computerized data including such personal information about a Delaware resident must conduct a good faith investigation when it becomes aware of a breach in the security of the system to determine whether the information has been or will be misused and, if so, to notify the resident as soon as possible (Del. Code tit. 6, § 12B-102(a); see Section I.C.8.). Under the amended law, effective April 14, 2018, an owner or licensee of information will have an affirmative duty to notify within 60 days of determination of the breach unless, within such 60-day time period, such person reasonably determines after an appropriate investigation that the breach is unlikely to result in harm. If the breach involves Social Security numbers, then the owner or licensee must offer credit monitoring, at no cost to the individual, to every Delaware resident whose Social Security number was breached.

11. Usernames & Passwords

Del. Code tit. 19, § 709A provides that an employer may not require or request an applicant to disclose a username or password to enable employer access to personal social media. For more information on this prohibition, see Section I.E.6.

The amended Computer Security Breaches Law, effective April 14, 2018, expands the definition of "personal information" to include usernames or e-mail addresses, in combination with a password or security question and answer that would permit access to an online account (Del. Code tit. 6, § 12B-101(7)(a)(5)).

12. Marketing to Minors

The Delaware Online Privacy and Protection Act (DOPPA) prohibits operators of Internet websites, online or cloud computing services, online or mobile applications directed to children or operators of the same with actual knowledge that a child is using such services or applications from knowingly using, disclosing, or compiling, or allowing another to use, disclose, or compile, the personal information of the child if that operator has actual knowledge that the child's personally identifiable information will be used for the purpose of marketing or advertising to the child a product or service that is prohibited under the act (Del. Code tit. 6, § 1204C(c)).

13. Location Data

Del. Code tit. 11, § 1335(a)(8) prohibits placing an electronic or mechanical location tracker in a motor vehicle without the consent of the owner. The prohibition does not apply to lawful use of such devices by law enforcement officials or to the installation of a device by a parent or legal guardian to track the location of a minor child.

Del. Code tit. 11, § 1335(a)(9), which governs violations of privacy in the context of disseminating images of a person who is nude or engaged in sexual conduct, includes "geolocation data" as a type of "personally identifiable information" that, when combined with other information, may lead to the identification of an individual.

The Student Data Privacy Protection Act (SDPPA), Del. Code tit. 14, § 8102A, includes "geolocation data" within the scope of its provisions.

14. Other Personal Data

The Delaware Online Privacy and Protection Act (DOPPA) prohibits book service providers from knowingly disclosing to a government entity, or from being compelled to disclose by any person or government entity, any book service information about a user of the provider's book service (Del. Code tit. 6, § 1206C(a)). "Book service information" is defined as any information that identifies, relates to, describes, or is associated with a particular user; a unique identifier or IP address when used for such identification purposes; or any information that relates to, or is capable of being associated with, a user's access to or use of a book service (Del. Code tit. 6, § 1202C(4)). A "book service" is defined as a service whereby an entity, as its primary purpose, provides individuals with the opportunity to rent, purchase, borrow, browse, or view books electronically or via the Internet (Del. Code tit. 6, § 1202C(3)). A "book service provider" is any commercial entity offering a book service to the public, except that a commercial entity that offers a variety of consumer products to the public will not qualify as a book service provider if its book service sales do not exceed 2% of the entity's total annual gross consumer sales in the U.S. (Del. Code tit. 6, § 1202C(5)).

Book service providers may disclose a user's book service information to a law enforcement agency or other governmental entity pursuant to lawful methods or in response to a court order if specified conditions are met (Del. Code tit. 6, § 1206C(a)(1)-(3) and (5)-(6)). In addition, disclosure is permitted if the user has given informed, affirmative consent in writing (Del. Code tit. 6, § 1206C(a)(4)). The law contains further requirements regarding reports that book service providers must submit regarding the number of requests received for book service information. The report must be posted on the provider's website prior to March 31 each year. If the provider does not have a website, it must post the report prominently on its premises or send the report in both paper and electronic format to the Consumer Protection Unit of the Department of Justice (Del. Code tit. 6, § 1206C(e)). However, a report is only required if the book service provider has disclosed book service information related to the access or use of a book service or book of more

than 30 total users consisting of users located in this State or users whose location is unknown and cannot be determined or of both types of users.

E. Sector-Specific Provisions

1. Advertising & Marketing

DOPPA requirements on marketing to minors: The Delaware Online Privacy and Protection Act (DOPPA) prohibits operators of Internet websites, online or cloud computing services, or online or mobile applications directed at children from marketing or advertising specified products or services on their sites, services, or applications (Del. Code tit. 6, § 1204C(a)). "Children" are defined as Delaware residents under the age of 18 (Del. Code tit. 6, § 1202C(6)). An "Internet website, online or cloud computing service, or online or mobile application directed at children" means any such operation that is targeted or intended to reach an audience comprised predominantly of children. A site, service, or application will not be deemed to be "directed at children" simply because it refers or links to another site, service, or application directed at children (Del. Code tit. 6, § 1202C(11)). Similar prohibitions apply to operators of sites, services, or applications that are not directed at children but that have actual knowledge that a child is using the site, service, or application (Del. Code tit. 6, § 1204C(b)-(c)). The term "operator" does not include third parties that operate, manage, or host, but do not own, a site, service, or application (Del. Code tit. 6, § 1202C(14)).

