Privacy Law Fundamentals and Emerging Issues for IP Lawyers: In-House Counsel's Perspective

What is Data Privacy?

- FIPPS—developed in 1970s from a set of safeguards proposed by US Department of Health, Education, and Welfare and later adopted by OECD
  - **Collection Limitation**
  - **Data Quality**
  - **Purpose Specification**
  - **Use Limitation**
  - **Security Safeguards**
  - **Openness**
  - **Individual Participation**
  - **Accountability**

Privacy in the US

- Privacy has its roots in the US Constitution and privacy case law in the US largely developed through the 4th Amendment, which regulates government intrusion into private affairs
- In 1974, the first US privacy law, The Privacy Act, was passed to govern the collection of personal data by the US government
- The FTC Act prohibits unfair or deceptive commercial practices, including those affecting consumer privacy and data security
- US privacy system is mostly sectoral, meaning it regulates privacy of certain information—health, financial, education, children, telecommunications, etc. though various laws and regulations
- Outside sectoral regimes, US privacy laws focus on consumers' rights and primarily grant "opt-out" rights, like CAN-SPAM
- California passed the first comprehensive state consumer privacy law, followed by CO, VA, UT, and CT with many more bills in state legislatures.

Privacy in EEA and UK

- Privacy is first legislated in the German state of Hesse in 1970, and within the decade many EU member states had national privacy laws
- Privacy laws in Europe developed largely from the UN Convention on Human Rights (1948), which declares privacy a fundamental human right
- EEA and UK have a comprehensive privacy framework, meaning individuals (not consumers) have control over the use of their personal data and primarily focus on “opt-in” rights
- GDPR is the law in EEA, but each individual EEA country can make additional rules, called derogations, and enforce the regulation in its discretion through its supervisory authority
- ePrivacy Directive governs electronic communications through public networks, including the placement of cookies (ePrivacy Regulation still in process to replace and comply w/GDPR)

Privacy in APAC

- There are numerous national laws in place throughout APAC, including China, Singapore, Japan, Australia, and New Zealand. Many of these are closely aligned with aspects of GDPR, such as extraterritoriality, data subject rights, cross-border transfers, and hefty fines
- There are some nuances to APAC privacy regimes that make it important to assess applicable laws individually, such as data localization rules in mainland China, and potential criminal penalties in Hong Kong

China’s Personal Information Protection Law (PIPL)

- Adopted on Aug. 20, 2021, at the 30th Session of the Standing Committee of the 13th national People’s Congress.
- Personal information is defined as any kind of information, electronically or otherwise recorded, related to an identified or identifiable natural person within the People’s Republic of China (PRC).
- Strong data localization provision, requiring that personal information reaching certain quantities be stored within China and that transfer of such data overseas be subject to a security assessment by the Cyberspace Administration of China prior to transfer (Article 40).

Other Data Protection Regimes

- Canada has national and regional privacy laws applicable mostly to consumer and employee personal data. PIPEDA has been in effect for over 20 years and may soon be overhauled.
- Brazil's LGPD closely tracks GDPR but has not been fully operationalized.
- In Argentina, personal data is data of any type that refers to an individual, and is regulated by national law.
- Switzerland's law is generally aligned with GDPR but has some differences.
- Turkey in effect prohibits transfer of personal data outside the country without consent of the data subject.

Privacy Ethics

- We are seeing an increase in the concept of ethics in privacy, and that means regardless of the letter of the law there are becoming de facto expectations about data privacy.
  - Privacy by design
  - Following best practices
  - Codes of ethics and clear usage guidelines

Emerging Issue--Biometrics

- Biometrics typically refer to human biology measurements and behavioral characteristics that can be used to identify a specific individual,
  - Examples are facial geometry, iris scans, voiceprints, and fingerprints, etc.
  - IP lawyers should be attuned to what constitutes biometric data collection so they can identify it early on in product/service development process.
- Illinois, TX, and WA all have biometric privacy laws, but IL BIPA law has a private right of action and is frequently litigated and in the news for large settlements and most recently a $228 million jury verdict.
- IL Supreme Court recently confirmed that each separate violation of BIPA constitutes a distinct and separately actionable violation of the statute.
  - a separate claim accrues each time a private entity scans or transmits an individual's biometric identifier or information in violation of BIPA→ potentially enormous liability for orgs and insurance companies

Emerging Issue—Ideas as Personal Data

- Under U.S. law, you cannot patent an idea.

- Plagiarism
  - Plagiarism is not limited to just words. You can plagiarize an idea, thought or fact (at least one that isn't common knowledge).

- US v. China-Patent and Copyright Wars
  - World Intellectual Property Organization (WIPO) data show that Chinese filers dominate patent applications for inventions, utility models, or designs
  - Three types of patents are granted in China: invention patents, utility model patents and design patents.
    - Over the last several years, there has been a significant increase in applications for ideas or "junk patents" and the numbers coming out of WIPL suggest they are being granted.

BUT, is your idea personal data that is protected under Privacy Laws?

Emerging Issues—AI and Data Ethics

- Ethical use of data and algorithms means working to do the right thing in the design, functionality, and use of data in AI and in general.
  - Evaluate how data is used and what it's used for
  - Who does and should have access
  - Anticipate how data could be misused
  - What data should and should not be connected with other data
  - How to securely store, move, and use it

Ethical use considerations include privacy, bias, access, personally identifiable information, encryption, legal requirements and restrictions, and what might go wrong.

EVEN IF THERE IS NO LAW, RULE OR REGULATION SAYING WE CANNOT USE DATA IN A CERTAIN WAY, WE SHOULD BE ASKING OURSELVES: SHOULD WE BE USING THE DATA THIS WAY?

Privacy Enforcement in US

- Penalties for violation of privacy regulations vary widely
  - TCPA violation between $500 and $1500 per individual
  - Up to $16,000 per email
  - FTC civil penalties range from $43,800 to $46,500 for violations of Section 5
  - Many settlements are in the millions
- US regulators are getting creative in enforcement of privacy laws and indicating they will continue to enact new standards:
  - FTC de facto Breach Notification Requirement (Uber and GoodRx)
  - SEC proposed rule on cybersecurity risk management and incident disclosure by public companies
- Stockholder litigation (Marriott and SolarWinds litigation in Delaware Chancery Court)

Regulatory Movement in EMEA

- Penalties are steep; up to €20 million or 4% worldwide turnover
- Enforcement power is distributed--there are 27 enforcement authorities in EEA
- Regulators are inconsistent, and certain jurisdictions are much stricter in interpreting GDPR
- European Commission has ordered authorities to be more accountable for pending cases against Big Tech in an effort to accelerate dormant cases but also standardize the enforcement of GDPR across the EU bloc
- Many regulators are enforcing cookie consent requirements

Biometric Data Laws: Overview

by Practical Law Data Privacy & Cybersecurity

Maintained • Illinois, Texas, USA (National/Federal), Washington

A Practice Note comparing the biometric data laws in Illinois, Texas, and Washington and recommended best practices to comply with those laws. This Note also includes examples of other states and cities that regulate biometric data in general and sector-specific privacy laws.

