International Comparative Legal Guides

Data Protection 2020

A practical cross-border insight into data protection law

Seventh Edition

Featuring contributions from:

Addison Bright Sloane
Anderson Mōri & Tomotsune
Chandler MHM Limited
Clyde & Co
DDPV Studio Legale
Deloitte Kosova Shpk
Deloitte Legal Shpk
D'LIGHT Law Group
DQ Advocates Limited
Drew & Napier LLC
Elzaburu S.L.P.
FABIAN PRIVACY LEGAL GmbH
Herbst Kinsky Rechtsanwälte GmbH
Homburger AG
Khaitan & Co LLP
King & Wood Mallesons
Koushos Korfiotis Papacharalambous LLC
Lee and Li, Attorneys-at-Law
Leśniewski Borkiewicz & Partners
LPS L@w
LYDIAN
Marval O'Farrell Mairal
Matheson
Mori Hamada & Matsumoto
Naschitz, Brandes, Amir & Co., Advocates
NEOVIAQ IP/ICT
Nyman Gibson Miralis
OLIVARES
Pellon de Lima Advogados
PPM Attorneys
Rothwell Figg
Semenov&Pevzner
SEOR Law Firm
SKW Schwarz Rechtsanwälte
SSEK Indonesian Legal Consultants
S. U. Khan Associates Corporate & Legal Consultants
Synch Advokatpartnerselskab
Templars
White & Case LLP
White & Case, s.r.o., advokátní kancelář
Wikborg Rein Advokatfirma AS

ICLG.com

Expert Chapters

Q&A Chapters

Q&A Chapters Continued

Privacy, Data Protection, and Cybersecurity: A State-Law Analysis


Martin M. Zoltick


Jenny L. Colgate

Rothwell Figg

Introduction

While some countries have enacted comprehensive privacy and data protection laws, like the EU's General Data Protection Regulation (GDPR), the United States does not have a single, comprehensive federal law regulating the collection, use, and disclosure of personal information. Instead, U.S. privacy and data protection legislation is comprised of a patchwork system of federal and state laws and regulations – *hundreds of them!* This chapter aims to identify and provide some guidance regarding the state privacy and data protection laws. We have divided these U.S. state laws into three sections: (1) Technology-Specific Laws; (2) Industry-Specific Laws; and (3) Generally Applicable Laws.

Technology-Specific Laws

Biometric and facial recognition

While there currently is no federal regulatory regime specific to biometric data, several states have enacted statutes regulating the collection and use of biometric data, including Illinois, Texas, and Washington. Legislation is currently pending in several other states, including Arizona, Florida, Massachusetts, Montana, New Hampshire, New York, Oregon, Rhode Island, and Vermont. Further, states that have enacted more comprehensive privacy legislation, such as California, include biometric data as part of the definition of personal information that is covered by the respective act (e.g., the California Consumer Privacy Act – CCPA). It is also noteworthy that at least one city in the U.S. – San Francisco – has banned the use of facial recognition technology by police and other government departments.

The states' enacted and pending legislation typically requires that companies give notice when they are collecting, using, or storing biometric information; obtain written consent before collecting biometric data from any individual; have a written biometric data policy regarding retention and destruction of biometric data; and provide for awarding monetary fines, including attorneys' fees, if a violation is found. There has been, and continues to be, active enforcement of these biometric data laws, including addressing jurisdictional issues, what specific information qualifies as a biometric identifier, and what remedies are appropriate.

Biometric data, such as fingerprints, retinal/iris scans, voiceprints, facial recognition scans, and other unique biological patterns or characteristics that are used to identify a specific individual, are unlike other personal identifiers. Social security numbers, driver's licence numbers, and passport numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual and, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions. Acknowledging the heightened risks associated with misuse of biometric information, as evident in recent case law concerning, for example, the Illinois Biometric Information Privacy Act (BIPA), individuals have standing to sue where their biometric information has been obtained in violation of the statute, even where they did not allege any specific injury.

Internet of Things and "connected" devices

Currently, two states – California and Oregon – have enacted specific legislation directed at Internet of Things (IoT) and connected devices. These newly enacted laws, which took effect in January 2020, require manufacturers of connected devices to equip those devices with "reasonable security features". Several other states, including Illinois, Kentucky, Maryland, Massachusetts, New York, Rhode Island, Vermont, and Virginia, are currently considering legislation similar to the California and Oregon laws.