The prohibition applies to the following:

- Alcoholic liquor;
- Tobacco products, smokeless tobacco products, and moist snuff;
- Tobacco substitutes;
- Firearms;
- Electronic control devices;
- Fireworks;
- Tanning equipment or facilities;
- Dietary supplements;
- Specified lottery games;
- Salvia divinorum or derivative therefrom;
- Body piercing;
- Branding;
- Tattoos;
- Drug paraphernalia;
- Tongue-splitting; and
- Pornographic materials, as defined by the statute (Del. Code tit. 6, § 1204C(f)(1)-(16)).

An operator directing its offerings at children, in which marketing or advertising is provided by an advertising service, is not required to comply with DOPPA but must inform the advertising service

that its operations are directed at children. In turn, the advertising service must comply with DOPPA provisions (Del. Code tit. 6, § 1204C(d)-(e)). The statute defines "advertising service" as a person who provides, creates, plans, or handles marketing or advertising for another person (Del. Code tit. 6, § 1202C(1)).

Do-not-call: Although Delaware does not have a "do-not-call" statute specific to the state, the National Do Not Call registry does apply in the state (Do Not Call Brochure, Delaware Attorney General). Additionally, under the Delaware Telemarketing Fraud Act, it is a prohibited telemarketing practice to willfully call or contact a customer by telephone for ten years after having been contacted, orally or in writing, by the customer or his representative to cease and desist from such calls or contacts. A contact or call is "willful" if the person making it knows, or should have known, about the customer's instruction not to call or contact (Del. Code tit. 6, § 2507(a)(3)).

2. Education

The Student Data Privacy Protection Act (SDPPA) prohibits online operators from engaging in any of the following activities:

- engaging in targeted advertising based on information, including student data and state-assigned student identifiers, acquired by the operator;
- using such information to amass a profile about a student except in furtherance of K-12 school purposes;
- selling student data except under certain specified circumstances; or
- disclosing student data, unless an exception applies (Del. Code tit. 14, § 8105A(1)-(4)).

"Student data" is defined as personally identifiable information that: (a) is student performance information; (b) is created or provided by a student or parent to an employee or agent of the Department of Education, school district, or school; (c) is created or provided by a student or parent to an operator in the course of using the operator's site, service, or application for K-12 school purposes; (d) is created or provided by an employee of the Department, school district, or school to the operator; or (e) is gathered by the operator and can be used to trace the identity of the student or is linked to information that can be used for this purpose, including a host of statutory examples, such as name, address, phone number, and educational records, among others (Del. Code tit. 14, § 8102A(16)).

"Operators" include any person other than the Department of Education, school districts, or schools to the extent that they: (a) operate an Internet website, online or cloud computing service, or online or mobile application that is used primarily for K-12 purposes and was designed and marketed for K-12 school purposes; or (b) collect, maintain, or use student data in a digital or electronic format for K-12 school purposes (Del. Code tit. 14, § 8102A(10)).

In addition to the above prohibitions, operators must implement and maintain reasonable security procedures to protect student data from unauthorized access, use, destruction, modification, or disclosure and that, at minimum, meet Department of Technology and Information requirements (Del. Code tit. 14, § 8104A(1)). Operators must delete a student's data within a reasonable time (not to exceed 45 days) on the request of a school district or school having control of the data (Del. Code tit. 14, § 8104A(2)). The law specifically excludes general audience Internet websites and specifies that Internet service providers are not limited from providing Internet connectivity to schools and students, among other exclusions (Del. Code tit. 14, § 8106A).

3. Electronic Commerce

The provisions of the Delaware Online Privacy and Protection Act (DOPPA) regarding the prohibition against advertising and marketing of certain products and services to children; the requirement that specified commercial Internet websites, services, and applications to conspicuously post their privacy policies; and the prohibition on the disclosure of book service information by book service providers each apply to the electronic commerce sector. For more information on these restrictions, see Section I.D.2., Section I.D.12., and Section I.D.13.

The provisions of the Delaware Computer Security Breaches Law also are applicable to any commercial entity engaged in electronic commerce that discovers such a breach. For more information, see Section I.B.2. and Section I.C.8.

4. Financial Services

Del. Code tit. 6, § 5001C through Del. Code tit. 6, § 5004C establish requirements for the safe destruction of records containing personal identifying information by commercial entities, but by the terms of the law, it does not apply to banks or other financial institutions subject to the federal Gramm-Leach-Bliley Act (Del. Code tit. 6, § 5004C(1)) or to consumer reporting agencies subject to the Federal Credit Reporting Act (Del. Code tit. 6, § 5004C(3)).

Restrictions apply to the disclosure of nonpublic personal financial information by entities regulated under the Insurance Code (see Section I.E.7.).

5. Health Care

The Computer Security Breaches Law, Del. Code tit. 6, § 12B-101 through Del. Code tit. 6, § 12B-104, includes medical history, medical treatment by a healthcare professional, diagnosis of mental or physical condition by a healthcare professional, DNA profile, health insurance policy number, subscriber identification number, and any other unique identifier used by a health insurer, in the definition of personal information. However, a person regulated by the federal Health Insurance Portability and Affordability Act (HIPAA) is not obligated to comply with the Computer Security Breaches law to the extent that it maintains procedures for breach pursuant to HIPAA and notifies affected Delaware residents of a data breach in accordance with such procedures. (Del. Code tit. 6, § 12B-103)

Del. Code tit. 6, § 5001C through Del. Code tit. 6, § 5004C establish requirements for the safe destruction of records containing personal identifying information by commercial entities, but by the terms of the law, it does not apply to health care providers subject to the privacy and security standards of the federal Health Insurance Portability and Affordability Act (HIPAA) (Del. Code tit. 6, § 5004C(2)).

