Bloomberg Law®

Domestic Privacy Profile: New York

Prepared in cooperation with

Craig A. Newman

Partner, Patterson Belknap Webb & Tyler LLP, New York

Bloomberg Law
Privacy & Data Security

Domestic Privacy Profile: NEW YORK

Craig A. Newman, a partner with Patterson Belknap Webb & Tyler LLP in New York, provided expert review of the New York Profile and wrote the Risk Environment section. He gratefully acknowledges the assistance of George S. Soussou, an associate at the firm. [Last updated May 2018. – Ed.]

TABLE OF CONTENTS

I. APPLICABLE LAWS AND REGULATIONS

A. CONSTITUTIONAL PROVISIONS

Article I, § 1 of the New York State Constitution provides that no member of the state may be deprived of any right or privilege secured to any citizen, unless by law or the judgment of his or her peers. However, the Constitution does not contain an explicit provision regarding the privacy rights of individuals.

B. PERSONAL DATA PROTECTION PROVISIONS

1. Who is covered?

The Information Security Breach and Notification Act (Breach Statute), N.Y. Gen. Bus. Law § 899-AA, is the primary legislation governing the obligations of businesses to notify "any resident of New York state whose private information was, or is reasonably believed to have been, acquired by a person without authorization."

The Personal Privacy Protection Law (PPPL), N.Y. Pub. Off. Law § 91 et seq., also imposes specific obligations on New York state agencies regarding the collection, disclosure, use, and maintenance of personal information of a "data subject." A data subject is defined as "any natural person about whom personal information has been collected by an agency" and is not expressly limited to residents of New York state. N.Y. Pub. Off. Law § 92(3).

In addition, the Internet Security and Privacy Act, N.Y. State Tech. § 201 et seq., supplements both the Breach Statute and the PPPL. It requires state agencies that maintain an internet website to adopt an internet privacy policy and to provide a user access to his or her personal information (N.Y. State Tech. § 205). It requires that such agencies notify "any resident of New York state" (N.Y. State Tech. § 208(2)) of any breach of their private information as required under the Breach Statute.

2. What is covered?

The Information Security Breach and Notification Act (Breach Statute), N.Y. Gen. Bus. Law § 899-AA, applies to breaches of private information. "Private information" includes personal information (information that can be used to identify a natural person) consisting of any information in combination with a specified data element (social security number; driver's license or identification

card number; or account number, debit card number, or credit card number) where the information is not encrypted or when the data key to encrypted information has been acquired (N.Y. Gen. Bus. Law § 899-AA(1)(b)).

The Personal Privacy Protection Law (PPPL), N.Y. Pub. Off. Law § 91 et seq., applies to any personal information possessed by a state agency. "Personal information" includes any information concerning a data subject that–because of name, number, symbol, marker, or other identifier–can be used to identify a data subject (N.Y. Pub. Off. Law § 92(7)). An agency is not required to provide a data subject with access to a record if "the agency does not have the possession of such record." The PPPL does not separately define the term private information as the Breach Statute does.

The Internet Security and Privacy Act covers personal information (defined similarly to the PPPL) that is collected through the use of a state agency website (N.Y. State Tech. § 202, § 204).

3. Who must comply?

The Information Security Breach and Notification Act is applicable to all persons or businesses conducting business in New York that own or license computerized data that includes private information (N.Y. Gen. Bus. Law § 899-AA(2)). For more information, see Section I.C.8.

Both the Personal Privacy Protection Law and the Internet Security and Privacy Act apply to all state agencies. "Agency" is defined as a governmental entity that performs a governmental function of the state, but does not include the courts, the state legislature, or any unit of local government (N.Y. Pub. Off. Law § 92(1); N.Y. State Tech. § 202(6)).

C. Data Management Provisions

1. Notice & Consent

The Personal Privacy Protection Law requires all agencies to provide notice to all individuals from whom they request information to be maintained in a record, at the time of the initial request. The notice must include the authority under which the agency is collecting the information, the impact on the individual of not providing such information, the purpose of the collection, and the uses that may be made of the information (N.Y. Pub. Off. Law § 94(1)(d)).

No agency may disclose any record or personal information unless it is pursuant to a written request by, or the voluntary consent of, the data subject. The request or consent must specify the specific personal information to be disclosed, the person or entity to which it will be disclosed, and the uses to which that person or entity will put the information (N.Y. Pub. Off. Law § 96(1)(a)). The statute provides for a number of exceptions to the consent requirement (see Section I.C.3.).

The Internet Security and Privacy Act provides that consent of the user of a state website is required before a state agency may disclose personal information about the user to any third party. The voluntary disclosure of information by a user to a state agency website, whether solicited or unsolicited, constitutes consent to the collection or disclosure of the information by the state agency for the purposes for which the user disclosed the information (N.Y. State Tech. § 204). The Internet Security and Privacy Act also requires state agencies to comply with data breach notification provisions that are substantially identical to those contained in the Information Security Breach and Notification Act. (N.Y. State Tech. § 208; see Section I.C.8.).

2. Collection & Use

The Personal Privacy Protection Law requires state agencies to collect personal data only from the data subjects themselves whenever practicable, unless the information is collected for purposes of making a quasi-judicial judgment (N.Y. Pub. Off. Law § 94(1)(c)). An agency may only maintain such personal information that is relevant and necessary to accomplish a purpose of the agency that is

required or to implement a program authorized by law, unless the data subject "provides an agency with unsolicited personal information." (N.Y. Pub. Off. Law § 94(1)(a)). The agency shall "maintain all records used by the agency to make any determination about any data subject with accuracy, relevance, timeliness, and completeness provided however, that personal information or records received by an agency from another governmental unit for inclusion in public safety agency records shall be presumed to be accurate." (N.Y. Pub. Off. Law § 94(b)).

The Internet Security and Privacy Act provides that no state agency may collect personal information concerning a user through an agency website unless the user has consented to the collection (N.Y. State Tech. § 204). Certain exceptions are provided, including where the collection is necessary to perform state agency duties, is made pursuant to a court order or by law, is for the purpose of validating the identity of the user, or is used solely for statistical purposes and is in a form that cannot be used to identify the user (N.Y. State Tech. § 206).

3. Disclosure to Third Parties

The Personal Privacy Protection Law (PPPL), N.Y. Pub. Off. Law § 91 et seq., prohibits state agencies from disclosing personal information of individuals except through written request or written consent of the data subject (see Section I.C.1.), or if one of the following circumstances are present:

- Disclosure to an official, employee, or contractor of the agency that is necessary in the performance of that person's lawful agency duties;
- Disclosures under the state's Freedom of Information Law;
- Disclosures to other government agencies under specified circumstances;
- Disclosures for a "routine use";
- Disclosures specifically authorized by statute or federal rule or regulation;
- Disclosures to the U.S. Census Bureau;
- Disclosures solely for statistical research (provided that the record is transferred in a form that is not personally identifiable);
- Disclosures to the state archives;
- Disclosures required by a legal process such as a subpoena;
- Disclosure for inclusion in law enforcement records (but such information may only be used for a law enforcement function);
- Disclosure pursuant to a search warrant; and
- Disclosure pursuant to an executive order if the records are to be used solely for research purposes (N.Y. Pub. Off. Law § 96(1)(b)-(o)).

Generally, "except for disclosures made for inclusion in public safety agency records when such record is requested for the purpose of obtaining information required for the investigation of a violation of civil or criminal statutes within the disclosing agency," agencies must maintain an accounting of disclosures as part of the agency's records. The accounting for such disclosures must include the date, nature, and purpose of the disclosure and the recipient of the information (N.Y. Pub. Off. Law § 94(3)(i)(a)).

The Internet Security and Privacy Act specifies that personal information about a user of the agency website may not be disclosed to any third party without the consent of the user (N.Y. State Tech. § 204). Certain exceptions are provided, including where the disclosure is necessary to perform state agency duties, is made pursuant to a court order or by law, is for the purpose of identifying the user, or is used solely for statistical purposes and is in a form that cannot be used to identify the user (N.Y. State Tech. § 206).

4. Data Storage

The Personal Privacy Protection Law requires state agencies to maintain all records containing personal information with accuracy, relevancy, timeliness, and completeness (N.Y. Pub. Off. Law § 94(1)(b)). In addition, agencies must ensure that no record is modified or destroyed to avoid the requirements of the privacy law (N.Y. Pub. Off. Law § 94(1)(e)). Agencies are required to establish written policies governing the responsibilities of any person involved in the design, development, operation, or maintenance of any records system, outlining the requirements of the privacy law and the penalties for noncompliance (N.Y. Pub. Off. Law § 94(1)(g)).