Defining Biometrics

Using Biometric Data

Federal Regulation of Biometric Data

State Biometric Data Laws

Scope of Coverage

Definitions

Notice and Consent

Sale, Use, and Disclosure Restrictions

Security Requirements

Storage, Retention, and Destruction

Enforcement

Statute of Limitations

Determining Whether Collector or Possessor Obligations Apply

Additional Laws Affecting Biometric Data

Biometrics typically refer to human biology measurements and behavioral characteristics, such as facial geometry, iris scans, voiceprints, and fingerprints, which an organization can use to identify a specific individual.

Organizations throughout the world increasingly use biometric technology for many reasons, including:

- Enhancing security.

- Verifying the identities of customers and employees.
- Monitoring employee work time.
- Examining consumers' shopping behaviors.
- Facilitating financial and retail transactions.

Biometric data collection, use, disclosure, and storage present challenging privacy and security concerns because individuals cannot change their biometric data. In response to the risks presented by this data, Illinois, Texas, and Washington have adopted the following laws focused specifically on biometric data handling:

- The Illinois Biometric Information Privacy Act (BIPA) (740 ILCS 14/5).
- The Texas Capture or Use of Biometric Identifier Act (CUBI) (Tex. Bus. & Com. Code Ann. § 503.001).
- Washington State's law regarding biometric identifiers (RCW §§ 19.375.010 to 19.375.040) (Washington Biometric Law).

Organizations collecting biometric data should take steps to ensure compliance with these laws, to address regulatory risk and, under BIPA, avoid private lawsuits, by:

- Assessing whether BIPA, CUBI, and the Washington Biometric Law apply to their data collection (see Scope of Coverage and Definitions).
- Determining whether possessor or collector obligations, or both, apply (see Determining Whether Collector or Possessor Obligations Apply).
- Ensuring they comply with notice and consent requirements (see Notice and Consent).
- Implementing security measures to protect biometric data (see Security Requirements).
- Establishing a retention schedule for biometric data (see Storage, Retention, and Destruction).
- Disclosing biometric data only with a permitted statutory basis (see Sale, Use, and Disclosure Restrictions).

Certain other states regulate biometric data in their general or sector-specific privacy laws or data breach notification laws. This Note does not cover in detail other privacy laws that may include biometrics within their scope, but includes examples of those laws (see Additional Laws Affecting Biometric Data).

For more on handling biometrics in the workplace, see Practice Note, Biometrics in the Workplace. For more information on litigation under BIPA, see Practice Note, BIPA Compliance and Litigation Overview.

Defining Biometrics

While there is no universally accepted definition of biometrics, the term usually refers to either:

- Measurable human biological and behavioral characteristics that can be used to identify an individual.
- Automated methods used to recognize individuals based on human biological and behavioral characteristics.

Biometric identifiers include, for example:

- Data captured by:
  - facial recognition technology;
  - iris recognition technology or retinal scans;
  - fingerprints and palm prints;
  - audio recording and voiceprint matching; and
  - genetic testing.
- Measurable behavioral traits that differ among individuals, such as:
  - style or manner of walking, also called gait; and
  - computer keystroke patterns.

For state-specific definitions of biometric data, see Definitions.

Using Biometric Data

Biometric technology has evolved significantly in recent years. Some of the most common uses for biometric technology include:

- **Identifying individuals.** For example, many social media platforms use facial recognition technologies to instantly identify people in photographs and videos.
- **Health and fitness tracking.** Consumer products, such as wearable health trackers, can track and record a person's heart rate, activity level, gait, sleep quality, and more.

- **Identity authentication for transactions.** Many consumer-facing organizations, like banks and retailers, rely on biometric identity verification using fingerprints and other identifiers to authenticate a consumer's identity and complete financial transactions.

- **Enhancing corporate security.** Organizations increasingly use biometric technology for internal operational security purposes, such as:
    - retina and hand scanning for highly secured areas; and
    - collecting and maintaining fingerprint data for background investigations.

- **Timekeeping for employees.** This includes using fingerprints, hand scanning, or other biometric technologies to allow employees to punch in and out on biometric timeclocks to reduce time theft and "buddy punching," the practice of one employee clocking in for another employee.

- **Enhancing security of remote work.** This includes establishing biometric access controls, such as fingerprint scanning or facial recognition technology, on employer-provided laptops, smartphones, tablets, and company networks.

Federal Regulation of Biometric Data

No federal law directly addresses the collection, use, storage, and disclosure of biometric data. However, **Section 5 of the Federal Trade Commission (FTC) Act** gives the FTC broad authority to protect consumers from unfair and deceptive trade practices in or affecting commerce (15 U.S.C. § 45(a)(1) to (a)(2)).

Under that authority, the FTC may take enforcement action against commercial organizations that engage in unfair and deceptive practices involving biometric data. If an organization that collects and uses biometric data fails to keep its promises to consumers regarding its handling of that data, it risks an FTC enforcement action.

For example, in early 2021, the FTC settled with Everalbum, Inc., a California-based developer of a photo storage app over allegations that it deceived consumers about its use of facial recognition technology. Everalbum enabled a facial recognition feature in its app by default for most users and did not provide a way for users to turn off the feature, which violated its own stated policies. The settlement order required Everalbum to:

- Delete the photos and videos of app users who deactivated their accounts and the models and algorithms it developed by using the photos and videos uploaded by its users.

- Stop misrepresenting how it collects, uses, discloses, maintains, or deletes personal information and the extent to which it protects privacy and security.

- Obtain users' express consent before using facial recognition technology on their photos and videos.

For more on this settlement, see Legal Update, FTC Announces Settlement with Photo Storage App Company Over Improper Facial Recognition Use Allegations and FTC Finalizes Settlement with Photo App Developer Related to Misuse of Facial Recognition Technology, 2021 WL 1827334 (F.T.C. News Release May 7, 2021).

The FTC has also issued recommendations for companies on using facial recognition technology (see FTC: Facing Facts: Best Practices for Common Uses of Facial Recognition Technologies (2012)).