Del. Code tit. 16, § 1121(6) requires nursing facilities to keep all medical records confidential and prohibits their disclosure without the express consent of the patient or resident. In addition, Del. Code tit. 16, § 1121(19) gives patients and residents at nursing facilities the right to inspect all records pertaining to them on oral or written request within 24 hours of notifying the facility. The patient or resident also has the right to purchase copies of the records, at a reasonable cost, on written request with two days of notice of the request to purchase. The Department of Health and Social Services may impose civil penalties for violations of these provisions (Del. Code tit. 16, § 1109(c); see Section II.C.).

Del. Code tit. 18, § 3820 prohibits any dental plan organization from disclosing information pertaining to the diagnosis, treatment, or health of any enrollee except to the extent necessary to

comply with laws governing dental plan organizations or with the express consent of the enrollee. Exceptions apply to disclosures pursuant to court order or pertaining to a claim or litigation between the organization and the enrollee. Failure to comply with this prohibition subjects an organization to possible suspension or revocation of its certificate of authority (Del. Code tit. 18, § 3815), a cease-and-desist order (Del. Code tit. 18, § 3816), or civil penalties (Del. Code tit. 18, § 3817; see Section II.C.).

Similar provisions to those described above for dental plan organizations apply to managed care organizations (Del. Code tit. 18, § 6412). Organizations violating the nondisclosure requirement are subject to civil penalties (Del. Code tit. 18, § 6419; see Section II.C.).

Del. Code tit. 16, § 2220(6) specifies that a substance abuse treatment facility must treat patient records confidentially and may not disclose the records publicly without the consent of the patient.

Del. Code tit. 16, § 5161(b)(13) specified that mental health hospitals and residential centers must release their records to the patient or the patient's guardian, unless a statutory exception applies. In addition, such facilities may not release such records to any other person without the consent of the patient or guardian except under specified circumstances.

6. HR & Employment

Inquiries into criminal records and credit history: Del. Code tit. 19, § 711(g) makes it an unlawful employment practice for an employer to inquire into or consider the criminal record, criminal history, credit history, or credit score of an applicant during the initial application process, up to and including the first interview. If an applicant is otherwise qualified, employers may inquire into or consider these items after the first interview. Public employers may disqualify an applicant based on criminal history where the exclusion is related to the position in question and consistent with business necessity. In making such a disqualification, the public employer must consider the nature of the offense or conduct, the time that has passed since the incident or the completion of a sentence, and the nature of the job being sought. The prohibition does not apply to police jobs or any other position where federal or state law requires or permits a consideration of criminal history.

Access and correction of personnel files: Del. Code tit. 19, § 732 mandates that employers permit an employee, upon request, to inspect the employee's personnel files used to determine his qualifications for employment, promotion, additional compensation, termination, or disciplinary action. Employers must make such records available during regular business hours, although they may require employees to inspect them during their own free time. Employers may, at their discretion, require employees to file a written form requesting access and indicating either the purpose of the inspection or the particular parts of the record requested.

On receiving a record pursuant to the above requirements, an employee may make notes, but employers are not required to allow employees to remove the record from the employer's premises. The employer may require the inspection to take place in the presence of a designated official. The employee must be given sufficient time for inspection commensurate with the volume of the file. Inspections may be limited to once a year, except for reasonable cause (Del. Code tit. 19, § 733).

An employee who disagrees with any information contained in his personnel files may reach an agreement with the employer concerning the removal or correction of the information. If an agreement cannot be reached, the employee has the right to submit a written statement explaining his position that must be attached to the file and must accompany any transmittal or disclosure of the records to a third party (Del. Code tit. 19, § 734).

An employer who refuses an employee access to personnel files in violation of Labor Law requirements is subject to a civil penalty of from $1,000 to $5,000 per violation. The same civil penalties apply to an employer who discharges or discriminates against an employee because the employee has made a complaint, given information to the Department of Labor, caused a proceeding to be instituted, or testified in such a proceeding (Del. Code tit. 19, § 735).

Disposal of personnel records: Del. Code tit. 19, § 736 requires employers seeking to permanently dispose of records containing an employee's personal identifying information to take all reasonable steps to destroy or arrange for the destruction of the records by shredding, erasing, or otherwise destroying or modifying the personal identifying information in the records to make it unreadable or indecipherable. Employees are entitled to bring a civil action against an employer for intentional or reckless violations of this requirement.

Social media accounts: Del. Code tit. 19, § 709A provides that an employer may not require or request an applicant to do any of the following:

- Disclose a username or password to enable employer access to personal social media;
- Access personal social media in the presence of the employer;
- Use personal social media as a condition of employment;
- Divulge any personal social media, unless an exception applies;
- Add a person, including the employer, to the list of contacts associated with the personal social media of the employee or applicant, or invite or accept an invitation from any person, including the employer, to join a group associated with such personal social media; or
- Alter the settings of an employee's or applicant's personal social media that affect a third party's ability to view its contents (Del. Code tit. 19, § 709A(b)).

The restrictions do not apply to accessing devices or services provided by the employer for work purposes or to electronic data stored on the employer's network. In addition, employers may conduct investigations concerning employee misconduct and may view information about an employee or applicant available in the public domain (Del. Code tit. 19, § 709A(c)-(g)). Finally, employers are prohibited from discharging, disciplining, threatening to discharge or discipline, or otherwise retaliating against an employee for refusing to comply with a demand for access that violated these provisions (Del. Code tit. 19, § 709A(h)).

