What Companies Need to Know About Privacy and Data Protection

Aaron Charfoos (CIPP/US) and Stephen Tupper (CIPP/US and CIPP/E)

Each year businesses are gathering more and more information about their customers, clients and even their own employees. That information can also be shared globally in an instant. But what privacy and data security obligations do business have? This article covers the high points of U.S. privacy law as it applies to private-sector commercial actors. It is intended to provide a generalized survey that assists in identifying issues and the resources for additional analysis if required.

Europe and the U.S.: A Study in Opposites

The European Union (and by extension the EEA) and the United States take fundamentally different views of privacy and data security. Beginning in 2018, Europe will be governed by a single, uniform data security law, the General Data Protection Regulation (GDPR). The GDPR will replace a more decentralized scheme that has been in place since 1995 with a comprehensive, mostly "one-stop shop" for privacy rules. The GDPR, like its predecessor law, protects "personal data" which is broadly defined to include "any information relating to an identified or identifiable natural person" and will place broad obligations on controllers and processors of data to protect data throughout its entire life cycle.

The U.S. follows a sectoral model of privacy law, which is to say that privacy is regulated mostly with respect to particular subject matter and there is no overarching statutory or regulatory privacy law.

U.S. Federal Privacy Laws

The U.S. Constitution provides that the federal government may regulate commerce to the extent that it if affects interstate and/or international commerce. In practice, this gives the U.S. government broad powers to legislate and regulate commercial conduct, including that associated with information privacy and security.

Following are the most commonly invoked federal regulatory schemes. This list includes regulated areas as they apply to non-governmental actors. A great deal of privacy regulation exists for governmental agencies, but such regulation is beyond the scope of this article.

	Applicable Law	***Information Covered***	***Persons Covered***	***Additional Information***
Health Information	Health Insurance Portability and Accountability Act of 1996 (HIPAA; Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996) ("HIPAA"). **Privacy Rule:** 45 CFR Part 160 and Subparts A and E of Part 164. Establishes national standards to protect individuals' medical records and other personal health information **Security Rule:** 45 CFR Part 160 and Subparts A and C of Part 164. Identifies three types of security safeguards required for compliance: Administrative, physical, and technical, and prescribes required security measures. Health Information Technology for Economic and Clinical Health ("HITECH") Act (42 U.S.C. §§ 17921 – 17954)	"Protected Health Information" or "PHI." "[I]ndividually identifiable health information: (1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium. (2) Protected health information excludes individually identifiable health information: (i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv); (iii) In employment records held by a covered entity in its role as employer; and (iv) Regarding a person who has been deceased for more than 50 years.	"Covered entities," which, generally speaking, are health care clearinghouses, health plans, health insurers, and medical service providers that engage in certain electronic transactions. See 45 CFR §§ 160.102. "Business associates," which include: (i) a Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information; (ii) a person that offers a personal health record to one or more individuals on behalf of a covered entity; and (iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate. (45 CFR § 160.103)	https://www.hhs.gov/hipaa/for-professionals/privacy/ http://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/

	Applicable Law	*Information Covered*	*Persons Covered*	*Additional Information*
Financial Information	Gramm–Leach–Bliley Act ("GLBA" or "GLB"), also known as the Financial Services Modernization Act of 1999, (Pub.L. 106–102, 113 Stat. 1338, enacted November 12, 1999) (15 U.S.C. § 6801, 16 C.F.R. § 313) Financial Privacy Rule: 15 U.S.C. §§ 6801–6809 Safeguards Rule: 15 U.S.C. §§ 6801–6809. Requires (a) designation of at least one person to supervise safeguards, (b) conduct of risk assessments, (c) development, monitoring, and testing a program to secure the information, and (c) changing the safeguards as needed.	"Nonpublic personal information" or "NPI." Per the Federal Trade Commission, NPI is "any 'personally identifiable financial information' that a financial institution collects about an individual in connection with providing a financial product or service, unless that information is otherwise 'publicly available.'	Financial institutions. Note that the definition is broad enough to cover many businesses that are not banks, such as non-bank mortgage lenders, real estate appraisers, loan brokers, some financial or investment advisers, debt collectors, tax return preparers, and real estate settlement service providers. A good example is auto dealerships when they accept loan applications and essentially serve as the front end of a bank or other provider of credit.	https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm
Credit Information	Fair Credit Reporting Act as amended ("FCRA") (including the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"or "FACTA")) (15 U.S.C. § 1681 et seq., (Pub. L. 108-159, 111 Stat. 1952); 16 C.F.R. § 682; 72 Fed. Reg. 63718 et seq. (Nov. 9, 2007))	Information about a consumer's "credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living." Credit card numbers (which must be truncated on certain receipts and other documents). Account information regarding payments and possible fraud ("red flags").	Credit reporting agencies. Note that persons creating and maintaining databases of information about any consumer's "credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living" could be construed to be a reporting agency. Certain merchants. Creditors and financial institutions.	https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/fair-credit-reporting-act https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf

	Applicable Law	*Information Covered*	*Persons Covered*	*Additional Information*
Social Security Numbers	Privacy Act of 1974 (5 U.S.C. § 552a)	Social security account numbers Except in certain situations, federal, state and local government cannot deny an individual "any right, benefit, or privilege provided by law because of such individual's refusal to disclose his Social Security account number."	Units of government and certain private parties.	https://www.justice.gov/opcl/privacy-act-1974
Video Rental or Sale Records	Video Privacy Protection Act of 1988 (18 U.S.C. § 2710).	Information that identifies a person as having requested or obtained specific video materials or services from a video tape service provider.	Any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials, or any person or other entity to whom a disclosure is made under the law.	https://epic.org/privacy/vppa/
Cable Service Information	Cable Communications Policy Act ("CCPA") (47 U.S.C. § 551, Pub. L. 98-549)	Personal customer information held by cable service providers.	Providers of certain cable, wire, and radio communications services.	http://www.consumerprivacyguide.org
Driver License Information	Driver's Privacy Protection Act of 1994 (also referred to as the "DPPA") (18 U.S. Code § 2721).	Information in U.S. state driver license records, including the following. Information that identifies an individual, including an individual's photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status. An individual's photograph or image, social security number, medical or disability information.	Any user of the information. The statute provides a list of 14 permissible uses of such information and provides penalties for other use of such information. Note that many U.S. data brokers maintain driver license information for permitted purposes. Such brokers are understandably protective of this information and impose onerous requirements on users of the data so as to assure that the information is only used for permitted purposes.	https://epic.org/privacy/drivers

	Applicable Law	*Information Covered*	*Persons Covered*	*Additional Information*
Education Information	Family Educational Rights and Privacy Act of 1974 (20 U.S.C. § 1232g); 34 CFR Part 99.	Educational information, personally identifiable information, and directory information.	Units of government and certain private parties.	http://www.naceweb.org/public/ferpa0808.htm
Personal Information about Children under 13	Children's Online Privacy Protection Act of 1998 ("COPPA) (15 U.S.C. §§ 6501–6506 and 16 CFR Part 312).	Personal information about, or collected from, children under the age of 13 when collected online.	Per the Federal Trade Commission, "[O]perators of commercial websites and online services (including mobile apps) directed to children under 13 that collect, use, or disclose personal information from children. It also applies to operators of general audience websites or online services with actual knowledge that they are collecting, using, or disclosing personal information from children under 13. The Rule also applies to websites or online services that have actual knowledge that they are collecting personal information directly from users of another website or online service directed to children."	https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions
Genetic Information	Genetic Information Nondiscrimination Act of 2008 ("GINA") (Pub. L. 110-233)	Expands Title VII of the Civil Rights Act of 1964 prohibit employers from discriminating against employees on the basis of "genetic information" in hiring, firing, and other activities.	Employers and potential employers.	https://www.eeoc.gov/laws/statutes/gina.cfm
Payment Card Information	Payment Card Industry Data Security Standards ("PCIDSS"). Not law as such. Rather, it is a standard required by many payment card organizations.	Payment card data.	Anyone party to a merchant agreement with a card subscribing card issuer organization.	https://www.pcisecuritystandards.org/

	Applicable Law	*Information Covered*	*Persons Covered*	*Additional Information*
Unfair or Deceptive Trade Practices Generally	Federal Trade Commission Act of 1914 (15 U.S.C. §§ 41-58)	The Federal Trade Commission (the "FTC") has broad powers to act to "prevent unfair methods of competition, and unfair or deceptive acts or practices in or affecting commerce." The FTC enforces other specific legislation, such as FCRA, FACTA, COPPA, and others, but also has broad powers to pursue those who commit other less-specific bad acts. In the privacy field, the FTC has brought enforcement actions in two main categories: (1) Where the actor has made promises (such as in a privacy statement) and then breached them and (2) where the actor is reckless or careless with personal information.	Generally, commercial enterprises with some exceptions where deferral legislation gives specific enforcement powers to other agencies.	https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act

U.S. State Privacy Laws

Generally speaking, individual U.S. states regulate privacy considerations in a manner similar to the way the U.S. government regulates privacy. In fact, many states have their own counterparts of many of the above federal regulatory schemes.