In addition, several other federal statutes address privacy in various contexts which may overlap with biometrics. For example:

- The **Health Insurance Portability and Accountability Act** (HIPAA) addresses requirements for protecting individually identifiable health information and protected health information (see Practice Note, HIPAA Privacy Rule).
- The **Genetic Information Nondiscrimination Act** (GINA) prohibits employers from requesting, requiring, or buying an employee's genetic information or that of an employee's family member (see Practice Note, Discrimination Under GINA: Basics).

State Biometric Data Laws

BIPA, CUBI, and the Washington Biometric Law are the three state laws focused specifically on biometric data. The requirements under these laws vary but they include provisions on:

- The scope of coverage (see Scope of Coverage).
- Important definitions (see Definitions).
- Notice and consent requirements (see Notice and Consent).
- Restrictions on sale, use, and disclosure of biometric data (see Sale, Use, and Disclosure Restrictions).
- Security requirements (see Security Requirements).
- Storage, retention, and destruction requirements (see Storage, Retention, and Destruction).
- Enforcement (see Enforcement).

BIPA, CUBI, and the Washington Biometric Law all impose distinct obligations on persons or entities that collect biometric data versus those that "possess" biometric data (see Determining Whether Collector or Possessor Obligations Apply).

Persons and entities subject to BIPA, CUBI, and the Washington Biometric Law must also understand the statute of limitations for private or regulator actions under the laws (see Statute of Limitations).

Scope of Coverage

The scope of coverage under BIPA, CUBI, and the Washington Biometric Law are similar, but the laws differ in the following respects:

- BIPA broadly applies to private entities collecting or possessing biometric identifiers or biometric information, while CUBI and the Washington Biometric Law only apply to biometric identifiers collected or possessed for commercial purposes (for more on the definition of biometric identifiers and biometric information see Definitions).
- Unlike BIPA and the Washington Biometric Law, CUBI does not specify the persons and entities subject to the law. CUBI also provides fewer exceptions from the law than BIPA and the Washington Biometric Law.
- The Washington Biometric Law specifically applies to biometric identifiers enrolled for a commercial purpose (for more on the definition of "enrolled" see Washington).

If an organization collects, uses, stores, or possesses biometric data, it should consider the following factors to assess whether BIPA, CUBI, or the Washington Biometric Law applies:

- Whether the biometric data originated from Illinois, Texas, or Washington.
- If the organization collects, possesses, uses, or stores biometric data in Illinois, Texas, or Washington.
- Where the organization collecting, possessing, using, or storing biometric data does business, or whether the organization is incorporated, or registered to do business, in Illinois, Texas, or Washington.
- Whether the organization collecting biometric data targets online or cloud-based services or products in Illinois, Texas, or Washington.

The organization should also consider:

- The applicable laws' scope and biometric data definition (see Definitions).
- Whether any exclusions under the biometric data laws apply (see Scope of Coverage and Definitions).
- The purposes for biometric data collection, use, storage, and possession and whether the organization collects biometric data for commercial purposes under CUBI or the Washington Biometric Law (see Scope of Coverage and Definitions).
- Whether the biometric data qualifies as an enrolled biometric identifier collected for a commercial purpose under the Washington Biometric Law (see Scope of Coverage).

Illinois

BIPA applies to private entities including:

- Individuals.
- Partnerships, corporations, or limited liability companies.
- Associations or other groups, however organized.

(740 ILCS 14/10.)

BIPA does not cover:

- State or local government agencies or their contractors, subcontractors, and agents.
- Any court of Illinois, court clerk, or judge.
- A financial institution or affiliate of a financial institution covered by the **Gramm-Leach-Bliley Act** (GLBA) and its rules.
- The information excluded from the definition of biometric identifiers and biometric information (see Definitions).

(740 ILCS 14/10.)

Texas

CUBI applies to the collection and possession of biometric identifiers for a commercial purpose (Tex. Bus. & Com. Code Ann. § 503.001(b)). However, CUBI does not define commercial purpose or specify the persons and entities the law covers.

CUBI excludes from its scope voiceprint data retained by financial institutions or their affiliates as defined under the GLBA (Tex. Bus. & Com. Code Ann. § 503.001(e)).

Washington

The Washington Biometric Law covers all individuals and legal entities except:

- Government agencies.
- Financial institutions and affiliates subject to the GLBA.
- Activities subject to HIPAA.

- Law enforcement activity.

(RCW §§ 19.375.010(7) and 19.375.040.)

The Washington Biometric Law limits its coverage to biometric identifiers (see Definitions) that are both:

- Enrolled, meaning the process of:
  - capturing or collecting a biometric identifier;
  - converting the biometric identifier into a reference template that cannot be reconstructed into the original output image; and
  - storing it in a database that matches the identifier to a specific individual.
- Used for a commercial purpose (see Definitions).

(RCW §§ 19.375.010(5) and 19.375.020(1).)

The law does not apply to the disclosure or retention of biometric identifiers that:

- Have been unenrolled.
- Are used to support a "security purpose," defined as:
  - preventing shoplifting, fraud, or other misappropriation or theft; and
  - other purposes to protect the security or integrity of software, accounts, applications, online services, or any person.

(RCW §§ 19.375.010(8) and 19.375.020(6), (7).)

Definitions

The defined terms in BIPA, CUBI, and the Washington Biometric Law differ in the following respects:

- BIPA defines and includes biometric identifiers and biometric information, while CUBI and the Washington Biometric Law only define and include biometric identifiers.
- CUBI does not define commercial purpose, which differs from the Washington Biometric Law.

- BIPA and the Washington Biometric Law exclude more information from their biometric data definitions than CUBI.

Illinois

BIPA covers biometric identifiers and biometric information.

Biometric identifiers include:

- Retina or iris scans.
- Fingerprints.
- Voiceprints.
- Scans of hand or face geometry.

(740 ILCS 14/10.)

BIPA's biometric identifier definition specifically excludes certain information, including:

- Writing samples and written signatures.
- Photographs.
- Human biological samples used for valid scientific testing or screening.
- Demographic data.
- Tattoo descriptions.
- Physical descriptions such as:
    - height;
    - weight;
    - hair color; or
    - eye color.
- Information:

- captured from a patient in a healthcare setting; or
- collected, used, or stored for healthcare treatment, payment, or operations under HIPAA.

(740 ILCS 14/10.)