Employee monitoring: Del. Code tit. 19, § 705(b) prohibits employers from monitoring or intercepting a telephone conversation, e-mail or electronic transmission, or Internet access or use information of an employee unless the employer either: (a) provides an electronic notice of such monitoring policies to the employee during each day the employee accesses the employer-provided e-mail or Internet access; or (b) has first given a one-day notice to the employee of the monitoring activity that is in writing, in an electronic record, or other electronic form, and has been acknowledged by the employee in writing or electronically. Exceptions are provided for court-ordered actions (Del. Code tit. 19, § 705(b), second paragraph) and for computer system maintenance or protection processes (Del. Code tit. 19, § 705(e)). Civil penalties apply to violations (Del. Code tit. 19, § 705(c); see Section II.C.).

References: An employer who discloses information about a current or former employee's job performance to a prospective employer is presumed to be acting in good faith and is immune from civil liability in connection with the disclosure unless a lack of good faith is shown. In addition to job

performance, information may include acts committed by the employee that would constitute a violation of federal, state, or local law; or an evaluation of the ability (or lack thereof) of the employee to meet the standard of the employee's position. A lack of good faith may be shown when the information provided was knowingly false, deliberately misleading, or rendered with malicious purposes; or when it was disclosed in violation of a nondisclosure agreement or was otherwise legally confidential (Del. Code tit. 19, § 709).

Genetic information: Employers may not intentionally collect, directly or indirectly, any genetic information concerning an employee or applicant, or a member of the family of such employee or applicant, unless it can be demonstrated that the information is job-related and consistent with business necessity or that the information is sought in connection with the retirement system of the employer or the underwriting or administration of an employee benefit plan (Del. Code tit. 19, § 711(e)). Violations of this prohibition fall under the general enforcement provisions governing unfair labor practices (Del. Code tit. 19, § 712 and Del. Code tit. 19, § 713), as well as the provisions governing civil actions by an aggrieved employee (Del. Code tit. 19, § 714 and Del. Code tit. 19, § 715; see Section I.G.4.).

Electronic surveillance: Provisions of the Criminal Code applicable to electronic surveillance and privacy violations are applicable in the employment context (see Section I.F.).

7. Insurance

Del. Code tit. 18, § 535 prohibits insurers regulated under the Delaware Insurance Code from disclosing any nonpublic personal financial information in violation of the federal Gramm-Leach-Bliley Act. The Delaware Commissioner of Insurance has adopted regulations specifying these nondisclosure requirements (Del. Admin. Code tit. 18, § 904-1.0 through Del. Admin. Code tit. 18, § 904-16.0). While the title of the regulations refers to the privacy of consumer financial and health information, they define "nonpublic personal information" to encompass nonpublic personal financial information, which in turn is defined to include personally identifiable financial information as set forth in the regulations.

Under the HIV Testing for Insurance Act (Del. Code tit. 18, § 7401 through Del. Code tit. 18, § 7405), an insurer may not require that an applicant submit to an HIV test unless the insurer obtains the applicant's prior written consent, reveals the uses to which test results may be put and to whom they may be disclosed, and provides the applicant with written information on the testing (Del. Code tit. 18, § 7403). Insurer disclosure of test result information is strictly limited by the statute to situations like reports to a medical information exchange agency (Del. Code tit. 18, § 7404 and Del. Code tit. 18, § 7405).

The Computer Security Breaches Law, Del. Code tit. 6, § 12B-101 through Del. Code tit. 6, § 12B-104, includes health insurance policy number, subscriber identification number, and any other unique identifier used by a health insurer, in the definition of personal information. However, a person regulated by the federal Health Insurance Portability and Affordability Act (HIPAA) is not obligated to comply with the Computer Security Breaches Law to the extent that it maintains procedures for breach pursuant to HIPAA and notifies affected Delaware residents of a data breach in accordance with such procedures. (Del. Code tit. 6, § 12B-103)

Del. Code tit. 6, § 5001C through Del. Code tit. 6, § 5004C establish requirements for the safe destruction of records containing personal identifying information by commercial entities, but by the terms of the law, it does not apply to health insurers subject to the privacy and security standards of the federal Health Insurance Portability and Affordability Act (HIPAA) (Del. Code tit. 6, § 5004C(2)).

8. Retail & Consumer Products

A number of the privacy and data security provisions discussed in this profile are applicable to businesses operating in the retail and consumer product sector, including the following: (a) provisions of the Delaware Online Privacy and Protection Act (DOPPA) restricting online marketing of specified products or services to minors (see Section I.E.1.), requiring commercial Internet websites, online and cloud computing services, and online or mobile applications to conspicuously post their privacy policies (see Section I.D.2.), and prohibiting the disclosure of book service information by book service providers (see Section I.D.13.); (b) provisions of the Delaware Computer Security Breaches Law (see Section I.B.2. and Section I.C.8.); and (c) requirements for the safe destruction of records containing personal identifying information by commercial entities (see Section I.C.7.).

9. Social Media

Del. Code tit. 19, § 709A restricts employers from accessing the personal social media of applicants or employees under specified circumstances (see Section I.E.7.).

10. Tech & Telecom

There do not appear to be any provisions regarding privacy and data security specifically applicable to the telecommunications industry. However, relevant provisions for this sector include provisions of the Delaware Online Privacy and Protection Act (DOPPA) requiring commercial Internet websites, online and cloud computing services, and online or mobile applications to conspicuously post their privacy policies (see Section I.B.2. and Section I.D.2.); provisions of the Delaware Computer Security Breaches Law (see Section I.B.2. and Section I.C.8.); and requirements for the safe destruction of records containing personal identifying information by commercial entities (see Section I.C.7.). See also Section I.F. regarding electronic surveillance.