Although U.S. law provides for preemption of state law by federal legislation, the preemptive effect, when it comes to privacy, is usually aimed at creating minimum standards and states are frequently free to impose regulatory controls that are more stringent than federal law.

State Consumer Protection Acts

All states have some form of consumer protection law, usually contained in a "consumer protection act" or similarly-named statute with regulatory and enforcement authority usually given to a state consumer protection agency, the state attorney general, or both. Such state statutes are commonly called "Little FTC Act" because they closely mirror the language and intent of the federal FTC Act. Little FTC Acts may address many or most of the same issues co0vered by the FTC act and most also go on to regulate specific practices, which can include privacy matters.

State Data Protection Laws

Several states (and the number is growing) require that businesses use "reasonable security procedures and practices . . . to protect personal information from unauthorized, access, destruction, use, modification, or disclosure." (Civ. Code § 1798.81.5) or require that businesses adhere to security guidelines (e.g., Mass. 201 CMR 17.00). Such standards are rarely specific in terms of

technologies, encryption strengths, or similar matters because the arms race between businesses and hackers changes the landscape frequently and any particular specification could be quickly outmoded. The California Attorney General has gone so far as to declare that the Center for Internet Security's Critical Security Controls constitutes the minimum acceptable standard.

State Data Breach Laws

At least 47 states require that certain kinds of data breaches must be reported to the data subjects and, in certain cases, to the state attorney general. State laws vary in terms of what kind of information is covered (electronic vs. paper records, information likely to aid in identity theft vs. other kinds of information, etc.), what data subjects are covered (usually residents of the state), what notice must be given, what information cannot be disclosed, whether the attorney general or law enforcement personnel must be notified, and when such notice must be given.

The U.S. Congress has considered a federal data breach notification statute, but versions introduced in the last six congresses have failed to result in federal law. Except in narrow cases (such as breaches involving healthcare information under HIPAA and HI TECH), data breach notification is expected to remain a state law matter for the foreseeable future.

Tort Law

Tort law fills in the gaps left by specific regulatory schemes and the more general authority of the FTC.

Tort law in the U.S. is almost exclusively a matter of state law, but is treated separately here because, unlike the federal and state regulatory regimes above, it is almost entirely a creature of common law. U.S. state law evolved mostly from the English common law and, although tort law has developed and diverged somewhat since the late unpleasantness of the 1770s and 1812, many of the causes of action will be familiar to European lawyers.

Generally speaking, those torts include intrusion upon seclusion or solitude, or into private affairs, public disclosure of embarrassing private facts, and publicity that places a person in a false light in the public eye. The elements of these torts and the standards applicable to each vary among the states.

Because of the First Amendment to the U.S. Constitution and its emphasis on free speech, certain public figures enjoy less protection in tort actions of the kind above. Public officials or other people pervasively involved in public affairs qualify as public figures. Additionally, a person can be a "limited purpose public figure" if he or she has "thrust themselves to the forefront of particular public controversies in order to influence the resolution of the issues involved."

US state law also recognizes the tort of appropriation of name or likeness and several states (notably California (Ca. Civ. Code §§ 3344-3346)) and other states with substantial ties to the entertainment industry) have statutory rights of publicity that permit a famous person to recover for misappropriation of his or her name, voice, signature, photograph, or likeness.

Consistent with the philosophy of the First Amendment, the burden of proof with respect to an invasion of privacy or misappropriation of a right of publicity lies with the plaintiff.

Transfer of Personal Data to and from the U.S.

Very little U.S. law addresses the transfer of personal data of U.S. citizens to other jurisdictions. Absent national security considerations, there is no real prohibition under U.S. law limiting transfers of personal data.

With the exception of the limited circumstances covered by the US-EU Privacy Shield program, the U.S. has not been determined by the European Commission to have "adequate protections" for personal data of EEA member state citizens and, accordingly, transfers of European personal data to the U.S. require the fully informed consent of the data subject or some other mechanism to accomplish legally.

Many U.S. enterprises are certified under the US-EU Privacy Shield, a program administered by the U.S. Department of Commerce. The program requires that enterprises abide by an EC-approved set of privacy principles, specify the data to be transferred (including nature and purpose), and certify such compliance annually. Certifying U.S. enterprises are subject to enforcement by the FTC or the Department of Transportation if they fail to perform as required by the Privacy Shield program.

On October 6, 2015, the European high court invalidated the previous U.S. Safe Harbor program. Although some organizations remain certified under Safe Harbor, that certification no longer supports legal transfers of European personal data and, in fact, representations made by enterprises that the Safe Harbor allows such transfers could result in enforcement for making deceptive statements.