The applicability of California's IoT law is massive. The definition of "connected device" is "any device, or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address". And the law applies to all connected devices sold or offered for sale in California, regardless of where they were manufactured. Just think about all of those connected devices that you have on you right now, in your office, at your home, and add to that all of the connected devices used in industry, such as in manufacturing plants, in server farms, for utilities… the list goes on. Oregon's law, in contrast, is narrower in its application, as it is limited to connected devices used primarily for personal, family, or household purposes.

While there has not yet been any enforcement of these new IoT and connected devices laws, we expect that this will be an active area, given the proliferation of these devices' expected growth, especially in view of the current health crisis and the necessity for widespread global teleworking. The California IoT law is clear that there is no private right of action and that the CA Attorney General, a city attorney, a county counsel, or a district attorney have exclusive authority to enforce the law. The Oregon law, in contrast, provides for a private right of action. What is absent from the California legislation and to date, unknown, is the penalty for violating the law. This surely is an area that requires attention, particularly for manufacturers of IoT and connected devices.

Remote tracking and surveillance – cell phones, drones, and video

This year, some countries around the globe have used mass surveillance and tracking tools, such as cell phone geolocation data, drones, and video surveillance, to stop the spread of the novel coronavirus.

Cell phone geolocation data

In the United States, up until a couple of years ago, different states had different laws regarding the usage of cell phone location tracking data. However, in 2018, the Supreme Court held that the Fourth Amendment of the United States Constitution protects privacy interests and expectations of privacy in one's time-stamped cell-site location information (CSLI), notwithstanding that the information has been shared with a third party (i.e., one's cellular provider), and thus, for government to acquire such information, it must obtain a search warrant supported by probable cause. See *Carpenter v. U.S.*, 138 S. Ct. 2206 (2018).

Drones

Just last year, at least three states (California, Indiana, and Tennessee) enacted legislation related to drone privacy. All three laws are aimed at protecting people's personal privacy from drone surveillance. The California law is the narrowest (limited to homes/interior spaces with an expectation of privacy); the Indiana law prohibits drones over private property or to conduct surveillance; and the Tennessee law prohibits using drones to capture an image of an individual or event. Drone privacy will undoubtedly be the subject of additional privacy legislation, given forecasts regarding increased commercial, police, and hobbyist drone usage in the years to come. Indeed, the recent health crisis has made clear the case for drone delivery systems.

Video surveillance

Video surveillance is regulated by a number of states, and there are currently no federal laws in place in this area. State video surveillance laws typically fall into one of several categories. Some states require consent to use camera surveillance of any kind. Others require consent only if cameras are placed in locations that are considered private. Still other states allow camera surveillance in public locations but prohibit it in private locations. Further states allow video surveillance only if the cameras are in plain sight. In most states, the distinction between what is private *versus* public comes down to one's expectation of privacy in a location; as such, locations such as bedrooms, bathrooms, and dressing rooms are typically considered private.

Audio recordings

Notably, some states that allow video recording have strict restrictions (i.e., wiretapping laws) on audio recordings. Therefore, to the extent one intends to use cameras that record audio as well as video, audio recording laws must be followed, as well. Importantly, there is federal legislation providing that conversations can only be recorded where at least one of the individuals being recorded knows about it. While certain states have enacted legislation largely mirroring the federal legislation, a number of them prohibit audio recordings unless all individuals involved have given consent.

Artificial Intelligence

Artificial Intelligence (AI) is quickly transforming life and business, improving how we diagnose and treat illnesses, grow our food, manufacture and deliver new products, manage our finances, power our homes, and travel from point A to point B. Some current examples of everyday use of AI technology include autonomous/self-driving vehicles, autonomous drones, chatbots/AI-enabled customer assistants, AI-enabled robots/intelligent software agents, search engines, GPS applications, smart assistants, AI-enabled wearables, machine learning/deep learning algorithms, and facial and voice recognition systems. While this AI technology is surely having a positive impact, its benefits come with the risk that the use of these new AI tools will negatively impact the right to privacy.