5. Access & Correction

Within five business days of receipt of a written request from a data subject that reasonably describes the record being sought, state agencies must provide access to such records, provide a written statement of partial or complete denial of the request along with the reasons for the denial, or provide a written acknowledgment of receipt of the request with an approximate date on which the request will be granted or denied, which may not exceed 30 business days from receipt of the request (N.Y. Pub. Off. Law § 95(1)(a)). The agency is not required to provide access if it does not have the requested record, if the request is insufficiently specific, or if another exception to access applies (N.Y. Pub. Off. Law § 95(1)(b); see also N.Y. Pub. Off. Law § 95(6)-(7)) (providing additional exceptions).

Within 30 business days of receipt of a written request for a correction or amendment of a record, a state agency must either make the correction or inform the data subject of its reasons for refusing to do so (N.Y. Pub. Off. Law § 95(2)). If an access or correction request is denied, the data subject has 30 business days to appeal the decision in writing to the head of the agency. The agency head has seven business days from the receipt of an access denial appeal, or 30 business days from receipt of a correction denial appeal, to approve access or correction or to explain the factual and statutory reasons for continued denial and the data subject's judicial appeal rights (N.Y. Pub. Off. Law § 95(3)). The data subject may file a statement of disagreement with the agency's decision to deny correction that will be provided to any third party to whom a record is disclosed (N.Y. Pub. Off. Law § 95(4)).

When a data subject is entitled to access to personal information, agencies are required to disclose any record to which a data subject has requested access at a location near the residence of the data subject or by mail (N.Y. Pub. Off. Law § 94(1)(k)). In addition, agencies must develop procedures for verifying the identity of data subjects requesting access to personal information, for providing access, and in reviewing requests for access or correction and appeals of adverse determinations (N.Y. Pub. Off. Law § 94(2)).

The Internet Security and Privacy Act provides that state agencies must provide a user with access to his or her personal information collected through its state website. The access and correction requirements from the PPPL described above are incorporated by reference (N.Y. State Tech. § 205).

6. Data Security

The Personal Privacy Protection Law requires state agencies to "establish appropriate administrative, technical, and physical safeguards to ensure the security of records." (N.Y. Pub. Off. Law § 94(1)(h)).

7. Data Disposal

N.Y. Gen. Bus. Law § 399-H provides that no person or business entity, not inclusive of the state or its political subdivisions, "shall dispose of a record containing personal identifying information" unless the entity: "a) shreds the record before the disposal of the record; or b) destroys the

personally identifying information contained in the record; or, c) modifies the record to make the personally identifying information unreadable; or d) takes actions consistent with commonly accepted industry practices that it reasonably believes will ensure that no unauthorized person will have access to the personal identifying information contained in the record." § 399-H(2).

The Personal Privacy Protection Law requires state agencies to establish rules governing retention and timely disposal of covered records (N.Y. Pub. Off. Law § 94(1)(i)).

8. Data Breach

The Information Security Breach and Notification Act (Breach Statute), N.Y. Gen. Bus. Law § 899-AA, requires New York businesses that own or license computerized data that includes private information to notify affected New York residents following the discovery of a breach of security in their computer data systems. The Breach Statute does not define the term "computerized data." The notification must be made in the most expedient time possible, consistent with legitimate law enforcement needs or any measure necessary to determine the scope of the breach and restore system integrity (N.Y. Gen. Bus. Law § 899-AA(2)). Businesses that maintain computerized data but do not own it must inform the owner or licensee of the data if they discover such a breach (N.Y. Gen. Bus. Law § 899-AA(3)). The notification may be delayed if it will impede a criminal investigation, but notification must be made after law enforcement determines that the investigation would no longer be compromised (N.Y. Gen. Bus. Law § 899-AA(4)). The notice must include contact information for the business providing the notice and a description of the categories of information compromised and the elements of personal and private information that were, or are reasonably believed to have been, improperly acquired (N.Y. Gen. Bus. Law § 899-AA(7)).

The breach notification generally must be made by written notice, electronic notice (provided that the person to whom notice is required has consented to electronic notice and a log of such notices is maintained), or telephone notice (with a log maintained). Substitute notice is permitted if the business can show the attorney general that the cost of notice would exceed $250,000, that the class of persons to be notified exceeds 500,000 people, or that the business does not have sufficient contact information. Acceptable methods of substitute notice include notice via e-mail, conspicuous posting of the notice on the business's website, and notification to major statewide media (N.Y. Gen. Bus. Law § 899-AA(5)).

In addition to notifying New York residents of the breach, businesses are required to notify the state attorney general, the New York Department of State, and the Division of State Police with respect to the timing, content, and distribution of breach notifications and the approximate number of residents affected. In addition, if the business is notifying more than 5,000 residents at a time, it must notify consumer reporting agencies regarding the timing and number of residents (N.Y. Gen. Bus. Law § 899-AA(8)).

If the attorney general's office finds that the breach notification law has been violated, it may bring an action, within two years of the date of the act complained of or the discovery of the act, on behalf of the people of the state to enjoin the continued violation of the law. In such an action, a court may provide for preliminary relief and may award damages to individuals for actual costs and losses suffered as a result of the violation. Civil penalties also may be imposed (N.Y. Gen. Bus. Law § 899-AA(6)) (see Section I.G.1.). The statute is silent as to whether there is a private right of action. However, in *Abdale v. North Shore-Long Island Jewish Health System Inc.,* 49 Misc. 3d 1027, 1036-37, 19 N.Y.S.3d 850, 857-58 (N.Y. Sup. Ct. Aug. 14, 2015), the Court dismissed a complaint because there is not a private right of action in the statute.

The Internet Security and Privacy Act has data breach notification provisions that are applicable to state agencies owning or licensing computerized data containing private information and that are

substantially identical to those described above, except for the civil action provisions (N.Y. State Tech. § 208).

9. Cloud Computing

At present, there are no New York provisions specifically applicable to cloud computing.

10. Other Provisions

The Internet Security and Privacy Act provides that the State Office of Information Technology Services must adopt a model privacy policy for state agencies that maintain agency websites. The elements of the policy are specified by statute and include items such as the information the agency will collect, whether the agency will retain the information, access and correction procedures, whether collection is required or voluntary, and the steps the agency will take to ensure confidentiality (N.Y. State Tech. § 203).

D. Specific Types of Data

1. Biometric Data

N.Y. Lab. Law § 201-A prohibits employers, except as otherwise provided by law, from requiring the fingerprinting of employees as a condition of obtaining or continuing employment. This provision does not apply to state or municipal employees, employees of public hospitals or of medical colleges affiliated with such hospitals, or employees of private proprietary hospitals.

N.Y. Civ. Rights Law § 79-L places a variety of restrictions on the performance of genetic tests on biological samples without the prior written consent of the individual. Informed consent must, among other requirements, include the name of the persons or categories of organizations to which test results may be disclosed. Records, findings, and results of an individual's test are confidential and may not be disclosed without written informed consent, although certain exceptions (*i.e.*, court order or other provisions of law) apply. Similar provisions apply to genetic tests specifically conducted by insurers (N.Y. Ins. Law § 2615).

2. Consumer Data

N.Y. Gen. Bus. Law § 399-DD provides that no person or business entity may knowingly and intentionally procure, sell, or fraudulently transfer or use telephone record information from a telephone company without written authorization from the telephone customer to whom the record relates. This prohibition does not apply to actions pursuant to a subpoena or by law enforcement.

3. Credit Card Data

Credit and debit card numbers, together with any required security code or access code that would allow access to an individual's financial account, are defined as "private information" subject to the Information Security Breach and Notification Act (N.Y. Gen. Bus. Law § 899-AA), which requires New York businesses that own or license computerized data that includes such information to notify affected New York residents following the discovery of a breach in security in their computer data systems (N.Y. Gen. Bus. Law § 899-AA(1)(b)(3)). See Section I.C.8.

4. Credit Reports

Under the New York Fair Credit Reporting Act, consumer reporting agencies may furnish a credit report in connection with a credit transaction, for employment purposes, in connection with insurance underwriting, or where the requester has a legitimate business need for such a report, (N.Y. Gen. Bus. Law § 380-B(a)), but no such request may be made with respect to an application for credit, employment, insurance, or rental or lease of a residence unless the applicant is informed

in writing that the report may be requested. If a report is requested, the requestor must inform the applicant of the name and address of the agency providing the report (N.Y. Gen. Bus. Law § 380-B(b)).

Under N.Y.C. Admin. Code § 8-107(24), an employer, labor organization, or state agency may not request, or use for employment purposes, the consumer credit history of an applicant or employee. This prohibition does not apply to employers required by law or regulation to use a credit history for employment purposes, or to persons who are applying for a position meeting one of the following requirements: (1) a position as a peace officer or police officer; (2) a position that is subject to background investigation (but the employer may only use the credit history information if the position is one in which a high degree of public trust has been reposed); (3) a position required to be bonded; (4) a position requiring security clearance; (5) a non-clerical position having regular access to trade secrets, intelligence information, or national security information; or (6) a position having signatory authority over third-party funds or assets or fiduciary authority to enter into financial agreements exceeding $10,000. In addition, the prohibition does not affect persons required to disclose certain information regarding their creditors or debts to the conflicts of interest board.