11. Other Sectors

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

F. ELECTRONIC SURVEILLANCE

Criminal Code provisions: Delaware appears to have conflicting provisions in its Criminal Code regarding electronic surveillance. Del. Code tit. 11, § 2401 through Del. Code tit. 11, § 2412 impose restrictions on electronic surveillance and interception of communications. Under these provisions, no person may intentionally intercept, attempt to intercept, or procure any other person to intercept any wire, oral, or electronic communication. In addition, no person may use or disclose the contents of any information contained in a communication intercepted in violation of this prohibition (Del. Code tit. 11, § 2402(a)). However, such an interception is permissible if the person is a party to the communication or if one of the parties to the communication has given consent to the interception (Del. Code tit. 11, § 2402(c)(4)). Accordingly, it would appear that individuals would be allowed under this law to record their own conversations.

Meanwhile, Del. Code tit. 11, § 1335, which governs violations of privacy in the context of eavesdropping, prohibits the installation of any hearing, recording, amplifying, or broadcasting device without the consent of the persons entitled to privacy at the place of installation. In addition, the law makes it a violation of privacy to intercept a telephone communication without the consent of all parties (Del. Code tit. 11, § 1335(a)(4)). Thus, the privacy law appears to be more restrictive in its requirements than the interception law described above.

Both laws provide for exceptions to the prohibitions on interception and surveillance, including for specified law enforcement purposes or for certain telephone company functions (Del. Code tit. 11, § 2402(c) and Del. Code tit. 11, § 1335(b)). In addition, the interception law provides for a private cause of action for violations (Del. Code tit. 11, § 2409), and the privacy law provides that an illegal interception of communications and installation of an illegal recording device are class A misdemeanors (Del. Code tit. 11, § 1335(c)).

Motor vehicle tracking devices: Del. Code tit. 11, § 1335(a)(8) prohibits placing an electronic or mechanical location tracker in a motor vehicle without the consent of the owner. The prohibition does not apply to lawful use of such devices by law enforcement officials or to the installation of a device by a parent or legal guardian to track the location of a minor child.

Employee monitoring: Del. Code tit. 19, § 705(b) prohibits employers from monitoring or intercepting a telephone conversation, e-mail or electronic transmission, or Internet access or use information of an employee unless the employer either: (a) provides an electronic notice of such monitoring policies to the employee during each day the employee accesses the employer-provided e-mail or Internet access; or (b) has first given a one-day notice to the employee of the monitoring activity that is in writing, in an electronic record, or other electronic form, and has been acknowledged by the employee in writing or electronically. Exceptions are provided for court-ordered actions (Del. Code tit. 19, § 705(b), second paragraph) and for computer system maintenance or protection processes (Del. Code tit. 19, § 705(e)). Civil penalties apply to violations (Del. Code tit. 19, § 705(c); see Section II.C.).

G. PRIVATE CAUSES OF ACTION

1. Consumer Protection

A consumer who incurs actual damages due to a reckless or intentional violation of provisions requiring commercial entities to properly destroy records containing personal identifying information (see Section I.C.7.) may bring a civil action against the commercial entity (Del. Code tit. 6, § 5003C).

Subscribers or consumers of an electronic communications service that are aggrieved by a knowing and intentional violation of provisions prohibiting such services from divulging the content of electronic communications stored on the service's electronic storage (see Section I.D.7.) may recover appropriate relief in a civil action, including preliminary and other equitable or declaratory relief, damages, and reasonable attorney fees and costs. Damages include actual damages suffered by the victim and profits made by the violator, with a minimum recovery of $1,000. Any action must be filed within two years of the day the claimant first discovered or had a reasonable opportunity to discover the violation (Del. Code tit. 11, § 2427).

2. Identity Theft

Del. Code tit. 11, § 854 prohibits identity theft. "Identity theft" is defined as knowingly or recklessly obtaining, possessing, using, selling, giving, or transferring personal identifying information belonging to another person either with the intent to use the information to commit a crime or to knowingly or recklessly facilitate the use of the information by a third person to commit a crime (Del. Code tit. 11, § 854(a)-(b)). "Personal identifying information" includes a variety of personal data including name, address, social security number, savings and checking account numbers, and other forms of information (Del. Code tit. 11, § 854(c)).

Identity theft is a class D felony in Delaware (Del. Code tit. 11, § 854(d)). When a person is convicted of or pleads guilty to identity theft, the sentencing judge must order full restitution to the victim for monetary loss, including documented wage losses and reasonable attorney fees (Del. Code tit. 11, § 854(e)).

Victims of identity theft may be issued "identity theft passports" that may be presented to law enforcement officials and creditors to prevent the victim's arrest or to aid in a creditor's identity theft investigation (Del. Code tit. 11, § 854A).

Under the Delaware Clean Credit and Identity Theft Protection Act (Del. Code tit. 6, § 2201 through Del. Code tit. 6, § 2205), a consumer is authorized to place a security freeze on his own credit report, and consumer reporting agencies must place the freeze on the consumer's report no later than three business days after receiving the request. The agency must send a written confirmation of the freeze to the consumer within five business days of placing the freeze and must provide the consumer with a personal identification number that the consumer may use to permit a release of credit information for a specific period of time or to lift the freeze permanently (Del. Code tit. 6, § 2203(b)). The law specifies procedures for requesting release of information or for lifting the freeze, identifies circumstances under which the security provision does not apply and the agencies that are not required to place a security freeze, and provides for circumstances under which the reporting agency may charge the consumer in connection with a fee (Del. Code tit. 6, § 2203(b)(4)-(14)). Specific security freeze provisions apply to minors (persons under age 16) and persons who are incapacitated or protected persons for whom a guardian or conservator has been appointed (Del. Code tit. 6, § 2205).