Although the biometric identifier definition excludes photographs, most courts have determined that scans of photographs for facial geometry qualify under the biometric identifier definition (see, for example, *Monroy v. Shutterfly*, 2017 WL 4099846, at *1 (N.D. Ill. Sept. 15, 2017) ("[T]he court sees nothing in BIPA's statutory text to indicate that it lacks application" to Shutterfly's highly detailed facial maps derived from user-uploaded photographs); *Rivera v. Google Inc.*, 238 F. Supp. 3d 1088, 1096 (N.D. Ill. 2017) ("[I]f Google simply captured and stored the photographs and did not measure and generate scans of face geometry, then there would be no violation of the Act."); cf. *Gullen v. Facebook, Inc.*, 2018 WL 1609337 (N.D. Cal. Apr. 3, 2018), *aff'd*, 772 F. App'x 481 (9th Cir. 2019) (granting Facebook's summary judgment motion because the plaintiff failed to show a genuine dispute on whether Facebook ran facial recognition on the plaintiff's photo)).

BIPA defines biometric information as any information based on an individual's biometric identifier used to identify an individual (740 ILCS 14/10). For example, if an organization converts a biometric identifier into another form, such as a mathematical representation or a unique number assigned to the biometric identifier, that other form qualifies as biometric information under BIPA if it can still identify the person (see *Rivera*, 238 F. Supp. 3d at 1095).

Biometric information includes information such as:

- Converting iris image scans into "iris codes" for an iris-recognition system (see *Rivera*, 238 F. Supp. 3d at 1095 n.6).
- An electronically stored version of scanned and collected thumbprints (see *Rosenbach v. Six Flags Ent. Corp.*, 2019 IL 123186, ¶ 18).

Biometric information excludes information derived from the same items or procedures excluded under the definition of biometric identifier (740 ILCS 14/10).

Texas

Under CUBI, biometric identifiers include:

- Retina or iris scans.
- Fingerprints.
- Voiceprints (except voiceprint data retained by financial institutions or their affiliates under the GLBA).
- Records of hand or face geometry.

(Tex. Bus. & Com. Code Ann. § 503.001(a).)

CUBI is narrower than BIPA because it only applies to biometric identifiers:

- And not biometric information.
- Captured for a commercial purpose (Tex. Bus. & Com. Code Ann. § 503.001(b)).

CUBI does not define the term "commercial purpose."

CUBI recognizes that biometric identifiers may be collected "for security purposes by an employer," but does not specify whether a security purpose constitutes a commercial purpose (Tex. Bus. & Com. Code Ann. § 503.001(c)(3)(c-2)).

Washington

Under the Washington Biometric Law, biometric identifiers are data generated by automatic measurements of an individual's biological characteristics such as:

- Fingerprints.
- Voiceprints.
- Retinal or iris scans.
- Other unique biological patterns or characteristics used to identify an individual.

(RCW § 19.375.010(1).)

The Washington Biometric Law definition excludes:

- Physical or digital photographs.
- Video or audio recordings, and data generated therefrom.
- Information collected, used, or stored for health care activities regulated under HIPAA.

(RCW § 19.375.010(1).)

The Washington Biometric Law is narrower than BIPA because it only applies to biometric identifiers:

- And not biometric information.
- Collected or used for a commercial purpose.

(RCW § 19.375.020(1).)

Unlike CUBI, the Washington Biometric Law defines "commercial purpose" as:

- The sale or disclosure of a biometric identifier to a third party for marketing goods or services that are unrelated to the initial transaction in which the person obtained the biometric identifier.
- Excluding biometric identifiers collected for a security purpose (as defined in RCW § 19.375.020(7)) or law enforcement purpose.

(RCW §§ 19.375.010(4), (8) and 19.375.020(7).)

Notice and Consent

BIPA, CUBI, and the Washington Biometric Law all include notice and consent requirements. However:

- Unlike CUBI and the Washington Biometric Law, BIPA requires notice and consent to be in writing.
- In contrast to CUBI and the Washington Biometric Law, BIPA specifies the information that organizations must include when providing notice that they collect biometric identifiers and biometric information.
- BIPA requires organizations collecting biometric identifiers and biometric information to develop a publicly available written policy containing certain information, while CUBI and the Washington Biometric Law do not include a similar requirement.
- The Washington Biometric Law is less restrictive than BIPA and CUBI because it does not require organizations to provide notice and obtain consent to enroll a biometric identifier in all cases.

Organizations should ensure they implement a system for providing and tracking notice and obtaining consent. This can be done electronically, for example, before collecting a fingerprint scan by providing an electronic notice and consent where the individual clicks a box to consent.

Organizations should also implement a system for storing notices and consents obtained under any applicable statute of limitations (see Statute of Limitations).

Illinois

If a private entity collects, captures, receives through trade, or otherwise obtains biometric identifiers or biometric information, it must:

- Notify each individual or their authorized representative in writing:
  - that the organization collects or stores biometric identifiers or biometric information;

    - about the purposes for collecting, storing, and using the biometric identifiers or biometric information; and
    - how long the organization uses or stores the biometric identifiers or biometric information.

- Receive the individual's or their legal representative's written release to collect biometric identifiers or biometric information.
- Develop a publicly available written policy that includes:
    - a retention schedule; and
    - guidelines for permanently destroying the biometric identifiers and biometric information when the initial collection purpose no longer exists or within three years of an individual's last interaction with the private entity, whichever is earlier.

(740 ILCS 14/15(a), (b).)

A "written release" means an "informed written consent" or, in the employment context, "a release executed by an employee as a condition of employment" (740 ILCS 14/10). For more on handling biometric data in the workplace, see Practice Note, Biometrics in the Workplace.

Texas

Before a person or entity "captures" a biometric identifier for a commercial purpose, CUBI requires them to:

- Notify individuals.
- Receive the individuals' consent to capture the biometric identifier.

(Tex. Bus. & Com. Code Ann. § 503.001(b).)

Unlike BIPA, but like the Washington Biometric Law, CUBI does not require notice or consent to be in writing. CUBI does not specify what must be included in the notice.

Washington

Under Washington's Biometric Law, covered persons cannot enroll a biometric identifier in a database for a commercial purpose without first doing one of the following:

- Providing notice.

- Obtaining consent.
- Providing a mechanism to prevent the later use of a biometric identifier for a commercial purpose.

(RCW § 19.375.020(1).)

The type of notice and consent required to comply with the Washington Biometric Law is context dependent. Notice is specifically defined as a disclosure reasonably designed to be readily available to the affected persons (RCW § 19.375.020(2)).

Unlike BIPA, but like CUBI, the Washington Biometric Law does not require that notice and consent be in writing.

However, notice and consent are not required to enroll a biometric identifier and store it in a biometric system to support a security purpose to either:

- Prevent:
  - shoplifting;
  - fraud; or
  - any other misappropriation or theft of a thing of value, including tangible and intangible goods and services.
- Protect the security or integrity of:
  - software;
  - accounts;
  - applications;
  - online services; or
  - any person.