The privacy concerns centre on the use of AI technology to, for example: identify and track individuals across different devices, in their homes, at work, and in public spaces using voice or facial recognition; identify individuals who want to remain anonymous by re-identification or de-anonymisation; infer sensitive information about people from non-sensitive data; and to profile. Unchecked, this AI-driven identification, profiling, and automated decision-making can lead to unfair, discriminatory, and/or biased outcomes.

Currently, there are no states with specific legislation directed to AI-enabled technologies and privacy. Several states, however, have formed AI task forces to examine AI technologies and recommend how such technologies should be regulated. Those states include Vermont, Alabama, New York, and Washington.

E-Reader services and technologies

Digital book services and technologies have been around for many years now, and several states have specific legislation directed to protecting the personal information of users. Arizona, California, Delaware, and Missouri have each enacted e-Reader privacy laws. Generally, these laws require public libraries and library systems, as well as commercial electronic services and online booksellers, to protect the personal information of library patrons and users of digital book services and technologies, including, for example, records or other information that identifies a patron's borrowing information or use of library information resources, and about books browsed, read, or purchased from electronic services and online booksellers.

Internet Service Providers

Internet Service Providers (ISPs) have access to a wealth of personal information concerning their customers and, as a result, some states have laws already in place to govern the ISPs' collection, use, processing, storage, disclosure, sale, and retention of such information. California, Maine, Minnesota, and Nevada have enacted specific laws directed to ISPs, and 14 other states and the District of Columbia have pending legislation that would restrict how ISPs can collect, use, and disclose consumer data, including users' health and financial details, web browsing history, app usage, and geolocation data.

The Maine law, which passed and went into effect in 2019, is currently the most controversial. Earlier this year, four national associations that represent ISPs sued Maine, arguing that the law violates First Amendment protections. Maine's law requires an ISP to obtain consent from a consumer ("opt-in" consent) before sharing or using any personal data. California has a similar law, but it requires consumers to "opt-out" by asking their ISP to protect their data. Maine's ISP law also prohibits a provider from refusing to serve a customer, charging a customer a penalty, or offering a customer a discount.

The Nevada and Minnesota laws require that an ISP keep certain personal information about its customers private, unless the customer gives permission to disclose the information. Minnesota specifically requires permission from subscribers before disclosing information about the subscribers' online surfing habits and Internet sites visited.

Industry-Specific Laws

In addition to the aforementioned technology-specific privacy laws, there are a number of "sectoral" state privacy laws that overlap, expand, or limit (to what is expressly disclosed in the federal statute and nothing more) the protections and requirements of their federal counterparts. Below we review some of the more notable sectors.

Students

The Family Educational Rights and Privacy Act (FERPA) was enacted in 1974 and requires that federally funded institutions, administered by the U.S. Department of Education, comply with certain procedures regarding the disclosure and maintenance of educational records. Under FERPA, there are three categories of protected information: (1) personally identifiable information (which requires student or parent signature for disclosure); (2) directory information, such as students' names, addresses, telephone numbers, and ID numbers (which can be disclosed unless a student has "opted-out" of the disclosure); and (3) education information, such as transcripts, grades, grade point average, social security number, and evaluations (academic, attendance, psychological) (which can only be disclosed upon student or parent approval).

A large number of states have enacted their own student privacy legislation which, *inter alia*, adds privacy protections to some private schools; prohibits the collection of social security numbers; prohibits the collection of other personally identifiable information, including social media information; provides for data accessibility, transparency, and accountability; and governs student data security and data breaches. A majority of states have also passed legislation regarding the adoption of a state-wide longitudinal data system (SLDS), which links preschool, K-12, and post-secondary education records using unique identifiers that do not permit students to be individually identified, but which record information about the students to help, *inter alia*, audit the system.

Two common state statutes regarding student privacy are Student Online Personal Information Protection Acts (SOPIPAs), as well as statutes regulating contracts between educational institutions and third parties (which are sometimes incorporated into a state's SOPIPA statute). Both of these statutes should be considered carefully by entities involved in "remote learning" given the current health crisis and the closure of schools.

California SB 1177 is an example of a SOPIPA statute. It applies directly to website and application vendors with actual knowledge that their website, web service, or application is used *primarily* for K-12 school purposes and was designed and marketed for such purposes. The law prohibits the disclosure, use, and sharing of covered information; requires secure storage and transmission of covered information; and requires deletion of covered information upon the school district's request. "Covered information" is defined broadly to include any information or materials: provided by the student or the student's parent or guardian in the course of their use of the site or application; created or provided by employee or agent of educational institution; or gathered by the site or application that is descriptive of a student or otherwise identifies a student.