Consumers may file a civil action against a consumer reporting agency that negligently releases information placed under a security freeze. The consumer may be granted injunctive relief and may recover a civil penalty of up to $1,000 for each violation plus any damages available under other civil laws, as well as reasonable attorney fees, court costs and expenses (Del. Code tit. 6, § 2203(d)).

3. Invasion of Privacy

Del. Code tit. 11, § 1335 is Delaware's primary invasion of privacy law. It relates specifically to trespassing for the purpose of subjecting a subject to eavesdropping or surveillance and installing or using specified eavesdropping methods and equipment (see Section I.F.). In addition, the law prohibits placing an electronic or mechanical location tracker in a motor vehicle without the consent of the owner (Del. Code tit. 11, § 1335(a)(8)), recording persons in a state of undress (Del. Code tit. 11, § 1335(a)(6)-(7)), and knowingly reproducing or distributing a visual depiction of nudity or sexual conduct (Del. Code tit. 11, § 1335(a)(9)).

4. Other Causes of Action

An employee who incurs actual damages due to a reckless or intentional violation of provisions regarding the proper destruction of employee personnel records (see Section I.E.6.) may bring a civil action against the employer (Del. Code tit. 19, § 736(c)).

A person whose wire, oral, or electronic communications have been intercepted, disclosed, or used in violation of Del. Code tit. 11, § 2401 through Del. Code tit. 11, § 2412 (see Section I.F.) has a civil cause of action against the person committing the violation and may recover actual damages (not less than liquidated damages computed at the rate of $100 per day for each day of violation or $1,000, whichever is greater), punitive damages, and reasonable attorney fees and costs (Del. Code tit. 11, § 2409).

Employers who violate Labor Law provisions prohibiting the monitoring of employee telephone, e-mail, and Internet usage (see Section I.E.6.) are subject to civil penalties of $100 per violation. A civil penalty claim may be filed in any court of competent jurisdiction (Del. Code tit. 19, § 705(c)).

A person whose motor vehicle record information is impermissibly obtained (see Section I.D.6.) may bring a civil cause of action against the violator. A court may award actual damages (not less than $2,500 in liquidated damages), punitive damages if the violation is reckless or willful, reasonable attorney fees and costs, and other equitable relief (Del. Code tit. 21, § 305(o)).

An employee who is the victim of an employer violation regarding the disclosure of genetic information about the employee (see Section I.D.9.), upon exhausting administrative remedies provided by law, may file a civil action in Superior Court to redress the violation as employment discrimination (Del. Code tit. 19, § 714). Remedies available to the Superior Court include an order to cease and desist, the payment of compensatory damages, and reasonable attorney's fees and costs, as well as a fine of not less than $1,000 nor more than $5,000 for each violation (Del. Code tit. 19, § 715).

Persons who are victims of an unauthorized HIV test or of unlawful disclosure of their information concerning HIV testing (see Section I.D.9.) have a right of action in Superior Court. They may recover the greater of actual damages or $1,000 for negligent violations, the greater of actual damages or $5,000 for intentional or reckless violations, reasonable attorney fees, and other relief. The action must be brought within three years of the injured party's discovery that an unauthorized HIV test was performed or that an unlawful disclosure has occurred. Finally, the Attorney General may also bring a civil cause of action when appropriate (Del. Code tit. 19, § 713).

H. Criminal Liability

Del. Code tit. 11, § 1335 –which, among other provisions, prohibits the installation of any hearing, recording, amplifying, or broadcasting device without the consent of the persons entitled to privacy at the place of installation (see Section I.F.)–provides that violations constitute either a Class A misdemeanor or a class G felony, depending on the violation (Del. Code tit. 11, § 1335(c)).

II. REGULATORY AUTHORITIES AND ENFORCEMENT

A. Attorney General

The Attorney General's Division of Consumer Protection is responsible for the enforcement of the Delaware Computer Security Breaches Law (see Section I.C.8.), the Delaware Online Privacy and Protection Act (DOPPA) (see Section I.D.2., Section I.D.12., and Section I.D.13.), and the Student Data Privacy Protection Act (SDPPA) (see Section I.E.2.). The Division of Consumer Protection also has general powers to investigate and regulate consumer fraud and deceptive trade practices (Del. Code tit. 29, § 2517).

B. Other Regulators

The Delaware Department of Health and Social Services has the authority to impose sanctions against certain health care facilities for violations of certain provisions related to disclosure of, or access to, patient information (see Section II.C.).

The Delaware Insurance Commissioner may impose sanctions and fines on certain dental plan organizations and managed care organizations (see Section II.C.).

The Delaware Department of Labor may sanction employers who violate provisions regarding the disclosure of genetic information about an employee (see Section II.C.).

C. SANCTIONS & FINES

The Attorney General may bring an action in law or equity to address violations of the Computer Security Breaches Law (see Section I.C.8.), to recover direct economic damages, or both (Del. Code tit. 6, § 12B-104). It should be noted, however, that the Computer Security Breaches Law does not provide for a private cause of action to enforce its provisions.

The Division of Consumer Protection of the Department of Justice may investigate and prosecute violations of the Delaware Online Privacy and Protection Act (DOPPA), but specific sanctions or fines are not specified (Del. Code tit. 6, § 1203C).

The Division of Consumer Protection of the Department of Justice may investigate and prosecute violations of the Student Data Privacy Protection Act (SDPPA), but specific sanctions or fines are not specified (Del. Code tit. 14, § 8103A).