5. Criminal Records

N.Y. Exec. Law § 296(16) prohibits, unless specifically required or permitted by statute, any person, including a state agency, to make an inquiry–in connection with an individual's licensing or employment, or the provision of credit or insurance to the individual–about any arrest or criminal accusation of an individual that is not currently pending against the individual, that has been resolved in the individual's favor or by a youthful offender adjudication, or that has resulted in a sealed conviction. N.Y.C. Admin. Code § 8-107 (11-b) incorporates this prohibition for purposes of the New York City Human Rights Law.

In addition to the limitation described above, N.Y.C. Admin. Code § 8-107 (11-a)(a)(3) prohibits employers from making any inquiry related to the pending arrest or criminal conviction record of an applicant until after the employer has extended a conditional offer to the applicant. After making a conditional offer, an employer may inquire about the applicant's arrest or conviction record if it provides a written copy of the inquiry to the individual, performs the inquiry pursuant to Article 23-A of the New York Corrections Law, provides a copy of the analysis to the applicant (including any reasons for adverse action based on the analysis if applicable), and gives the applicant three business days to respond to the analysis (N.Y.C. Admin. Code § 8-107 (11-a)(b)). The prohibition does not apply to actions taken by employers with respect to federal, state, or local laws requiring criminal background checks or barring employment based on criminal history, or to actions taken with respect to applications for employment as a peace officer or other specified positions (N.Y.C. Admin. Code § 8-107 (11-a)(e)-(f)). The provisions described above are applicable to public agencies as well as private employers (N.Y.C. Admin. Code § 8-107 (11-a)(g)).

6. Drivers' Licenses/Motor Vehicle Records

Driver's license numbers and non-driver identification card numbers are defined as "private information" subject to the Information Security Breach and Notification Act (N.Y. Gen. Bus. Law § 899-AA), which requires New York businesses that own or license computerized data that includes such information to notify affected New York residents following the discovery of a breach in security in their computer data systems (N.Y. Gen. Bus. Law § 899-AA(1)(b)(2)). See Section I.C.8.

N.Y. Lab. Law § 203-D prohibits employers from communicating an employee's personal identifying information to the general public. The law's definition of personal identifying information includes an employee's driver's license number.

New York adheres to the provisions of the federal Driver's Privacy Protection Act, 18 U.S.C. § 2721. More information is available on the New York Department of Motor Vehicles website.

7. Electronic Communications/Social Media Accounts

N.Y. Penal § 250.05 prohibits any person from unlawfully engaging in wiretapping, mechanical overhearing of a conversation, or intercepting or accessing an electronic communication. New York law does not prohibit employers from viewing an applicant's public social media information, but such accounts may contain personal information that may not be considered by an employer in making a hiring decision.

Bills have been introduced in the New York Assembly and Senate that would expand privacy protections afforded to information contained in social media accounts and that would, among other items, prohibit employers from requiring an employee to provide access to his personal e-mail or social media accounts (see Section IV).

8. Financial Information

On March 1, 2017, the New York State Department of Financial Services (DFS) issued a regulation (23 NYCRR 500.00 et seq.) setting forth cybersecurity requirements applicable to entities in the state covered by the Financial Services Law or "similar authorization." The regulatory requirements are applicable to financial data that qualifies as nonpublic information under the regulation. The cybersecurity regulation is discussed in detail at Section I.E.4.

Insurance regulations also provide a variety of requirements that companies licensed under the New York Insurance Law must meet with respect to the privacy of consumer financial information (11 NYCRR 420.0 et seq.). The regulations require licensees to provide a notice to consumers and customers concerning their privacy policies and the individual's right to opt out (11 NYCRR 420.4-420.9), and describe the limits on disclosure of financial information (11 NYCRR 420.10-420.12) and the exceptions to these limits on disclosure (11 NYCRR 420.13-420.16).

9. Health Data

Insurance companies that maintain health data that qualifies as nonpublic information are also subject to the regulation issued on March 1, 2017, by the Department of Financial Services (DFS) setting forth cybersecurity requirements applicable to entities in the state covered by the Insurance Law (23 NYCRR 500.00-500.23). For a comprehensive discussion of the regulation, see Section I.E.4.

In addition, insurance companies required to be licensed under the New York Insurance Law are subject to regulatory requirements regarding the privacy of consumer and customer health information (11 NYCRR 420.17-420.21). See Section I.E.7.

For provisions applicable to the health care sector, see Section I.E.5.

10. Social Security Numbers

N.Y. Gen. Bus. Code § 399-DDD (first version) provides that no person or business entity may intentionally disclose any individual's social security number (SSN), print an individual's SSN on any identification card or tag, require an individual to transmit his SSN over the Internet unless the connection is secure or the number is encrypted, or require an individual to use his SSN to access an Internet website, "unless a password or unique personal identification number or other authentication device is also required to access the internet website." Although the term "secure" is not defined in the statute, it is commonly defined in the industry as "a connection that is encrypted by one or more security protocols to ensure the security of data flowing between two or more nodes." In addition, they may not include an individual's SSN on any materials mailed to the individual, except if required by state or federal law, and may not embed or encode an SSN on a

card through the use of a bar code, magnetic strip, or other technology in place of removing the SSN as otherwise required. A person or business entity having possession of an SSN for purposes of conducting business or trade must take reasonable measures to ensure that no officer or employee has access to SSN information for any non-legitimate or necessary purpose and must provide appropriate safeguards to protect confidentiality.

N.Y. Gen. Bus. Code § 399-DDD (second version) augments the provisions above by prohibiting any person or business entity from requiring an individual to disclose his SSN or refusing any service, privilege, or right of an individual based on the refusal to disclose an SSN. However, a number of exceptions apply, including if an individual consents to the acquisition and use of an SSN; the SSN is required by federal, state, or local law; the SSN is to be used for internal verification or fraud investigation; or the SSN is required for specified employment purposes, among other items (N.Y. Gen. Bus. Code § 399-DDD.3(a)-(m), second version).

Social security numbers are defined as "private information" subject to the Information Security Breach and Notification Act (N.Y. Gen. Bus. Law § 899-AA), which requires New York businesses that own or license computerized data that includes such information to notify affected New York residents following the discovery of a breach in security in their computer data systems (N.Y. Gen. Bus. Law § 899-AA(1)(b)(1)). See Section I.C.8.

The Personal Privacy Protection Law, N.Y. Pub. Off. Law § 91 et seq., specifically prohibits New York State and its political subdivisions from intentionally disclosing any individual's SSN, printing an individual's SSN on any identification card or tag, requiring an individual to transmit his SSN over the Internet unless the connection is secure or the number is encrypted, or requiring an individual to use his SSN to access an Internet website, unless a password or unique personal identification number or other authentication device is also required to access the internet website. In addition, they may not include an individual's SSN, save for the last four digits, on any materials mailed to the individual or on any e-mail material, except if required by federal law, and may not embed or encode an SSN on a card through the use of a bar code, magnetic strip, or other technology in place of removing the SSN as otherwise required (N.Y. Pub. Off. Law § 96-A(1)(a)-(d)).

N.Y. Lab. Law § 203-D prohibits employers from publicly posting or displaying an employee's SSN, visibly printing an SSN on any identification card or badge (including time cards), or placing an SSN in files with unrestricted access. In addition, an SSN may not be used as an identification number for occupational licensing purposes.

11. Usernames & Passwords

Bills have been introduced in the New York Assembly and Senate that would expand privacy protections afforded to information contained in social media accounts and that would, among other items, prohibit employers from requiring an employee to provide access to his personal e-mail or social media accounts (see Section IV., below).

12. Information about Minors

N.Y. Pub. Health Law § 18.3(c) (first version) provides that a subject over the age of 12 may be notified of the request of any qualified person (such as a parent or legal guardian) to review his patient information, and if the subject objects to the disclosure, the provider may deny the request for access.

N.Y. Pub. Health Law § 2782.4(e) allows physicians to disclose confidential HIV information about a protected individual to a person (including a parent or guardian of a minor) known to the physician to be authorized to consent to health care for the individual under most circumstances, but does not allow physicians to disclose such information if, in the judgment of the physician, the disclosure would not be in the best interest of the protected individual.

13. Location Data

N.Y. Penal § 120.45, which relates to the crime of stalking, defines "following" someone as including "the unauthorized tracking of such person's movements or location through the use of a global positioning system or other device."

N.Y. Gen. Bus. Law § 396-Z(13-a) prohibits a vehicle rental company from using "information from any global positioning system technology to determine or impose any costs, fees, charges, or penalties on an authorized driver for such driver's use of a rental vehicle." However, the use of GPS technology "shall not limit the right of a rental vehicle company to impose costs, fees, charges, or penalties to recover a vehicle that is lost, misplaced, or stolen."