Telephones and telemarketing

The Telephone Consumer Protection Act (TCPA) was enacted in 1991 for the purpose of restricting telemarketing calls. The TCPA has since been revised, including 2003 revisions which established a national Do-Not-Call registry.

A number of states have "mini-TCPA" laws, which piggyback on the federal TCPA law, but in many cases are much stricter. Perhaps the strictest of these mini-TCPA laws is the Connecticut telemarketing law (Conn. Gen. Stat. § 42-288a), which prohibits telephonic sales calls made without prior express written consent. A violation of the Connecticut law is deemed an unfair or deceptive trade practice, and under the Connecticut Unfair Trade Practices Act (CUTPA), a private plaintiff can seek actual damages, punitive damages, and attorneys' fees. The Connecticut law also provides for a fine of up to $20,000 for each violation, plus an additional $5,000 for wilful violations.

The majority of states also have Do-Not-Call registry legislation, though the majority of these states simply adopt the federal Do-Not-Call registry as their own.

Email spam

The Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (the CAN-SPAM Act) is a U.S. statute that was established to protect consumers from unsolicited commercial/business emails. The Federal Trade Commission's compliance guide for the CAN-SPAM Act includes the following "main requirements": (1) do not use false or misleading header information (from, to, reply-to, and routing information); (2) do not use deceptive subject lines; (3) identify the message as an ad; (4) tell recipients where you are physically located; (5) tell recipients how to opt-out of receiving future email from you; (6) honour opt-out requests promptly; and (7) monitor what others are doing on your behalf.

As with other sectoral areas, many states also have laws regulating unsolicited email (spam). The majority of state spam laws pre-date the federal CAN-SPAM Act, and many are now preempted in whole or in part by the CAN-SPAM Act. However, some provisions – such as specific "bulk email" restrictions – remain in effect.

It is noteworthy that states' "bulk email" statutes are typically limited to bulk *commercial* emails (and do not cover other speech, such as political or religious speech). Also noteworthy is that a handful of states, such as Georgia, Ohio, and Tennessee, consider violations of "bulk email" statutes to be criminal offences.

Children

In 1998, Congress enacted the Children Online Privacy Protection Act (COPPA) to limit the collection of personally identifiable information from children (under the age of 13) without their parents' consent. The Act took effect in April 2000. Among the requirements of COPPA, websites must: provide a privacy policy describing their information practices with respect to children; make reasonable efforts to notify parents regarding the site's practices concerning the personal information of children; obtain parental consent prior to collection/use/disclosure of personal information of children; establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of children's personal information; not require children to provide more information than is necessary to participate in the online activity; and delete children's personal information after the reason for which it was collected has passed.

There are at least two state statutes that are also directed at children's online privacy. California's Digital World Act, §§ 22580-22582, also called the "eraser" bill, *inter alia*, (1) permits minors [defined as a natural person under 18 years of age and who resides in the state] to remove or request/obtain removal of content or information posted on an Internet website, online service, or application; (2) prohibits operators of websites, online services, and applications from marketing/advertising to minors products and services that minors are legally prohibited from buying (such as alcoholic beverages, firearms and handguns, and ammunition); and (3) prohibits operators of websites, online services, and applications from marketing/advertising a product or service if the marketing or advertising "is specifically directed to that minor based upon information specific to that minor, including, but not limited to, the minor's profile, activity, address, or location sufficient to establish contact with a minor, and excluding Internet Protocol (IP) address and product identification numbers for the operation of a service".

Delaware also has a statute directed at children's online privacy, which mirrors several of the provisions in the aforementioned California statute. Section 1204C of the Delaware Online Privacy and Protection Act (DOPPA) is entitled "Prohibitions on online marketing or advertising to a child", and "child" is defined therein to be an individual under the age of 18 and resident in the state. Section 1204C of the DOPPA prohibits operators of websites, online or cloud computing services, and applications directed at children from placing marketing or advertising on their products or services that is inappropriate for children's viewing (such as alcohol, tobacco, firearms, and pornography). Also like the California statute, the DOPPA prohibits an operator of an Internet service who has actual knowledge that a child is using the Internet service from using the child's personally identifiable information to market or advertise products or services to the child.