An employer who refuses an employee access to personnel files in violation of Labor Law requirements (see Section I.E.6.) is subject to a civil penalty of from $1,000 to $5,000 per violation. The same civil penalties apply to an employer who discharges or discriminates against an employee because the employee has made a complaint, given information to the Department of Labor, caused a proceeding to be instituted, or testified in such a proceeding (Del. Code tit. 19, § 735).

A nursing facility employer who hires an applicant prior to conducting a criminal background check or who hires an applicant on a conditional basis without verifying that the applicant has been fingerprinted is subject to a civil fine of not less than $1,000 and not more than $5,000 (see Section I.D.5.) (Del. Code tit. 16, § 1141(f)). Applicants who fail to provide the proper information for such a check are subject to the same civil fines (Del. Code tit. 16, § 1141(j)). The same penalty provisions apply to home health employers and applicants (Del. Code tit. 16, § 1145(g) and (k)).

The Delaware Department of Health and Social Services may impose a civil penalty of up to $5,000 per violation for a nursing facility that improperly discloses health information of a patient or resident or that fails to provide access to records (Del. Code tit. 16, § 1109(c)). Each day of continuing violation is considered a separate violation subject to a maximum fine of $1,250 per day (Del. Code tit. 16, § 1109(e)).

Persons violating the provisions prohibiting the collection, retention, or disclosure of genetic information (see Section I.D.9.) are subject to fines as follows: for willfully retaining an individual's genetic information or sample, a fine of not less than $1,000 nor more than $10,000; and for willfully obtaining or disclosing genetic information, a fine of not less than $5,000 nor more than $50,000. Persons who unlawfully disclose an individual's genetic information also are liable to the victim for actual damages, including damages for economic, bodily, or emotional harm. Jurisdiction for violations lies in the Superior Court (Del. Code tit. 16, § 1208).

When a dental plan organization violates the prohibition on releasing health data about an enrollee, the Delaware Insurance Commissioner may subject the organization to suspension or revocation of its certificate of authority (Del. Code tit. 18, § 3815) or a cease-and-desist order (Del.

Code tit. 18, § 3816). In addition, such organizations are subject to a civil fine of no more than $1,000 per violation (Del. Code tit. 18, § 3817). With respect to the provision prohibiting similar disclosures by managed care organizations, the Insurance Commissioner may issue a cease-and-desist order and may impose a civil penalty of not less than $250 and not more than $10,000 for each day of violation. The Commissioner must give 10 days' notice of the levy, and the organization has 30 days to remedy the situation. In addition, the organization has the right to appeal under conditions specified in the law (Del. Code tit. 18, § 6419).

With respect to an employer violation regarding the disclosure of genetic information about an employee (see Section I.D.9.), the Department of Labor has the authority to sanction the employer under general rules governing unfair labor practices, including the commencement of a civil action (Del. Code tit. 19, § 712). In addition, the Attorney General may bring an action in the Court of Chancery if it finds that the violation denied the individual the full exercise of his employment rights (Del. Code tit. 19, § 713). Additionally, a charging party may file a civil action in Superior Court, after exhausting the administrative remedies provided herein and receipt of a Delaware Right to Sue Notice (Del. Code tit. 19, § 714).

D. Representative Enforcement Actions

There do not appear to be any specific enforcement actions that have been brought by the Division of Consumer Protection of Delaware's Department of Justice related to Delaware privacy and data security laws.

E. State Resources

The Attorney General's Division of Consumer Protection provides a form that consumers may use to apply for an identity theft passport (see Section I.G.2.). It also provides an online Consumer Complaint Form that consumers can use to alert the Division to a violation of a consumer protection law. In addition, the Division provides information on identity theft protection.

III. RISK ENVIRONMENT

To date, the Attorney General has not been aggressive in enforcing laws in Delaware regarding privacy and data security. However, the Attorney General's office, through its Director of Consumer Protection, has been involved in a significant number of multi-state investigations, such as the investigation into the Target Corporation data breach and most recently into the Equifax data breach. Typically, the multi-state investigations result in a lawsuit filed in one or more courts and ultimately a settlement. The current Computer Data Breaches Law does not provide significant enforcement authority, but the revised law effective April 14, 2018, increases obligations on businesses to maintain reasonable data security, and thus gives the Director of Consumer Protection significantly increased enforcement options. In addition, the Director of Consumer Protection has inherent power under Del. Code tit. 29, § 2517 to prohibit deceptive or fraudulent conduct. Through this authority, the Attorney General can enforce provisions of the Delaware Online Privacy and Protection Act (DOPPA), the Student Data Privacy Protection Act (SDPPA), and the Computer Security Breaches Law.

The Delaware Department of Justice's Division of Consumer Protection generally has been a complaint-driven office. The Division provides a form online for consumers to file complaints. In the future, we believe that the Division intends to become more proactive in light of the significant new

privacy and data security legislation discussed herein. We suspect that enforcement of the new data security requirements, Del. Code tit. 6, § 12B-100, will be challenging, as the statute does not spell out what security practices are "reasonable." The Director of Consumer Protection is likely to consider the facts and circumstances of every case and look to guidelines developing in other states, such as the guidelines promulgated by the New York Division of Financial Services, for guidance.