14. Other Personal Data

Our research has uncovered no other New York law provisions regarding personal data beyond those specified above.

E. Sector-Specific Provisions

1. Advertising & Marketing

N.Y. Gen. Bus. Law § 399-PP prohibits deceptive telemarketing practices by entities registered by the state. Telemarketers must provide specified information in the course of the call, including the purpose of the call, the telemarketer's name and the person on whose behalf the solicitation is being made, the identity and cost of the goods or service offered, and, in the case of a prize promotion, the odds of receiving a prize (N.Y. Gen. Bus. Law § 399-PP.6.b).

N.Y. Gen. Bus. Law § 399-Z permits the New York Department of State to establish a "do-not-call" list or to use the national "do-not-call" registry for this purpose. The law further prohibits any telemarketer from calling any customer whose name has been on the national list for a period of 31 days before the call is made (N.Y. Gen. Bus. Law § 399-ZZ (5)).

2. Education

N.Y. Educ. Law § 2-D requires all school districts and other educational agencies to develop a parent's bill of rights for posting on the agency website stating that a student's personally identifiable information cannot be sold or released for commercial purposes, and that parents have the right to inspect education records and to have any complaints about potential breaches of student data addressed. The law also covers requirements for data collection and security standards. More information on the parent's bill of rights is available at the New York State Education Department website.

3. Electronic Commerce

The New York Electronic Signatures and Records Act (N.Y. State Tech. § 301 through N.Y. State Tech. § 309) provides that electronic signatures are legally binding (N.Y. State Tech. § 304), and designates the Office of Information Technology Services as the electronic facilitator responsible for implementing its provisions (N.Y. State Tech. § 303). The law is designed to support electronic commerce and to streamline the use of electronic records by government entities.

4. Financial Services

As noted above, on March 1, 2017, the Department of Financial Services (DFS) issued a comprehensive regulation setting forth cybersecurity requirements applicable to all "covered entities" in the state (23 NYCRR 500.00 through 23 NYCRR 500.23). Covered entities include any individual or non-government entity required to operate under a license, registration, charter, or "similar authorization" under the New York Banking Law, Insurance Law, or Financial Services Law

(23 NYCRR 500.01(c)). Accordingly, the regulation generally applies to banks, financial service companies, and insurance companies licensed to do business in New York. The regulation requires covered entities to develop a cybersecurity program and policies, and include requirements regarding access control, systems and network security, and data retention and destruction, as outlined more fully below.

Exemptions: Not all companies regulated by the DFS are subject to the cybersecurity regulation. Entities that would otherwise be covered but that have fewer than 10 employees (including independent contractors), less than $5 million in gross revenue each of the last three years, or less than $10 million in year-end total assets are exempt from some of the regulatory requirements, as are entities that do not operate an information system or control nonpublic information. An otherwise-covered entity claiming an exemption must file a notice of exemption, and if it loses the exemption, it must comply with the regulations within 180 days after such time (23 NYCRR 500.19 and Appendix B).

Cybersecurity program and policy: Covered entities must maintain a cybersecurity program designed to protect the confidentiality, integrity, and availability of the entity's information systems and the nonpublic information stored on such systems. The program must be designed to identify risks; use defensive infrastructure to protect information systems and nonpublic information stored on them from unauthorized access; detect, respond to, and recover from cybersecurity events; and fulfill any regulatory reporting requirements. The entity may adopt the cybersecurity program of an affiliate, provided it meets the delineated regulatory requirements (23 NYCRR 500.02).

The regulation defines "nonpublic information," at a minimum, to include business-related information that, if tampered with or disclosed, would cause material adverse impact to the business; personal information about an individual that, by its nature, could be used to identify the individual (including social security numbers, driver's license numbers, account numbers or credit or debit card numbers, security codes or passwords, or biometric information); or information on the mental, physical, or behavioral health of the individual or a member of the individual's family (23 NYCRR 500.01(g)). The cybersecurity program must include penetration testing and vulnerability assessments or in the alternative "continuous monitoring". (23 NYCRR 500.05). The penetration testing must be performed annually for the "Covered Entity's Information Systems … based on relevant identified risks in accordance with the Risk Assessment." *Id.* The vulnerability assessment is conducted bi-annually, and includes "any systematic scans or reviews of Information Systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the Covered Entity's Information Systems based on the Risk Assessment." *Id.* In addition, the policy must include written procedures, guidelines, and standards ensuring the use of secure development practices for the development of in-house applications used by the covered entity (23 NYCRR 500.08).

In addition, a covered entity must implement and maintain a written cybersecurity policy setting forth its policies and procedures for the protection of its information systems. The regulation specifies 14 areas that must be covered in the policy, including information security, access controls, business continuity, disaster recovery, customer data privacy, and vendor and third-party management, among others (23 NYCRR 500.03).

Each covered entity must appoint a qualified individual to oversee the implementation of the cybersecurity program and to enforce its cybersecurity policy (the "Chief Information Security Officer," or "CISO"). The CISO may be an employee of the entity, an affiliate, or a third party, but if the CISO is employed by a third party, the covered entity retains responsibility for compliance, and must appoint a senior executive to direct the third party, and must require the third party to maintain a similar cybersecurity program. The CISO is required to make an annual report to the covered entity's board of directors, or if no such board or equivalent governing body exists, to a

senior officer that covers specified information concerning the cybersecurity program (23 NYCRR 500.04).

Risk assessment: Covered entities must also conduct a risk assessment, which will guide its development of a cybersecurity program and related policies. The risk assessment generally must evaluate and categorize the risks or threats facing the entity, the adequacy of current controls to address them, and mitigation requirements. It must allow for revision of controls in response to technological developments and evolving threats (23 NYCRR 500.09).

Access controls: The regulation provides that covered entities must limit user access privileges to information systems that provide access to nonpublic information and must periodically review any privileges granted (23 NYCRR 500.07). In addition, covered entities must use effective controls, including multi-factor or risk-based authentication (as defined in 23 NYCRR 500.01(f) and (l), respectively), to protect against unauthorized access to nonpublic information or information systems. Multi-factor authentication must always be used for any individual accessing a covered entity's internal network through an external network, unless the CISO certifies that equivalent or more stringent controls are used (NYCRR 500.12).

Data retention, destruction, and audit trails: Security systems must be designed to reconstruct financial transactions and allow for an audit trail, and any resulting records must be retained for at least five years (23 NYCRR 500.06). However, the regulations further provide that covered entities must include policies and procedures for the secure disposal of any nonpublic information that is not necessary for operations or other legitimate business purposes, unless the information is required to be maintained by law or where targeted disposal is not feasible (23 NYCRR 500.13).

Encryption: As part of its cybersecurity program, a covered entity must implement certain controls, including encryption, to protect nonpublic information either held at rest or in transit over external networks. If encryption is infeasible, the entity must secure the nonpublic information using alternative means certified by the CISO. If compensating controls are in use, the CISO must review them at least annually (23 NYCRR 500.15).

Training and personnel: In addition to appointing a CISO, covered entities must use qualified cybersecurity personnel sufficient to manage risk and comply with the regulations. The entity must provide cybersecurity personnel with updates and training sufficient to address relevant risks and must verify that such personnel are taking steps to maintain current knowledge. Affiliate or third-party providers may be used for this purpose, but such providers must meet the requisite security policy (see below) (23 NYCRR 500.10). In addition, an entity must implement procedures that monitor the activity of authorized users and detect unauthorized access to nonpublic information by such users, and must provide for regular, updated cybersecurity awareness training for all personnel (23 NYCRR 500.14).

Third-party service providers: To the extent that a covered entity uses third-party service providers, the entity must implement written policies and procedures designed to ensure the security of information systems and nonpublic information that are accessible to the provider. The procedure must address the third party's own procedures, including its access control, authentication processes, and encryption policies as discussed above, and must provide that third-party providers are assessed periodically (23 NYCRR 500.11).

Incident response plan: Each covered entity must establish a written incident response plan designed to respond promptly to, and recover from, cybersecurity events materially affecting its information systems or the continuing functionality of the entity's business or operations. The plan must address internal response plans, the goals of the plan, the definition of roles and responsibilities, communication and information sharing, identification of remediation

requirements, documentation of events, and subsequent evaluation and revision of the plan (23 NYCRR 500.16).

Reporting requirements: Covered entities are required to report a defined cybersecurity incident to the DFS within 72 hours of a "determination" that the event has occurred if the event requires notice to any government body, self-regulatory agency, or other supervisory body, or if the event has a reasonable likelihood of materially harming the entity's normal operations (23 NYCRR 500.17(a)). In addition, covered entities must file a report with DFS annually, by February 15, that the entity is in compliance with the cybersecurity regulation, and must maintain certain records and data supporting the documentation for a minimum of five years (23 NYCRR 500.17(b) and 23 NYCRR App. A).