(RCW §§ 19.375.010(8) and 19.375.020(7).)

A biometric system is an automated identification system that can do all the following:

- Capture, process, and store biometric identifiers.
- Compare biometric identifiers to references.

- Match biometric identifiers to individuals.

(RCW § 19.375.010(5).)

Sale, Use, and Disclosure Restrictions

BIPA, CUBI, and the Washington Biometric Law all restrict the sale, use, and disclosure of biometric data. Key differences between the laws include:

- Unlike CUBI and the Washington Biometric Law, BIPA prohibits the sale, lease, trade, or profiting from biometric identifiers or biometric information under any circumstance, including with the individual's consent. However, organizations may disclose, redisclose, or disseminate biometric identifiers or biometric information under BIPA for other purposes if they meet an exception.

- CUBI and the Washington Biometric Law allow organizations to sell, lease, or disclose biometric data if they meet an exception such as consent. However, the Washington Biometric Law allows for these disclosures with an individual's general consent, while CUBI only allows individuals to consent for identification purposes if they die or disappear.

Organizations subject to BIPA, CUBI, and the Washington Biometric Law must implement a system to ensure they do not:

- Disclose biometric data unless a statutory exception applies.

- Sell or otherwise profit from biometric data in the organization's possession unless a statutory exception applies.

The exceptions under each law differ so organizations must understand when the laws permit or restrict disclosures.

Illinois

Entities in possession of biometric identifiers or biometric information must not:

- Sell, lease, trade, or otherwise profit from an individual's biometric identifier or biometric information. BIPA does not provide for consent as an exception.

- Disclose, redisclose, or disseminate an individual's biometric identifier or biometric information, including to a third-party service provider, unless:

    - the individual or their legal representative consents to the disclosure or redisclosure;

    - the disclosure or redisclosure completes a financial transaction requested or authorized by the individual or the individual's legally authorized representative;

- state or federal law or municipal ordinance requires the disclosure; or
- a valid warrant or subpoena issued by a court of competent jurisdiction requires the disclosure.

(740 ILCS 14/15(a), (c), and (d).)

Texas

Unlike BIPA, but like the Washington Biometric Law, CUBI does not outright ban the sale of biometric identifiers if the person or entity satisfies a statutory exception.

Persons or entities in possession of biometric identifiers captured for a commercial purpose must not sell, lease, or otherwise disclose biometric identifiers unless either:

- The individual consents to the disclosure for identification purposes if the individual disappears or dies.
- The disclosure completes a financial transaction the individual requested or authorized.
- A federal or state statute, other than Chapter 552, Texas Government Code, permits the disclosure.
- The disclosure is made by or to a law enforcement agency for law enforcement purposes in response to a warrant.

(Tex. Bus. & Com. Code Ann. § 503.001(c).)

The consent for disclosure exception under CUBI is narrower than the consent exception under BIPA and the Washington Biometric Law.

Washington

Under the Washington Biometric Law, organizations cannot sell, lease, or disclose biometric identifiers that the organization enrolled for a commercial purpose to another person unless either:

- The individual consents to the sale, lease, or disclosure.
- The sale, lease, or disclosure is:
  - compliant with the law's requirements;
  - necessary to provide a product or service subscribed to, requested, or authorized by the individual;

- necessary to carry out, administer, enforce, or complete a financial transaction the individual requested or authorized, and the third-party recipient will not further disclose the biometric identifier unless authorized by the law;
- required or authorized by a federal or state statute or court order;
- made to a third party who contractually agrees not to further disclose and enroll the biometric identifier for a commercial purpose unless the disclosure complies with the notice and consent requirements of the law; or
- made for litigation purposes or to participate in the judicial process.

(RCW § 19.375.020(3).)

The disclosure limitations do not apply to biometric identifiers that have been unenrolled (RCW § 19.375.020).

Persons and entities that enroll a biometric identifier for a commercial purpose cannot use or disclose the identifier in a way that is materially inconsistent with the initial collection purpose without obtaining consent for the new use or disclosure (RCW § 19.375.020(5)).

Security Requirements

BIPA, CUBI, and the Washington Biometric Law all require persons and entities to protect biometric data using a reasonable standard of care. However, the laws do not define or provide guidance on what constitutes reasonable data security.

Organizations should conduct due diligence to ensure that they comply with any data security standards applicable to their industry and other generally recognized data security standards to protect biometric data.

For more on the reasonableness standard for data security measures commonly used in federal and state laws, see Practice Notes, State Data Security Laws: Overview and FTC Data Security Standards and Enforcement.

Illinois

Private entities must store, transmit, and protect from disclosure all biometric identifiers or biometric information in their possession:

- Using the reasonable standard of care in the organization's industry.
- In a manner that is the same or more protective than that used to store, transmit, and protect other confidential and sensitive information.

(740 ILCS 14/15(e).)

BIPA defines confidential and sensitive information as personal information that can uniquely identify an individual's account or property, such as:

- A genetic marker.
- Genetic testing information.
- A unique identifier number to locate an account or property.
- An account number.
- A PIN number.
- A passcode.
- A driver's license number.
- A Social Security number.

(740 ILCS 14/10.)

Texas

CUBI requires persons and entities that possess a biometric identifier captured for a commercial purpose to protect the identifiers in storage and transmission, using reasonable care and in a manner that is the same or more protective than that used for other confidential information (Tex. Bus. & Com. Code Ann. § 503.001(c)(2)).

Washington

Under the Washington Biometric Law, persons or entities who knowingly possess a biometric identifier that has been enrolled for a commercial purpose must take reasonable care to protect the identifiers against unauthorized access or acquisition (RCW § 19.375.020(4)(a)).

Storage, Retention, and Destruction

BIPA, CUBI, and the Washington Biometric Law all require the destruction of biometric data after a certain time, but no later than when the initial collection purpose ends.

Organizations should decide on a retention schedule and implement a system to ensure it destroys biometric data in the required timeframe. For example, if:

- An organization requires customers to scan fingerprints for entry to an amusement park, it can arguably retain that data for the duration of the amusement park season.

- An employer captures an employee's biometric data for security purposes, the purpose typically expires on termination of the employment relationship (see, for example, Tex. Bus. & Com. Code Ann. § 503.001(c-1) and (c-2)). For more information on handing biometrics in the workplace, see Practice Note, Biometrics in the Workplace.

To ensure they comply with retention obligations, organizations should retain an outside vendor or work closely with their information technology department.