Other agencies in Delaware—for example, the Insurance Department, the Department of Health and Social Services (DHSS), and the Department of Labor—have jurisdiction to investigate and enforce privacy and data security-related violations. Similarly with the Department of Justice, these departments tend to be complaint-driven. For example, the Long Term Care Residents Protection Division of DHSS has three main sections: long term care licensing, acute and outpatient care licensing, and investigation. A consumer complaint could initiate an investigation by the investigation unit. Also, issues that arise during a license review, such as evidence of an unauthorized release of records, could result in an investigation initiated by either of the licensing units. While we are not aware of any specific, stand-alone enforcement actions, privacy-related compliance issues have been the subject of investigation when a Department either conducts a statutory investigation or responds to an unrelated complaint.

We are not aware of any privacy-related class actions having been filed in Delaware based on a violation of Delaware law. However, because many business entities are incorporated in Delaware, class action litigation involving federal and other state law is commonplace. One such example is *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, No. 1:12-md-02358 (D. Del.), a consolidated class action in which the court approved a $5.5 million settlement on February 2, 2017. See 2017 BL 32259. That action involved, *inter alia*, alleged privacy violations based on Google's claimed circumvention of cookie-blocking settings on users' Internet Explorer and Apple Safari web browsers.

For such actions, or any claims brought based on Delaware law in federal court, Delaware's federal courts would follow Third Circuit precedent on matters relating to the determination of Article III standing to pursue a claim. The Third Circuit appears to have adopted an expansive view of Article III standing, ruling in *Susinno v. Work Out World, Inc.*, 862 F.3d 346 (3d Cir 2017), that allegations that a customer who received a single, unauthorized prerecorded sales voice mail call on her cell phone in violation of the Telephone Consumer Protection Act established a concrete injury sufficient to confer Article III standing. Thus, Delaware could become an attractive forum for privacy class actions.

Persons doing business in Delaware would be well advised to understand, monitor, and comply with a number of Delaware laws to reduce the potential for enforcement actions and litigation and their related costs and liabilities. This is particularly so for businesses that may not have a physical presence in Delaware, and therefore may be less familiar with Delaware's laws, but nevertheless conduct business in Delaware with Delaware residents (see DOPPA, Section I.B.2., and Computer Security Breaches Law, Section I.B.2.). Although many of these laws do not currently provide private rights of action, they do contain robust enforcement mechanisms, both civil and criminal, for Delaware to utilize in the event of a violation.

Compliance with these laws should not be overly burdensome, as the laws were drafted with the purpose of balancing practical adherence with protection of Delaware residents. However, businesses should carefully review their internal policies and procedures to ensure that they maintain compliance with Delaware's privacy laws.

Although the Delaware Department of Justice has not aggressively pursued privacy-related enforcement actions in the past, the suite of privacy laws enacted in 2015 (DOPPA, SDPPA, etc.) coupled with the recent amendment to the Computer Security Breaches Law indicate that the enforcement priorities within the Attorney General's office are shifting toward this area. Delaware's new requirement to provide credit monitoring in the event of a breach of security involving Social Security numbers, one of only two states to have such a requirement, demonstrates Delaware's resolve to protect its residents. Given this new focus, individuals and entities should closely monitor future developments in both the enforcement and development of these laws to ensure compliance and reduce the risk of liability.

IV. EMERGING ISSUES AND OUTLOOK

A. Recent Legislation

1. Data Breach Notification

On August 17, 2017, Delaware's Governor Carney signed legislation to update Delaware's Computer Security Breaches Law by, among other things, specifically requiring businesses to safeguard personal information and expanding the definition of personal information to include biometric data, usernames together with passwords, routing numbers to accounts, taxpayer ID numbers, health insurance identifiers, passport numbers, and medical information. The new law is effective April 14, 2018. 81 Del. Laws ch. 129.

Under the new law, persons who conduct business in Delaware and who own, license, or maintain personal information will be obligated to implement and maintain reasonable procedures and practices to prevent the unauthorized acquisition, use, modification, disclosure, or destruction of personal information collected or maintained in the regular course of business (Del. Code tit. 6, § 12B-100). It is likely that enforcement authorities in Delaware will look to guidelines issued by other states and by various industry groups to determine what data security procedures and practices are "reasonable."

In addition, the revised version strengthens the law's notice requirements by requiring notice within 60 days whenever personal information is, or reasonably believed to have been, breached unless an investigation determines specifically that the breach is unlikely to result in harm (see Section I.B.2.). For a discussion regarding the substantive revisions to the Computer Security Breaches Law, see Section I.B.2. and Section I.B.3.

2. Health Information

On July 21, 2017, Governor Carney signed legislation that grants access to data from the prescription monitoring program to the Drug Overdose Fatality Review Commission, which significantly enhances the Commission's ability to meet its statutory duties. Section 1 of the Act clarifies the scope of records that may be compelled for production by the Commission. Sections 2 and 3 of the Act allow the Drug Overdose Fatality Review Commission to obtain and review medical records, including mental health and substance abuse records, in furtherance of its statutory duties and in compliance with Delaware's privacy and confidentiality laws. 81 Del. Laws ch. 94.

B. Proposed Legislation

1. Educational Privacy

HB 72, introduced Mar. 9, 2017, would remove the broad exemption that the University of Delaware and Delaware State University currently receive under the state Freedom of Information Act. In recognition of the sensitive nature of some records held by public universities, this Act would also add some specific exemptions for public universities. Specifically, confidential letters or statements related to admission, employment or honors would not be a public record for purposes of FOIA. Universities would not be required to disclose scholarly research or information related thereto where such information is of a proprietary nature. Finally, certain information related to fundraising activities would be protected from disclosure. Delaware's FOIA, as currently written, already exempts personally identifiable student information protected by the federal Family Educational Rights and Privacy Act (FERPA).

C. Other Issues

1. Equifax Breach

In September 2017, Delaware Attorney General Matt Denn joined 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.