Health

HIPAA stands for the Health Insurance Portability and Accountability Act, which is the main federal law that protects personal health information (PHI) in the United States. There are three main "rules" under HIPAA: (1) the privacy rule, which sets national standards for when PHI may be used and disclosed; (2) the security rule, which specifies safeguards that covered entities and their business associates must implement to protect the confidentiality, integrity, and availability of electronic PHI (ePHI); and (3) the breach notification rule, which requires covered entities to notify affected individuals, the U.S. Department of Health and Human Services, and, in some cases, the media, of a breach of unsecured PHI. HIPAA's standards and requirements apply to: (1) covered entities, which include (a) providers of health or medical care services, such as doctors, dentists, clinics, pharmacies, and nursing homes, and (b) any health plans that provide or pay the cost of health care, such as company health plans, government programmes (such as Medicare and Medicaid), health insurance companies, and health maintenance organisations (HMOs); and (2) "business associates" of covered entities (i.e., people/organisations that create, receive, maintain, or transmit PHI on behalf of a covered entity).

Most states have also enacted laws regarding the use, collection, and disclosure of health information. As with other statutes, where HIPAA already speaks on a specific area, HIPAA applies and the state law is preempted; state law takes effect if there is no HIPAA provision on a specific subject, if the state law is more stringent than HIPAA, or if there is an exception under HIPAA.

Some examples of state-specific laws related to health privacy include genetic privacy acts, insurance information and privacy protection acts, and general health information protection acts that are more stringent than HIPAA (and thus override HIPAA's requirements and penalties).

With respect to genetic data, it is important to remember that HIPAA's protections only apply if the data is being processed by a "covered entity" or a "business associate" of a covered entity. Thus, there is a lot of genetic data out there that is not covered by HIPAA, such as that processed and stored by various online genetic testing companies, like 23andMe. State genetic privacy laws tend to focus on consent – that is, consent required to perform genetic testing and consent required to disclose genetic information. It is also noteworthy that at least five states define genetic information as personal property (Alaska, Colorado, Florida, Georgia, and Louisiana).

A second type of state health-related privacy law are Insurance Information and Privacy Protection Acts. *See, e.g.,* NC Gen Stat § 48-39-5; Conn. Sec. 38a-975 through 999; and California Insurance Code §§ 791-791.27. The purpose of these laws is to establish standards for the collection, use, and disclosure of information gathered in connection with insurance transactions by insurance institutions, agents, or insurance-support organisations. A third type of state health-related privacy law are HIPAA-like statutes that provide for more stringent requirements. An example of such a statute is the California Confidentiality of Medical Information Act (CMIA). Section 56.10(a) of the CMIA provides that "[n]o provider of health care, health service plan, or contractor shall disclose medical information regarding a patient of the provider of health care or an enrollee or subscriber of a health care service plan *without first obtaining an authorization*, except as provided in subdivision (b) or (c)". Section 56.13 further expands the CMIA's restriction on disclosure: "[a] recipient of medical information pursuant to an authorization… may not further disclose that medical information except in accordance with a new authorization that meets the requirements of 56.11[.]" Thus, one could argue that the CMIA requires authorisation for *any* disclosure of medical information, by anyone.

Financial

There are a number of federal financial privacy and data protection laws. For example, the Gramm-Leach-Bliley Act (GLBA) is a federal law in the United States that requires financial institutions to explain how they share and protect customers' private information. The requirements and protections provided by the GLBA include, but are not limited to, the following: (1) financial institutions must create privacy policies; (2) financial institutions must specifically disclose their information-sharing practices; and (3) financial institutions must give customers an "opt-out" to allow customers the ability to prevent the disclosure/sharing of private information.

Several states, such as Alaska, California, Connecticut, Florida, Illinois, and Vermont, have financial privacy laws in place that are "stricter versions" of the GLBA, i.e., providing individuals with the right to receive notice and opt-in (instead of opting-out) to allow a financial institution to share non-public personal information with third parties. Some states' financial privacy laws also allow consumers to choose not to have their information shared with affiliates of their financial institution.