Enforcement: The cybersecurity regulation is subject to enforcement by the Superintendent of DFS pursuant to its authority under applicable laws (23 NYCRR 500.20). The DFS has issued a series of frequently asked questions to assist covered entities in conducting their compliance activities, which is updated as needed by DFS.

Transition: In general, covered entities were required to have certain of the requirements of the new cybersecurity regulation in place within 180 days of their effective date (August 28, 2017). However, many of the provisions have extended transition periods, ranging from one to two years from the date of implementation, as specified by statute (23 NYCRR 500.22).

Other provisions related to financial services sector: N.Y. Exec. Law § 296(16) prohibits any person, in connection with the provision of credit to an individual, to inquire about any arrest or criminal accusation of the individual that is not currently pending against the individual, that has been resolved in the individual's favor or by a youthful offender adjudication, or that has resulted in a sealed conviction.

5. Health Care

N.Y. Pub. Health Law § 18.2(a)-(c) gives individuals the right to access and inspect any patient information in the possession of their health care providers, including health care facilities and practitioners. Access must be granted within 10 days of receiving a written request (N.Y. Pub. Health Law § 18.2(a)-(c)). Exceptions to the requirement are provided for, such as when access will cause substantial or identifiable harm to the subject or others (N.Y. Pub. Health Law § 18.3(a), (b), and (d). In addition, access may be denied if the information concerns a minor and a request for access from a parent or guardian would have a detrimental impact on the provider's relationship with the patient (N.Y. Pub. Health Law § 18.2(c)), or if the minor objects to the disclosure (N.Y. Pub. Health Law § 18.3(c)).

Health care providers are required to keep patient information confidential and may only disclose it in accordance with the Public Health Law. N.Y. Pub. Health Law § 18.6 allows for such information to be disclosed only with patient authorization or in accordance with law. Certain disclosures may be made without patient authorization, such as when it is to practitioners or other personnel employed by the provider or to government agencies under specified circumstances. The amount of information disclosed must be limited only to the amount necessary in light of the reason for disclosure, and the information must be kept confidential by the party receiving it (N.Y. Pub. Health Law § 18.6). An individual may challenge the accuracy of information held by the provider and may require that a statement be inserted as part of his information that will be provided together with any information released that addresses any alleged inaccuracy (N.Y. Pub. Health Law § 18.8).

N.Y. Mental Hyg. § 33.13 and N.Y. Mental Hyg. 33.16 contain provisions applicable to mental health facilities that are substantially similar to the provisions of the Public Health Law outlined above, classifying records maintained by such facilities as nonpublic and confidential, restricting disclosure except under specified circumstances, and providing for patient access to records.

The Health Privacy Project of the Institute for Health Care Research and Policy at Georgetown University has issued a document called "The State of Health Privacy" that provides a comprehensive overview of New York privacy provisions applicable to the health care sector.

6. HR & Employment

N.Y. Lab. Law § 203-D prohibits employers from publicly posting or displaying an employee's social security number (SSN), visibly printing an SSN on any identification card or badge (including time cards), placing an SSN in files with unrestricted access, or communicating an employee's personal identifying information to the general public. In addition to SSNs, personal identifying information includes home address or telephone number, personal e-mail address, Internet identification name or password, parent's surname prior to marriage, or driver's license number. In addition, an SSN may not be used as an identification number for occupational licensing purposes.

N.Y. Lab. Law § 203-C(1) prohibits employers from causing a video recording being made of an employee in a restroom, locker room, or room designated for use by employees to change clothing, unless authorized by a court order. In addition, no video recording made in violation of this provision may be used by an employer for any purpose (N.Y. Lab. Law § 203-C(2)). The prohibition does not apply to any law enforcement personnel engaged in the conduct of authorized duties (N.Y. Lab. Law § 203-C(5)).

Under N.Y.C. Admin Code § 8-107(24), a New York City employer, labor organization, or state agency may not request, or use for employment purposes, the consumer credit history of an applicant or employee, unless a specified exemption applies. See Section I.D.4.

N.Y. Exec. Law § 296(16) prohibits employers from making any inquiry about any arrest or criminal accusation of an individual that is not currently pending against the individual, that has been resolved in the individual's favor or by a youthful offender adjudication, or that has resulted in a sealed conviction.

N.Y.C. Admin. Code § 8-107 (11-a)(a)(3) prohibits employers in New York City from making any inquiry related to the pending arrest or criminal conviction record of an applicant until after the employer has extended a conditional offer to the applicant. After making a conditional offer, an employer may inquire about the applicant's arrest or conviction record if it provides a written copy of the inquiry to the individual, performs the inquiry pursuant to Article 23-A of the New York Corrections Law, provides a copy of the analysis to the applicant (including any reasons for adverse action based on the analysis if applicable), and gives the applicant three business days to respond to the analysis (N.Y.C. Admin. Code § 8-105 (11-a)(b)). The prohibition does not apply to actions taken by employers with respect to federal, state, or local laws requiring criminal background checks or barring employment based on criminal history, or to actions taken with respect to applications for employment as a peace officer or other specified positions (N.Y.C. Admin. Code § 8-105 (11-a)(e)-(f)).

N.Y. Lab. Law § 201-E provides that a person charged with the custody of the health records of employees treated at an on-site occupational health service center may not disclose any employee patient record to an employer without the express authorization of the employee, or as otherwise allowed by law.

7. Insurance

Insurance companies subject to the New York Insurance Law are subject to regulatory requirements regarding the privacy of consumer and customer health information (11 NYCRR 420.17 through 11 NYCRR 420.21). Specifically, the regulations provide that no licensee may disclose nonpublic health information about a consumer or customer unless an authorization is obtained from the consumer or customer (11 NYCRR 420.17(a)). The regulations provide for several

exceptions from this requirement, including claims administration and management, investigation of fraud or misconduct, and disclosures required by law, among several others (11 NYCRR 420.17(b)). The regulations specify the form of the required authorization (11 NYCRR 420.18) and prohibit discrimination by the insurer against any consumer or customer who has not authorized such disclosure (11 NYCRR 420.20). For a discussion of the regulations that govern insurance company obligations with respect to the privacy of consumer financial information, see Section I.D.8.

Regulations setting forth cybersecurity requirements applicable to financial services companies in the state (23 NYCRR 500.00 et seq.) are applicable to companies operating under a license or registration under the State Insurance Law, Banking Law, or Financial Services Law (23 NYCRR 500.01(c)). For a comprehensive discussion of these requirements, see Section I.E.4. For information on how these regulations are expected to interact with existing federal requirements under the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), see "Dueling Cybersecurity Regulations for Health Care: HHS Meets New York State," *Privacy Law Watch*, March 21, 2017.

N.Y. Ins. Law § 3217-A(b)(5) requires insurance companies to provide, on the request of an insured or potential insured, information on procedures used by the insurer for protecting the confidentiality of medical records and other insurance information. A similar provision on the Insurance Law applies to health service, hospital service, and non-profit medical expense indemnity corporations (N.Y. Ins. Law § 4324(b)(5)).

N.Y. Ins. Law § 321 provides that any insurance company that is a member of a medical information exchange center or that otherwise transmits medical data to a similar facility must obtain an applicant's informed consent prior to making a transmission to such a facility. Informed consent will not be considered to have been given unless the insurance company gives clear and conspicuous notice to the applicant furnishing a description of the facility, the circumstances under which the facility may release the information to other persons, and the applicant's right to request the facility to disclose information or to correct any inaccuracies in the information. In addition, medical information exchange centers must maintain information pertaining to HIV tests with a code.

N.Y. Exec. Law § 296(16) prohibits any person, in connection with the provision of insurance to an individual, to inquire about any arrest or criminal accusation of the individual that is not currently pending against the individual, that has been resolved in the individual's favor or by a youthful offender adjudication, or that has resulted in a sealed conviction.

N.Y. Ins. Law § 2615 prohibits insurers from requesting or requiring an individual proposed for insurance coverage to be the subject of a genetic test without written, informed consent that includes names of the persons or organizations to which the information may be disclosed, and requires additional written informed consent prior to disclosing the information to persons or organizations that are not covered by the original consent.

8. Retail & Consumer Products

N.Y. Gen. Bus. Law § 218-A requires retail mercantile establishments to conspicuously post their refund policies. The statute requires that the notice must be posted on the retail item itself, on a sign affixed to each cash register, on a sign situated to be seen from a cash register, or at each entrance to the store. The statute specifies the items that must be included in the notice, including the conditions for a refund and the consumer's entitlement to a written copy of the policy. A consumer is entitled to a cash refund or a credit if the retailer violates this provision for a period of 30 days from the date of purchase.