Illinois

Under BIPA, private entities in possession of biometric identifiers or biometric information must develop a publicly available written policy that includes:

- A retention schedule.

- Guidelines for permanently destroying the biometric identifiers or biometric information after whichever occurs first:
    - the initial collection purpose no longer exists; or
    - within three years of an individual's last interaction with the private entity.

(740 ILCS 14/15(a).)

Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity must comply with its established retention schedule and destruction guidelines (740 ILCS 14/15(a)).

Texas

Under CUBI, persons or entities that possess biometric identifiers captured for a commercial purpose must destroy those identifiers within a reasonable time, but no later than one year after the collection purpose ends, with limited exceptions. If an employer captures an employee's biometric identifier for security purposes, the purpose for collecting the identifier presumably expires on termination of the employment relationship. (Tex. Bus. & Com. Code Ann. § 503.001 (c)(3), (c-1), and (c-2).)

Washington

The retention requirements under the Washington Biometric Law are similar to those under BIPA and CUBI. A person or entity that knowingly possesses a biometric identifier covered by the statute may retain the identifiers for no longer than reasonably necessary to:

- Provide the services for which the identifier was enrolled.
- Comply with retention requirements under law or court order.
- Protect against or prevent fraud, criminal activity, liability, or security threats.

(RCW § 19.375.020(4)(b).)

Enforcement

BIPA differs from CUBI and the Washington Biometric Law because it provides a private right of action. The attorneys general have the authority to enforce CUBI and the Washington Biometric Law.

Illinois

BIPA provides a private right of action as an enforcement mechanism (740 ILCS 14/20). The plaintiff may seek to recover:

- For each negligent violation, the greater of:
  - liquidated damages of $1,000; or
  - actual damages.
- For each intentional or reckless violation, the greater of:
  - liquidated damages of $5,000; or
  - actual damages.
- Reasonable attorneys' fees and costs.
- Injunctive or other appropriate relief.

(740 ILCS 14/20.)

For more on BIPA enforcement, see Practice Note, BIPA Compliance and Litigation Overview: BIPA Enforcement.

Texas

Unlike BIPA, CUBI does not provide a private right of action. The Texas Attorney General has the sole authority to enforce CUBI and may bring suit to recover civil penalties of up to $25,000 per violation (Tex. Bus. & Com. Code Ann. § 503.001(d)).

In 2022, the Texas Attorney General filed a lawsuit against Meta Platforms, Inc. for alleged violations claiming that it:

- Unlawfully captured the biometric identifiers of Texans for a commercial purpose without their informed consent, disclosed those identifiers to others, and failed to destroy collected identifiers within a reasonable time in violation of CUBI.
- Engaged in false, misleading, and deceptive acts and practices in violation of the Texas Deceptive Trade Practices-Consumer Protection Act (Tex. Bus. & Com. Code §§ 17.41 to 17.63).

Washington

Like CUBI, the Washington Attorney General has the sole power to enforce the Washington Biometric Law.

However, it potentially creates the greatest monetary exposure. The Washington Biometric Law provides for the same remedies available under Washington law for an unfair or deceptive act or method of competition, which carries penalties up to:

- $180,000 for individuals.
- $900,000 for legal and corporate entities.

(RCW §§ 19.86.140 and 19.375.030(2).)

Statute of Limitations

Illinois

BIPA does not specify a statute of limitations. However, under Illinois law:

- A one-year statute of limitations applies to actions for slander, libel, or publication of matters violating the right of privacy (735 ILCS 5/13-201).
- A two-year statute of limitations applies to actions for a "statutory penalty" or personal injury claims (735 ILCS 5/13-202).
- A five-year catch-all statute of limitations applies to all other civil actions not covered by the one- and two-year statute of limitation provisions (735 ILCS 5/13-205).

Defendants routinely argue that courts should apply the one-year limitations period for privacy violation claims. Alternatively, they have argued for the two-year limitations period applicable to both statutory penalties and personal injury claims (see, for example, *Burlinski v. Top Golf USA Inc.*, 2020 WL 5253150, at *6-8 (N.D. Ill. Sept. 3, 2020); see also *Tims v. Black Horse Carriers, Inc.*, 2021 IL App (1st), 200563, ¶ 31 (appellate court concluded that the applicable limitations period varies depending on whether the duty violated involves an "element of publication or dissemination")).

For a further discussion on the statute of limitations under BIPA, see Practice Note, BIPA Compliance and Litigation Overview: Statute of Limitations.

Texas

CUBI does not specify a statute of limitations for the Texas Attorney General to bring an action. However, the Texas law governing the statute of limitations for civil actions provides for a two-year limitation period for conversion of personal property, the taking or detaining of the personal property of another, and personal injury, which may arguably apply for CUBI actions (see Tex. Civ. Prac. & Rem. Code Ann. § 16.003).

Washington

The Washington Biometric Law does not specify a statute of limitations for the Washington Attorney General to bring an action. However, the law gives the Attorney General enforcement power under the Washington State Consumer Protection Act (RCW § 19.375.030(2)).

Any action to enforce a claim for damages under the Consumer Protection Act must be commenced four years after the cause of action accrues (RCW § 19.86.120).

Determining Whether Collector or Possessor Obligations Apply

BIPA, CUBI, and the Washington Biometric Law impose specific obligations on persons or entities "in possession" of biometric data versus those that collect biometric data. Private entities may have both collector and possessor obligations. However, collector obligations exceed possessor obligations.

Under BIPA, private entities in possession of biometric identifiers or biometric information must:

- Not disclose or otherwise disseminate it except under certain circumstances (see Sale, Use, and Disclosure Restrictions).
- Develop publicly available retention schedules and destruction deadlines (see Storage, Retention, and Destruction).
- Satisfy BIPA's security requirements (see Security Requirements).

Similarly, under CUBI, persons or entities in possession of biometric identifiers captured for a commercial purpose must:

- Not disclose the identifier unless they satisfy a statutory exception (Sale, Use, and Disclosure Restrictions).
- Comply with the retention and destruction requirements (Storage, Retention, and Destruction).
- Satisfy CUBI's security requirements (Security Requirements).

Under the Washington Biometric Law, persons or entities who knowingly possess a biometric identifier that has been enrolled for a commercial purpose must:

- Satisfy the retention requirements (see Storage, Retention, and Destruction).
- Comply with the security requirements (see Security Requirements).