Generally Applicable Laws

The CCPA has received a lot of attention in recent years for being the "*de facto*" United States privacy law. However, there

are a number of other states that have passed, or have pending, general privacy legislation. For example, the Nevada Privacy Law (SB-220), which went into effect on October 1, 2019, requires the posting of certain information in companies' privacy policies (including the categories of data collected, data subject rights to request and change data, and the effective date of the policy), and grants consumers a right to opt-out of the sale of their personal data. The Nevada statute also provides for a $5,000 penalty per violation, as well as temporary and permanent injunctions.

Below is an overview of some categories of other generally applicable (i.e., not industry- or technology-specific) state privacy laws.

Privacy policy creation and posting laws

Several states have laws requiring the creation and disclosure of a privacy policy. For example, Del. Code Tit. 6 § 205C requires an operator of a commercial Internet website, online or cloud computing service, online application, or mobile application that collects personally identifiable information through the Internet about individual users residing in Delaware who use or visit the operator's website, service, or application to make its privacy policy conspicuously available on its website, service, or application. Some states have similar privacy policy creation and posting laws but they are restricted to specific industries or types of information. For example, Conn. Gen. Stat. § 42-471 requires any individual, firm, partnership, association, corporation, limited liability company, organisation, or other entity who collects social security numbers (SSNs) in the course of business to create and publicly display a privacy policy on a web page, and the policy must protect the confidentiality of the SSNs, prohibit the unlawful disclose of the SSNs, and limit access to the SSNs.

Data sharing and data broker registration

The CCPA and the Nevada Privacy Law both allow consumers to opt-out of the sale and sharing of their personal information. It is expected that other state laws will soon follow suit, requiring companies to allow consumers to opt-out of the sale and sharing of their personal information.

It is also noteworthy that sectors which require opt-in consent to process personal information already have a *de facto* restriction on selling and sharing personal information. *See, e.g.,* "Biometric and facial recognition" and "Children" (above).

Some states have additionally started to require data brokers to register with the state, upon which the state makes the registry available to the public via a website. Vermont started this trend with the passage of H.764, and it was later followed by California, which adopted legislation (A.B. 1202) supplemental to the CCPA requiring the registration of data brokers.

Under Vermont H.764, "data broker" is broadly defined as "a business, or unit or units of a business, separately or together, that knowingly collects and sells or licenses to third parties the brokered personal information of a consumer with whom the business does not have a direct relationship". California A.B. 1202 similarly broadly defines "data broker" to encompass entities which engage in non-monetary data sharing. It is expected that more states will likely implement data broker registries in the future.

Data destruction and secure disposal

The majority of U.S. states have enacted disposal laws, requiring that personal information be securely disposed of, destroyed, or otherwise rendered unreadable/indecipherable. (It is notable that there are also sectoral federal laws requiring secure data destruction and disposal, such as HIPAA and the FTC's Disposal Rule, which has secure disposal requirements for information contained in consumer reports.) Most of the state disposal laws apply to both paper and electronic records. Also, most of the state disposal laws apply to businesses and governments, though a minority of states' disposal laws apply only to businesses. Virginia's disposal law applies only to government bodies.

Data breach notification

All U.S. states (as well as the District of Columbia, Guam, Puerto Rico, and the U.S. Virgin Islands) have enacted data breach notification laws, requiring that individuals and entities affected by a data breach notify their customers and other parties about the breach and take specific outlined steps to remedy the situation. (It is notable that, like with secure disposal, there are also sectoral federal laws regarding data breach notification, including HIPAA and the GLBA.)

California enacted the first data breach notification law, which became effective in 2003, and most states have piggybacked on this law in passing their own legislation. Typical requirements of state data breach notification laws require businesses to notify customers of data breaches where the breached information comprises personal information (which is a defined term, and varies from state to state) and, in some cases (usually based on the amount of compromised information), to notify the state Attorney General.

Data security

The majority of U.S. states have enacted data security laws, requiring businesses and/or government agencies that own, license, or maintain personal information to implement and maintain "reasonable security procedures and practices" (or some similar phrase) to protect the information from unauthorised access, use, and destruction. (It is notable that, like with secure disposal and data breach notifications, there are also sectoral federal laws regarding data security, including HIPAA and the GLBA.)