N.Y. Gen. Bus. Law § 218-AA governs retailer's obligations with respect to giving notice concerning warranties for "grey markets merchandise." Grey markets merchandise is defined as a brand-name

consumer product (used for personal, family, or household purposes only) normally accompanied by a warranty valid in the U.S. that was imported to the U.S. through channels other than the manufacturer′s authorized U.S. distributor, for sale in New York, that may not be accompanied by the manufacturer′s express written warranty. Retailers offering such items for sale must post a notice disclosing that some of such products, or a specific product, are not accompanied by a manufacturer′s warranty valid in the U.S., accompanied by instructions in English, or eligible for a manufacturer′s rebate. The law provides for posting requirements and subjects retailers failing to provide notice to liability for refunds or credits to buyers for 20 days after the date of purchase.

N.Y. Gen. Bus. Law § 396-T requires retailers to disclose specified information prior to selling merchandise to a consumer pursuant to a layaway plan. The disclosure must contain several specified elements, including a description of the merchandise, total costs, the amount of charge attributable to the layaway, the duration of the layaway plan, required payment schedules, and refund policies.

9. Social Media

There are no state privacy laws specifically applicable to social media. However, bills have been introduced in the New York Assembly and Senate that would expand privacy protections afforded to information contained in social media accounts and that would, among other items, prohibit employers from requiring an employee to provide access to his personal e-mail or social media accounts (see Section IV., below).

In addition, social media companies maintain on their platforms a variety of information that would be characterized as "private information" subject to the Information Security Breach and Notification Act (N.Y. Gen. Bus. Law § 899-AA), which requires New York businesses that own or license computerized data that includes such information to notify affected New York residents following the discovery of a breach in security in their computer data systems (see Section I.C.8.).

10. Tech & Telecom

N.Y. Gen. Bus. Law § 390-C requires businesses offering Internet access to the public to post a warning advising users that they should install a firewall or other security measures when accessing the Internet.

N.Y. Gen. Bus. Law § 399-DD provides that no person or business entity may knowingly and intentionally procure, sell, or fraudulently transfer or use telephone record information from a telephone company without written authorization from the telephone customer to whom the record relates. This prohibition does not apply to actions pursuant to a subpoena, by a law enforcement agency, or in accordance with other applicable laws.

11. Other Sectors

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

F. Electronic Surveillance

N.Y. Penal § 250.05 prohibits any person from unlawfully engaging in wiretapping, mechanical overhearing of a conversation, or intercepting or accessing an electronic communication. Accordingly, any audio surveillance or video surveillance with accompanying audio is prohibited.

For information regarding video recording of employees, see Section I.E.6.

G. PRIVATE CAUSES OF ACTION

1. Consumer Protection

Under the Information Security Breach and Notification Act (N.Y. Gen. Bus. Law § 899-AA), if the attorney general's office finds that the breach notification law has been violated, it may bring an action, within two years of the date of the act complained of or the discovery of the act, on behalf of the people of the state to enjoin continued violation. In such an action, a court may provide for preliminary relief and may award damages to individuals for actual losses suffered as a result of the violation. If the court finds that the violation is knowing or reckless, it may impose a civil penalty of the greater of (a) $5,000 or (b) $10 per instance of failed notification, up to a cap of $150,000 (N.Y. Gen. Bus. Law § 899-AA(6)).

N.Y. Gen. Bus. Law § 399-DD (third version) provides that the attorney general may bring an action on behalf of the people to enjoin a violation of the prohibition of the procurement of telephone record information from a telephone company without written authorization from the telephone customer to whom the record relates. Injunctive relief and damages are available, and civil penalties of up to $1,000 may be imposed.

N.Y. Gen. Bus. Law § 399-H.3 provides for a civil cause of action whenever a business violates provisions prohibiting the disposal of records containing personally identifying information without shredding the record or otherwise negating the personal information (see Section I.D.2.). The action provides for injunctive relief, and under specified circumstances, civil penalties of up to $5,000 per violation may be imposed.

N.Y. Gen. Bus. Law § 399-DDD (first version) titled "Confidentiality of social security account number," provides for a civil cause of action against a person or business entity that violates its provisions prohibiting such entities from communicating an individual's social security number (SSN) or otherwise failing to protect the confidentiality of an SSN (see Section I.D.10.). Civil penalties also are authorized, up to $1,000 for a single violation or $100,000 for multiple violations resulting from a single act or incident. Subsequent violations are subject to a civil penalty of up to $5,000 for a single violation or $250,000 for multiple violations arising out of the same incident. N.Y. Gen. Bus. Law § 399-DDD (second version), titled "Disclosure of social security number," provides that no person or business entity may require an individual to disclose his SSN, or refuse any service, privilege, or right of an individual based on the refusal to disclose an SSN, unless an enumerated exception applies (see Section I.D.10.)–calls for a civil cause of action by the attorney general and civil penalties of up to $500 for a first offense and $1,000 for subsequent offenses.

Retailers that violate provisions of the General Business Law regarding required notices regarding warranties for "grey markets merchandise" (see Section I.E.8.) are subject to a civil cause of action to enjoin or restrain the violation. A court finding a violation may impose a civil penalty of up to $500 per violation (N.Y. Gen. Bus. Law § 218-AA.6).

Retailers that violate provisions of the General Business Law requiring disclosure of specified information prior to selling merchandise to a consumer pursuant to a layaway plan (see Section I.E.8.) are subject to a civil cause of action to enjoin or restrain the violation (N.Y. Gen. Bus. Law § 396-T(d)).

2. Identity Theft

N.Y. Penal § 190.77 through N.Y. Penal § 190.80-A define actions constituting identity theft in New York and provide for criminal penalties for varying degrees of identity theft, including identity theft in the third through first degrees and aggravated identity theft. Third-degree identity theft is a class A misdemeanor (up to one year in prison and a fine of up to $1,000 or double the amount of the gain from the theft), second-degree identity theft is a class E felony (up to four years in prison and a

fine of up to $5,000 or double the amount of the gain from the theft), and first-degree and aggravated identity thefts are class D felonies (up to seven years in prison and a fine of up to $5,000 or double the amount of the gain from the theft).

Similar provisions apply to the unlawful possession of personal identification information (N.Y. Penal § 190.81 through N.Y. Penal § 190.83) and unlawful possession of a skimmer device (N.Y. Penal § 190.85 through N.Y. Penal § 190.86).

For New York's recent adoption of an emergency rule establishing the Identity Theft Prevention and Mitigation Program, see Section IV.C.3.

3. Invasion of Privacy

N.Y. Civ. Rights Law § 50 provides that any person, firm, or corporation that uses the name, portrait, or picture of any person for advertising or trade purposes without written consent is guilty of a misdemeanor. In addition, the victim of such an action can maintain an equitable action in court for injunction of a violation and for damages (N.Y. Civ. Rights Law § 51).

N.Y. Civ. Rights Law § 50-B requires that the identity of a victim of a sex offense or an offense involving the transmission of HIV must remain confidential, except under specified circumstances. A person whose identity is disclosed in violation of this provision may bring a private action to recover damages, including reasonable attorney fees (N.Y. Civ. Rights Law § 50-C).

4. Other Causes of Action

A data subject who has been aggrieved by a violation of the Personal Privacy Protection Law by a state agency may seek judicial review and relief. If the data subject prevails, a court may award attorney fees and disbursement reasonably incurred (N.Y. Pub. Off. Law § 97).

Any person aggrieved by a violation of New York City's Human Rights Law, including prohibitions on persons inquiring about an individual's credit history (see Section I.D.4.) or criminal record (see Section I.D.5.), may bring a civil cause of action before the city's Commission on Human Rights. The law sets forth procedural requirements for such an action, including potential mediation or conciliation and investigative requirements. On the issuance of a decision or order by the Commission, judicial review is available to either party (N.Y.C. Rules § 8-109 through N.Y.C. Rules § 8-123).

If an individual is denied access to his patient records, the individual may seek judicial review of the provider's refusal (N.Y. Pub. Health Law § 18.3(f)).

N.Y. Lab. Law § 203-C(3) allows for a civil cause of action to be brought against an employer that violates the prohibition against video recording of employees in restrooms, locker rooms, and other changing areas (see Section I.F.). In such an action, a court may award damages and reasonable attorney fees and costs, as well as injunctive relief against the employer.

H. Criminal Liability

N.Y. Penal § 156.00 through N.Y. Penal § 156.50 make it a crime to use another person's computer without authorization or to trespass or tamper with a computer for various illegal purposes. Violations range from a misdemeanor to a Class C felony, depending on the offense.

N.Y. Gen. Bus. Law § 380-P provides that any officer or employee of a consumer reporting agency who provides information about an individual from the agency's files to a person who is not authorized to receive it is subject to a fine of up to $5,000, one year in prison, or both.