Organizations must analyze whether they collect or possess biometric data or both. In Illinois, case law can help organizations assess what constitutes possession of biometric identifiers or biometric information. For example, the Illinois Supreme Court has held that possession "occurs when a person has or takes control of the subject property or holds the property at his or her disposal" (*People v. Ward*, 215 Ill. 2d 317, 325 (2005); see also *Heard v. Becton, Dickinson & Co.*, 440 F. Supp. 3d 960, 968 (N.D. Ill. 2020) (court found that the plaintiff failed to adequately plead "possession" because, among other things, the complaint contained no allegations regarding defendant's dominion or control over the biometric data)).

However, there are no reported cases or guidance on the meaning of possession under CUBI or the Washington Biometric Law. Organizations may therefore decide that compliance with both collector and possessor obligations under these laws is the best way to protect against regulatory action.

If a third-party vendor offers biometric technology or services to customers collecting biometric data in Illinois, Texas, or Washington, it may be a possessor under the laws. These third parties and their customers should address any potential obligations through contractual clauses by examining:

- Whether the customer collects biometric data in Illinois, Texas, or Washington.
- Which party must comply with all obligations under applicable laws.
- Whether the contract should include indemnification clauses, such as requiring reimbursement for lawsuits, regulatory inquiries, and any other costs associated with biometric data law violations.
- Whether the clients or third-party vendors have adequate insurance to cover biometric data claims and violations.

Additional Laws Affecting Biometric Data

Although only three states have enacted comprehensive statutes addressing biometric data handling, many states regulate some aspect of biometric data in other ways. For example:

- Certain states have legislated aspects of biometric data, including in:
    - the employment context;
    - identity theft protection laws; and
    - the laws applicable to biometric data collection by public schools.

  For more on these laws, see Practice Note, Biometrics in the Workplace: Additional Laws Affecting Biometric Information.

- Certain states include an individual's unique biometric data in the definition of personal information found in their general data breach notification statutes. For more information on data breach notification laws that include biometric data in the definition of personal information, see Practice Note, State Data Breach Laws Protected Personal Information Chart: Overview.

- California, Colorado, Connecticut, Virginia, and Utah have enacted comprehensive privacy laws that include biometric information in the definition of personal information (see Cal. Civ. Code § 1798.140(b); Colo. Rev. Stat. Ann. § 6-1-716(1)(a); Connecticut Data Privacy Act (S.B. 6) (effective July 1, 2023); Va. Code Ann. § 59.1-575 (effective Jan. 1, 2023); Utah Consumer Privacy Act § 13-61-101(6)(b) (effective Dec. 31, 2023)).

In addition, several US cities have adopted ordinances governing biometric data, including New York City, Portland, and Baltimore. For example, New York City's biometrics identifier law (N.Y.C. Admin. Code §§ 22-1201 to 22-1205) requires certain commercial establishments to provide notice of their biometric data collection and use practices and prohibits the sale of biometric data. For more information on the Baltimore and Portland ordinances, see Legal Updates, Baltimore Enacts Facial Recognition Moratorium and Portland, Or. Bans Private Entity Use of Face Recognition Technologies in Public Spaces.

Mobile App Privacy Compliance Checklist

by Richard Raysman, Holland & Knight LLP, Christopher G. Cwalina and Steven B. Roosa, Norton Rose Fulbright, with Practical Law Data Privacy & Cybersecurity

Maintained • USA (National/Federal)

A Checklist setting out key measures for addressing end-user privacy and security considerations when developing and distributing a mobile application (app). This Checklist provides a general framework for mobile apps and highlights the particular issues a mobile app developer must consider based on the specific app and its business, including the types of information it will collect, the target audience (for example, children), and whether the app includes third-party content or advertising.

Begin with Privacy and Security by Design

Privacy by Design

Consider and address consumer privacy protections throughout the organization. This should include addressing privacy at every stage of mobile application (app) development and deployment. Specifically, the company should:

- Not collect information it does not need (see Know the Business Rationale).
- Enable consumer choice and opt-outs of data collection or disclosure, where possible.
- Provide for secure transmission and storage of **personal information** and device identifiers.
- Implement reasonable data retention and disposal policies.
- Take steps to ensure the information the company maintains is accurate.
- Make privacy the default setting.
- Embed privacy within the design as a core element of the functionality.

(For a detailed discussion of the **Federal Trade Commission** (FTC) privacy by design principles, see FTC Report: Protecting Consumers in an Era of Rapid Change.)

Security by Design

Begin with security in mind. The company should:

- Develop and implement a comprehensive information security program for user information.
- Identify key individuals or groups responsible for:
    - maintaining custody and security of user information;
    - monitoring practices to ensure compliance; and
    - managing and responding to security related operating system updates and patches.
- Develop meaningful procedures for addressing violations.
- Conduct periodic reviews and audits to identify breaches and vulnerabilities.
- Routinely review and update the program as necessary to address vulnerabilities and account for developments in technology and market practices.
- Designate an administrative user with the power to remove files, threats, or users that do not belong in the system.
- Consider industry recommendations. For example, NowSecure, a mobile security firm, publishes a Secure Mobile Development Guide (registration required).

For a checklist identifying key security compliance considerations, see Common Gaps in Information Security Compliance Checklist. For additional resources, see Information Security Toolkit.

Broadly Consider both Traditional and Non-Traditional Types of Personal Information

Ensure privacy and security measures and disclosures address as personal information:

- Information traditionally considered to be personally identifying, including name and contact information.
- Information reasonably capable of identifying or linking to a particular individual or device.

- Files stored on a mobile device that the app may access, including, for example:
    - photos;
    - audio and video files; and
    - address book and calendar information.
- Global positioning system (GPS) or other **geolocation information**.
- Hardware identifiers, internet protocol (IP) addresses, and other information that may identify a particular device.
- Tracking information.
- Banking information, such as ATM card and financial statements and credit reports.
- Federal benefit program information such as **Medicaid**, **Medicare**, and Social Security.

Know the Business Rationale

- Only collect and share information where there is an articulated business reason for doing so.
- Ensure that each piece of information collected is necessary for the functions and activities of your business.
- Don’t collect personal information because you think it may be useful in the future.
- Document in writing:
    - the business need for collecting or sharing certain categories of information; and
    - the privacy protections and safeguards to be employed.

Maintain Technical and Legal Control

Take into account all persons and entities involved in developing the app or who otherwise may have access to or custody of a user's information to ensure:

- The company's privacy policies accurately and completely disclose its information practices.

- The company implements proper controls throughout the entire chain of custody for the information.

Technical Control

To maintain technical control over information collected through the app:

- Understand the source of all software code in the app's supply chain. In particular, require both in-house and third-party software developers to disclose:
  - the existence of all third-party code included in the mobile app's **source code**;
  - the function of the third-party code;
  - all ways, if any, the third-party code may automatically collect, use, store, or share information;
  - the third-party network traffic the code may trigger; and
  - whether the third-party code will modify the device settings or place icon on the mobile desktop.