Depending on the statute, specific security measures may be required – such as designating an employee or employees to coordinate the entity's security measures to protect against a security breach, identification of risks of a breach in security, retention of service providers to safeguard personal information, employee training, periodic security audits or assessments, development of standards or guidelines, and corporate reporting of security measures.

Conclusion

There are hundreds of state privacy and data protection statutes, and that number continues to grow as states regulate new areas (such as IoT and AI), as the world faces new challenges (such as the coronavirus pandemic, which has shed light on numerous changes that should be made to existing privacy laws), and as states increasingly enact general privacy statutes (similar to the CCPA). While it is virtually impossible for any individual to keep apprised of all laws and legal developments in the United States, what is possible – and practical – is to stay informed on the subject areas of regulation and the trends. This allows for issue-spotting, which then provides a starting point for further research into specific laws that may be applicable to any given situation.

Martin M. Zoltick is a shareholder with Rothwell Figg in Washington, D.C. He has been practising in the field of technology law for more than 30 years. His practice is focused primarily on IP matters, transactions, privacy, data protection, and cybersecurity. Mr. Zoltick is a Certified Information Privacy Professional in the United States (CIPP/US) and works with his clients to help them understand and navigate the rapidly evolving area of privacy and data protection law. He is working with clients to prepare, integrate, and implement best practices for the CCPA, other states' laws, and GDPR compliance. Mr. Zoltick has a degree in computer science and, prior to attending law school, he worked for several years as a software developer and engineer. This formal training has enabled him to handle complex software-related legal matters. With his technical background and expertise, he is uniquely positioned to work with IT and technical teams to understand potential exposure and minimise the risks of a breach.

Rothwell Figg
607 14th Street NW, Suite 800
Washington, D.C. 20005
USA

Tel: +1 202 783 6040
Email: mzoltick@rothwellfigg.com
URL: www.rothwellfigg.com

Jenny L. Colgate is an experienced intellectual property and data/privacy lawyer whose practice is focused mostly on litigation and contract/licensing matters. Ms. Colgate is a Certified Information Privacy Professional in the United States (CIPP/US) and has experience counselling clients on matters related to privacy, data protection, and cybersecurity, including privacy policies, data mapping, data subject rights, reasonable security measures, contracts related to privacy/cybersecurity issues, and discovery (litigation) issues related to privacy/cybersecurity issues. In addition, Ms. Colgate has advised clients and published analyses regarding numerous state and local privacy and cybersecurity laws, including but not limited to the CCPA, GDPR, BIPA, COPPA, FERPA, and HIPAA. Ms. Colgate has represented clients before numerous agencies and federal courts. Her litigation experience includes matters concerning data and trade secret misappropriation, breach of contract, unfair competition, patent infringement (including patents related to data storage and processing), trademark infringement, and copyright infringement. Ms. Colgate was named a Washington, D.C. *Super Lawyers* "Rising Star" for IP litigation eight years in a row from 2013 to 2020.

Rothwell Figg
607 14th Street NW, Suite 800
Washington, D.C. 20005
USA

Tel: +1 202 783 6040
Email: jcolgate@rothwellfigg.com
URL: www.rothwellfigg.com

The Privacy, Data Protection & Cybersecurity team at Rothwell Figg helps clients understand and navigate these rapidly evolving areas of law. We work with our clients to prepare, integrate, and implement compliance strategies, frameworks for risk management, and best practices. We have experience working closely with our clients to build data inventories and assess their legal obligations; to implement back-end and structural changes that are not only compliant, but also workable; to prepare written policies, assessments, forms, and notices to effectuate legal requirements and best practices; to negotiate, draft, and review agreements for compliance; and to help train staff. We can assist with the design and implementation of incident response plans, and if there ever is an incident, we can serve as trusted advisors, from the investigation stages through to litigation, helping you navigate disclosure requirements to public authorities.

Most of the attorneys in the practice group are experienced litigators with deep technical backgrounds, and have represented clients in a wide variety of venues, including before numerous government agencies, and in state courts, federal district courts and courts of appeal, and the United States Supreme Court.

www.rothwellfigg.com

ROTHWELL FIGG
IP Professionals

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Consumer Protection
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Tax
Cybersecurity
Data Protection
Derivatives
Designs
Digital Business
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Family Law
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Outsourcing
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Renewable Energy
Restructuring & Insolvency
Sanctions
Securitisation
Shipping Law
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by:

global legal group