N.Y.C. Rules § 8-129 provides that any person who violates an order of the Commission on Human Rights regarding a violation of the N.Y.C. Human Rights Law, including prohibitions on persons

inquiring about an individual's credit history (see Section I.D.4.) or criminal record (see Section I.D.5.), is subject to imprisonment for up to one year, a $10,000 fine, or both.

Any person who willfully violates provisions of the New York Civil Rights Law prohibiting the conduct of genetic testing without informed consent or the disclosure of information obtained from such a test without consent is guilty of a misdemeanor punishable by a civil fine of not more than $5,000, up to 90 days' imprisonment, or both (N.Y. Civ. Rights Law § 79-L.6(b).

II. REGULATORY AUTHORITIES AND ENFORCEMENT

A. Attorney General

The New York Attorney General's Bureau of Internet and Technology and Bureau of Consumer Frauds & Protection are responsible for enforcing a number of New York privacy laws, including most of the Information Security Breach and Notification Act (N.Y. Gen. Bus. Law § 899-AA) and other laws.

B. Other Regulators

The Department of Financial Services has enforcement powers over the provisions of the cybersecurity requirements applicable to all "covered entities" in the state (23 NYCRR 500.00 through 23 NYCRR 500.23) (see Section I.G.4.).

The New York City Commission on Human Rights is authorized to enforce the provisions of the N.Y.C. Human Rights Law (Title 8, Chapter 1 of the Administrative Code), including the investigation of claims regarding the violation of anti-discriminatory provisions, including prohibitions on persons inquiring about an individual's credit history (see Section I.D.4.) or criminal record (see Section I.D.5.) (N.Y.C. Rules. § 8-105).

C. Sanctions & Fines

Any person who violates provisions of the New York Civil Rights Law prohibiting the conduct of genetic testing without informed consent or the disclosure of information obtained from such a test without consent is subject to a civil fine of up to $1,000 (N.Y. Civ. Rights Law § 79-L.6(a)). Willful violations are subject to larger fines or imprisonment (see Section I.H.).

While there are no administrative fines or sanctions for a violation of the Information Security Breach and Notification Act, courts are entitled to impose civil penalties pursuant to an action brought by the attorney general under specific conditions (see Section I.G.1.).

Under N.Y.C. Rules § 8-126, the New York City Commission on Human Rights may impose civil penalties for violations of anti-discriminatory provisions, including prohibitions on persons inquiring about an individual's credit history (see Section I.D.4.) or criminal record (see Section I.D.5.). The penalty imposed may not exceed $125,000. If a violation is found to be willful, wanton, or malicious, or involves discriminatory harassment or violence, the fine may be as much as $250,000.

Employers that violate provisions of the New York Labor Law prohibiting the disclosure of an employee's personal identifying information (see Section I.D.6.) are subject to a civil fine imposed by the Commissioner of Labor of up to $500 for each knowing violation (N.Y. Lab. Law § 203-D(3)).

D. Representative Enforcement Actions

1. EmblemHealth

On March 6, 2018, the New York Attorney General announced a settlement agreement with healthcare provider EmblemHealth concerning a mailing error that resulted in more than 81,000 social security numbers being disclosed. A $575,000 penalty was imposed together with the requirements that the insurer implement a corrective action plan and comprehensive risk assessment.

2. Aetna

On Jan. 23, 2018, Aetna, Inc. settled with the New York Attorney General over claims the insurance provider sent letters that exposed, through a transparent address window, the HIV status of 2,460 state residents. The insurance provider will pay $1.15 million in civil penalties under the settlement agreement. Aetna didn't admit fault under the settlement, but agreed to update privacy protections for personal health information and hire outside consultants to monitor compliance with the settlement.

3. CoPilot

On June 15, 2017, the New York Attorney General announced a settlement with CoPilot Provider Support Services, Inc. based on its violation of the Information Security Breach and Notification Act (N.Y. Gen. Bus. Law § 899-AA). CoPilot failed to provide notification with respect to a data breach that exposed over 200,000 patient records. The company agreed to pay $130,000 in penalties and to improve its notification and legal compliance program. For more information on the settlement, see the Attorney General's press release.

4. TRUSTe

On April 6, 2017, the New York Attorney General announced a $100,000 settlement with True Ultimate Standards Everywhere (TRUSTe) based on the company's failure to prevent tracking technology from being used on a variety of children's websites. For more information on the settlement, see the Attorney General's press release.

5. Mobile Health App Developers

On March 23, 2017, the New York Attorney General reached a settlement with three mobile health app developers–Cardiio, Runtastic, and Matis–arising in part over irresponsible privacy practices. The settlement requires the application manufacturers to require affirmative consent to their privacy policies and to disclose that they collect information that may be personally identifying. For more information on the settlement, see the Attorney General's press release.

6. Trump Hotel Collection

On Sept. 23, 2016, the New York Attorney General reached a settlement with Trump Hotel Collection (THC) under which THC agreed to pay $50,000 in penalties and to shore up its data security policies and procedures. The case involved data breaches that led to the exposure of more than 70,000 credit card numbers. For more information on the settlement, see the Attorney General's press release.

E. State Resources

Information on breach notification requirements are available on the website of the New York Office of Information Technology Services.

The Attorney General's Bureau of Internet and Technology maintains a variety of information concerning privacy and identity theft on its website.

The Department of State's Committee on Open Government website contains information on the PPPL.

III. RISK ENVIRONMENT

New York's data security and privacy landscape is dominated by the sweeping initiative launched in early 2017 by the state's powerful banking and insurance regulator, the Department of Financial Services (DFS). Businesses covered by the new cybersecurity regulation are still working to implement its staggered requirements.

Most notable, the new cybersecurity regulation contains an annual certification–similar to Sarbanes Oxley on the federal level–which requires a senior corporate officer or board member to attest to an organization's compliance with the regulation. To our knowledge, this is the first such certification requirement in data security regulation. For a comprehensive discussion of the cybersecurity regulation, see the Bloomberg Law/Patterson Belknap Webb & Tyler LLP mini treatise available here.

And more recently, New York Governor Andrew M. Cuomo announced that he has directed the DFS to issue a new regulation requiring "credit reporting agencies to register with" the DFS, as well as comply with the Department's "first-in-the-nation cybersecurity standard." According to Governor Cuomo, the Equifax breach was a "wake-up call," and New York is now "raising the bar for consumer protections" with the "hope" the DFS's approach "will be replicated across the nation."

The DFS proposed regulation places credit reporting agencies squarely within the purview of the agency, prohibits them from committing "any unfair" act, and requires them to comply with the DFS cybersecurity regulation. The proposal, which is subject to the statutory 45-day-reporting and public-comment period, includes a litany of detailed and unprecedented requirements for "consumer credit reporting agencies." The public comment period expired on November 20, 2017.

In addition, the New York Attorney General's Office introduced a bill aimed at toughening data security standards more generally in the state. The Stop Hacks and Improve Data Security Act or SHIELD Act requires any business that owns or licenses computerized data housing New Yorkers' private information to "implement and maintain reasonable safeguards." The proposal makes a distinction between "personal" and "private" information. Personal information is defined as any information –name, number, personal mark, or other identifier–that can be used to identify a natural person. Private information is defined as the combination of personal information plus at least one or more data elements when either is not encrypted or when the encryption key has been accessed or acquired. The following qualify as data elements under the SHIELD Act:

- social security number;
- driver's license or identification card number;
- account number or credit or debit card number in combination with a password that would permit access to an individual's financial information;
- account number or credit or debit card number if such number could be used to access an individual's financial information without additional identifying information;
- biometric information, such as an individual's physical characteristics;
- user name or email address in combination with a password; or
- any unsecured protected health information.

Private information does not include publicly available information that is made available to the general public pursuant to federal, state, or local government records.

A covered entity triggers the SHIELD Act when a "breach of the security of the system" occurs. A "breach of the security of the system" is defined as the unauthorized access to or acquisition of computerized data that contains private information. An employee's good faith access to or acquisition of private information for purposes of the business does not constitute a breach if such private information is not used or subject to unauthorized disclosure.

To determine whether information has been accessed, or reasonably believed to be accessed, a business may consider whether the information was viewed, communicated, used, or altered by a person without valid authorization. And to determine whether information has been acquired, or reasonably believed to be acquired, a business may consider whether the information is in the physical possession of, has been downloaded or copied by, or has been used by a person without valid authorization.

Failure to comply with the SHIELD Act may result in injunctive relief, damages, or civil penalties. Indeed, the SHIELD Act provides that the New York State Attorney General may bring an action for injunctive relief, damages for actual costs or losses incurred by a person entitled to notice, or civil penalties, which, in certain situations, shall not exceed $250,000. The Attorney General must commence the action within 3 years of the date the Attorney General became aware of the violation or the date the notice was sent, whichever occurs first.

The SHIELD Act does not, however, create a private right of action.

The bill is currently pending in the legislature as Senate Bill S6933A. The Assembly version of the bill is A8884A.