Many U.S. organizations use EC-approved Standard Contractual Clauses to accomplish transfers. Until recently, European enterprises found themselves educating their U.S. counterparts about Standard Contractual Clauses or similar measures. The clauses became much more common during the time between the invalidation of the Safe Harbor and the approval of the Privacy Shield and U.S. enterprises now routinely execute supplementary agreements incorporating the Standard Contractual Clauses.

A relative few U.S. enterprises have put in place approved binding corporate rules and those that have done so are mainly pharmaceutical companies, information technology companies, and financial institutions.

What You Should Do to Create a Comprehensive Privacy and Data Security Program

Below are the steps that organization should take to comply with U.S. privacy laws.

Understand your data.
An organization must understand what information is collected, how it is used, how it is protected, with whom it is shared, and how long it is kept. Creating and maintaining data inventories and data flows are critical to staying on top of this evolving landscape.

Understand your legal and regulatory landscape.
A company's headquarters may be in Hamburg or New York, but its data resides in many different locations. This subjects to organization to many different legal regimes. With so many players, it is very easy for any organizations to stray into regulated space. Therefore, organizations must regularly identify what laws and regulations apply to their data at rest, what they require and be constantly vigilant as they change over time. The summary of U.S. privacy laws above should be the starting point for any compliance program.

Verify that your transfers of data comply with law.
Once an organization has dealt with its data at rest, it must identify its data flows and verify that each flow that crosses an international boundary is authorized (or at least not prohibited).

What do your privacy statements say?
It is not uncommon for organizations to have a number of different internal privacy policies and external privacy statements. Organizations should periodically review their privacy statements and policies to ensure that they accurately reflect the organization's business and are consistent with any relevant laws.

Do you really have consent?
Obtaining consent from data subjects can be a useful tool for organizations. However, particularly under the newly passed GDPR, that consent must be clear and unambiguous. Therefore, organizations should ensure that they are getting proper consent.

Are your certifications up to date?
Many organizations rely on certifications to both attract customers and reduce their legal risk. But organizations must keep those certifications up to date to ensure that they are keeping them current and following all of the necessary rules.

Be careful what you promise.
Several recent enforcement actions brought by the Federal Trade Commission (after a reported breach) and Consumer Financial Protection Bureau (before any breach had occurred) emphasize that organizations must be very careful what they promise their customers. These statements are likely some of the most difficult to police, but pose some of the greatest enforcement risk. To be sure, to the extent that any vulnerabilities are actually discovered, organizations should also review their marketing materials to ensure that there are no promises that are now inaccurate.

Do you have the right technical safeguards?
As discussed above, while many laws and regulations do not require any particular technical requirements, some do. Organizations will need to work closely with their technical team and vendors to ensure compliance.

Preparing for a Possible Breach

The process of dealing with a data breach should begin long before the breach occurs. The United States alone has many different state data breach notification laws and the minutes or hours after discovery of a breach are not the time to begin to determine what those are. Now is the time to make sure that your response plan accurately reflects the technical reality of the organization, as well as complies with all of the new changes in the law. The plan should be well defined, written down and accessible to all of the key players in the event of a data breach. In addition, organizations should prescreen all of the key partners necessary in the event of a breach including qualified outside legal counsel, technical data breach response experts, public relations firms and others.

Organizations should also run mock data breach drills to ensure that the plan can be implemented as drafted. These mock drills can range from tabletop exercises to full blown all-hands-on-deck scenarios. The key is to ensure that all of the pieces are in place for a competent, efficient and manageable response to the breach. Here, outside counsel can be particularly helpful in developing and running the drill and protecting it with the cloak of privilege (in some countries, such a privilege does not attach to communications involving in house counsel). An organization's well-rehearsed response to a breach may play a key role in defending against any future litigation or enforcement actions.

Privacy and data protection are increasingly significant legal risks and the laws in this arena are changing rapidly. With the impending passage of the GDPR, heightened focus on enforcement in the U.S. and risk of data breach (and potential litigation), now is the time to address all of the organizations privacy and data protection issues.

Aaron Charfoos is a member in Dykema's Privacy, Data Security and E-Commerce practice and is an experienced trial lawyer specializing in complex patent, privacy and data protection litigation and counseling. Stephen Tupper is the leader of the Firm's Privacy, Data Security, and E-Commerce practice. He focuses on information technology, outsourcing, electronic commerce, technology development and licensing, privacy and general corporate law matters.

Aaron D. Charfoos
Member
312-627-2573
acharfoos@dykema.com

Stephen L. Tupper
Member
248-203-0895
stupper@dykema.com