For more information, see Patterson Belknap's two-part series (Part One and Part Two) discussing the proposal.

IV. EMERGING ISSUES AND OUTLOOK

A. RECENT LEGISLATION

1. Cybersecurity Regulations

New York's new cybersecurity regulations took effect March 1, 2017. The Cybersecurity Requirements for Financial Services Companies, 23 NYCRR 500, require all individuals and nongovernmental agencies regulated by the Banking Law, Insurance Law, or Financial Services Law to establish and certify a cybersecurity program to the DFS. The regulations are discussed in detail in Section I.E.4., above.

2. Telemarketing Practices

In August 2017, New York enacted AB 6264 (SB 4361), which amended the general business law to require telemarketers to disclose at the beginning of a phone call that the call is being recorded. New York Acts, L 2017, ch. 239.

B. PROPOSED LEGISLATION (2017-2018 SESSION)

1. Consumer Privacy

SB 8149, introduced Apr. 9, 2018, would establish the Online Consumer Protection Act and provide that an advertising network shall post clear and conspicuous notice on the home page of its own website about its privacy policy and its data collection and use practices related to its advertising delivery activities.

2. Access to Personal Accounts

SB 3657 (AB 7521), introduced Jan. 25, 2017, would create the State Online Privacy Act, which, among many provisions, would prohibit employers, educational institutions, and landlords from requiring employees, students, or tenants to provide access to personal e-mail or social media accounts or from taking any adverse action based on a person's refusal to provide such access. The legislation would establish a state office to enforce the provisions of the new law.

AB 0192 (SB 4167), introduced Jan. 4, 2017, would prohibit employers from requiring employees or applicants to disclose means for accessing a personal account or service through an electronic communications device.

3. Data Deletion

AB 5323 (SB 4561), introduced Feb. 8, 2017, would create the Right to Be Forgotten Act, force online publishers to delete information that is flagged as inaccurate or irrelevant, and require publishers to remove this inaccurate or irrelevant information within 30 days after it is identified by a consumer.

4. Security and Breach Notification

SB 6933 (AB 8884), introduced Nov. 1, 2017, is known as the New York Data Security Act (a.k.a., the SHIELD Act) and would amend New York's data breach notification law by broadening the scope of information covered under the notification law, updating the notification requirements when there has been a breach of data, and broadening the definition of a data breach to include an unauthorized person gaining access to information.

AB 5232, introduced Feb. 7, 2017, would have expanded the state's data security and data breach notification law by requiring businesses to develop and maintain an information security program. The bill was similar in scope to other legislation introduced in the prior two sessions of the Assembly, but like those efforts, it failed to emerge from committee and was stricken on Feb. 9, 2017. A similar bill, AB 7997, introduced May 25, 2017, would have required persons or businesses that own or license computerized data containing personal information to develop, implement, and maintain an information security program. The bill failed to emerge from committee and was stricken on Dec. 15, 2017.

AB 8756 (SB 6933), introduced Oct. 31, 2017, in the wake of the Equifax data breach, would have amended New York's data breach notification law by broadening the scope of information covered under the notification law, updating the notification requirements following a breach, and broadening the definition of a data breach to include an unauthorized person gaining access to information. The bill failed to emerge from committee and was stricken on Dec. 15, 2017.

SB 6912 (AB 8782), introduced in Oct. 13, 2017, would require any business or organization that was the source of a breach that exposed or may have exposed personal information to offer, upon notification of the breach, to provide appropriate identity theft prevention and mitigation services at no cost to persons affected for not less than 12 months, along with all information necessary to take advantage of the offer.

5. Internet and Consumer Privacy

AB 7191B (SB 5603B), introduced Apr. 12, 2017, would prohibit Internet service providers (ISPs) from knowingly disclosing a consumer's personally identifiable information (PII) resulting from use of the service without express, written consent and also require ISPs to take reasonable and necessary steps to maintain the security and privacy of consumers' PII.

AB 7236 (SB 5576), introduced Apr. 12, 2017, would require ISPs to provide customers with privacy policies outlining the ISP's data collection and use practices, third party relationships, the purposes

of data collection practices, and the processes through which customers may exercise control over their information, and further require ISPs to obtain written and explicit permission from customers prior to sharing, using, selling, or providing a customer's sensitive data to a third party. A similar bill, SB 3367, introduced Jan. 23, 2017, would require ISPs to keep customer information confidential absent written consent.

SB 0072A (AB 8097), introduced Jan. 4, 2017, would require any business that collects information to allow customers to access that information free of charge, and also require any business that discloses information to third parties to make available the categories of data that were disclosed to third parties and also the names and contact information of all third parties to whom the information was disclosed.

AB 9691 (SB 8149), introduced Feb. 2, 2018, is known as the Online Consumer Protection Act and would require an advertising network to post clear and conspicuous notice on the home page of its own website about its privacy policy and its data collection and use practices related to its advertising delivery activities.

SB 7555 (AB 9780), introduced Jan. 23, 2018, is known as the Personal Information Protection Act and would establish a personal information bill of rights requiring parties having custody of residents' personal identifying information to ensure the security thereof; would provide for the approval of programs to secure personal identifying information by the office of information security; would require the notification of the division of state police and the subjects of information upon the breach of such information; would direct the office of technology services to establish an information sharing and analysis program to assess threats to cybersecurity; would establish standards for the protection of personal information and would provide for a private right of action in the event such standards are violated.

6. Child Online Privacy

AB 7045, introduced Mar. 29, 2017, would restrict marketing of certain prohibited products, such as guns, drugs, alcoholic beverages, and fireworks, to minors on websites, online services or applications, or mobile applications, and would also require providers to permit and facilitate the removal of a minor's personal data upon request.

7. Constitutional Protection

SB 3616, introduced Jan. 25, 2017, would amend the New York Constitution to provide that the "inherent right of each person to personal privacy shall not be infringed."

8. Automatic License Plate Readers

SB 0023, introduced Jan. 4, 2017, would prohibit the use of automatic license plate readers (ALPRs) by any individual, business, or non-law enforcement government entity, except for certain toll collection agencies, and would also place restrictions on the use and sharing of data captured by ALPRs and require that such data be destroyed after 14 days or once an application for a disclosure order has been denied.

C. Other Issues

1. DFS Information Request

On June 29, 2017, the New York Department of Financial Services issued an information request under N.Y. Ins. Law § 308 to all companies and fraternal benefit societies authorized to write life insurance in the state asking them to provide information on their use of external data or information sources in making underwriting decisions. The questions in the information request are

directed primarily to entities that use accelerated/algorithmic underwriting programs or non-traditional sources of so-called "big data."

2. Online Privacy Act

In September 2017, the New York State Department of Financial Services urged institutions that provide data to Equifax to "ensure that this incident receives the highest degree of attention and vigilance." If an "institution provides consumer or commercial related account and debt information to Equifax under any arrangement" the company must "ensure that the terms of the arrangement receive a very high level of review and attention to determine any potential risk associated with the continued provision of data in light of this cyberattack." The guidance also urges banks and insurers to install software on their IT systems.

3. Identity Theft Prevention and Mitigation Program

On Dec. 12, 2017, New York adopted an emergency rule establishing the Identity Theft Prevention and Mitigation Program. Intended to facilitate the timely provision of information and assistance to victims of identity theft, the emergency rule was promulgated in response to the Equifax breach. Because the "theft" of consumers' identities begins with a breach, Consumer Credit Reporting Agencies (CCRAs) are under an obligation to consumers to provide timely information concerning the status of their credit histories, what is being done to protect them and how they can protect themselves. The rule includes mechanisms to facilitate the provision of such information and assistance by:

- clarifying the status of a "victim of identity theft" as inclusive of an individual who has been victimized by a security breach;
- requiring, among other things, the filing of a form with the Division of Consumer Protection that CCRAs establish and notify the Division of a point of contact for Division inquiry and fact finding, and for such point of contact to be available for such dialogue for general matters during regular business hours and within 24 hours in event of a notification of a security breach; and
- the disclosure to the Division and consumers of proprietary and other products offered by the CCRA to consumers for the prevention of identity theft, with information as to the fees and contractual provisions associated therewith.

The announcement of the emergency rule also served as an announcement of its proposed adoption as a final rule, inviting comments until Feb. 10, 2018. The rule was formally adopted on April 16, 2018, effective May 2, 2018.

4. NYC Secure

On Mar. 29, 2018, New York City Mayor Bill de Blasio announced a cybersecurity initiative called "NYC Secure," which aims to protect New Yorkers online. According to the Mayor's press release, NYC Secure "will include a free City-sponsored smartphone protection app that, when installed, will issue warnings to users when suspicious activity is detected on their mobile devices." The free app is scheduled to be released in the summer of 2018. The Mayor also announced new protections for its public Wi-Fi networks.