- Consider possible information collection by:
  - mobile device and platform providers;
  - mobile carriers; and
  - mobile advertisers.

- Maintain records of all potential data collection, use, storage, and disclosure through the app.

Legal Control

- Identify all persons and entities that may collect or have access to information through the app, including, for example:
  - in-house and third-party app developers;
  - advertising networks serving ads to the app;
  - digital content providers; and

    - service providers (for example, third-party hosting and analytics providers).

- Conduct due diligence to understand a third party's information practices and vulnerabilities before:
    - engaging the third party to provide services for the app; or
    - allowing the third party to provide content (including advertising) to the app.

- Enter into signed contracts requiring these persons and entities to adhere to the company's privacy practices, at a minimum, or more restrictive practices established for third-party collection and use. Seek liberal rights to audit compliance and other contractual protections.

Commission Privacy Reviews or Audits

- Perform a privacy review of the actual network traffic associated with the app. Assume it will be tested by a sophisticated third party and that any vulnerabilities identified may expose the company to liability or adverse media attention.

- Have a privacy review performed of the app's local, app-specific storage.

Provide Users with Choice

For all information users are asked to provide, determine whether the information is:

- Generally necessary for accessing and using the app.

- Necessary for only certain nonessential features.

- Not necessary.

Requested Information

- When the user is asked to provide information:
    - limit the information requested to the information that is necessary; and

- identify whether each requested item is required or discretionary. This may also include presenting required fields with an asterisk or in a different color.

- Consider requesting information that is necessary for certain features only when the user accesses or uses those features.

Information Collected Automatically

- For all information the app may collect using automatic data collection, disclose in published privacy policies:
  - the methods that may be used to collect information;
  - the information that may be collected; and
  - whether and, if so, how the users can prevent the information from being collected, used, or disclosed.

- When possible, enable end users to choose whether certain of their information will be:
  - collected;
  - used for all or certain purposes; or
  - shared with others.

Comply with State or Industry-Specific Laws

- Consider whether the app may be subject to specific regulations based on, for example, the app's:
  - industry;
  - features and purposes; or
  - target audience.

- In particular, if the app:
  - collects information from California residents, consider the California Consumer Privacy Act of 2018 (CCPA) (see Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy

Rights Act (CPRA)) and the recently passed California Privacy Rights Act of 2020 that will amend the CCPA on January 1, 2023 (see Article, Expert Q&A: The California Privacy Rights Act of 2020 (CPRA));

- collects information from residents of other states with comprehensive consumer privacy laws, such as Virginia or Colorado (see Practice Note, Quick Comparison Chart (CPRA and VCDPA) and Legal Updates, Virginia Enacts Consumer Data Protection Act and Colorado Enacts Privacy Act);
- collects information from residents of other states with more restrictive privacy requirements, such as Nevada's personal information sales opt-out law (see Nevada's Personal Information Sales Opt-Out Law Checklist) or Maine's internet privacy law (see Legal Update, Maine's Governor Signs New Internet Privacy Law);
- collects healthcare information, consider the **Health Insurance Portability and Accountability Act** (HIPAA) (see Practice Note, HIPAA Privacy Rule);
- provides information about or promotes medical devices, consider rules and guidance by the **Food and Drug Administration** (FDA) and the FTC's Mobile Health Apps Interactive Tool;
- relates to financial services, consider the **Gramm-Leach-Bliley Act** (see Practice Note, GLBA: The Financial Privacy and Safeguard Rules);
- provides for the streaming or downloading of video content, consider the **Video Privacy Protection Act** (VPPA), which contains a private right of action;
- targets users located in the EU or UK, consider the EU **General Data Protection Regulation** (GDPR) and the UK GDPR (see Practice Note, Overview of EU General Data Protection Regulation, Country Q&A, Data Protection in the UK (England and Wales): Overview and GDPR Resources for US Practitioners Toolkit);
- implicates data broker regulation, consider the **Fair Credit Reporting Act** (FCRA), and state data broker laws (see Legal Updates, Vermont Enacts First Data Broker Law and California Enacts Data Broker Law); or
- targets children under the age of 13 or contains child-directed content, consider the **Children's Online Privacy Protection Act of 1998** (COPPA) (see Practice Notes, Children's Online Privacy: COPPA Compliance and Mobile App Privacy: The Hidden Risks: COPPA Rule Changes).

Comply with Industry and Regulatory Guidelines and Best Practices

Consider, for example:

- Mobile Marketing Association resources, including its Mobile Application Privacy Policy Framework (registration required), which sets out guidelines to address core privacy issues and data processes of mobile apps. The framework includes model policy language (see Legal Update, Mobile Marketing Association Releases Privacy Policy Guideline for Mobile Apps).

- FTC reports providing guidance, including:
    - Mobile Privacy Disclosures: Building Trust Through Transparency, which promotes more effective mobile privacy disclosures;
    - App Developers: Start with Security, which provides recommendations to app developers for addressing mobile app security;
    - Marketing Your Mobile App: Get It Right from the Start, which gives guidelines to comply with truth-in-advertising standards and basic privacy principles;
    - What's the Deal?: An FTC Study on Mobile Shopping Apps, which provides guidelines addressed to developers of shopping apps; and
    - Mobile Security Updates: Understanding the Issues, which recommends best practices for ensuring mobile operating system security.
- The California Attorney General's report, Privacy on the Go: Recommendations for the Mobile Ecosystem.
- Resources on the Digital Advertising Alliance (DAA) website, including:
    - Application of Self-Regulatory Principles to the Mobile Environment guidance, which applies to companies that collect and use data for use in interest-based advertising (IBA) (see Legal Updates, DAA Releases Self-Regulatory Principles for the Mobile Environment); and
    - Application of the DAA Principles of Transparency and Control to Data Used Across Devices guidance that addresses the practice of using cross-app and multi-site data collected from different computers or devices (see Legal Update, DAA Publishes Guidance on Applying Self-Regulatory Principles to Cross-Device Data Collection).
- The National Telecommunications and Information Administration's (NTIA) Short Form Notice Code of Conduct to Promote Transparency in Mobile App Practices.
- The Network Advertising Initiative's (NAI) 2020 NAI Code of Conduct on tailored advertising and related guidance, including Guidance for NAI Members: Use of Non-Cookie Technologies for Internet-Based Advertising, which applies to members' use of non-cookie technologies, like digital fingerprinting. Additional guidance is available on the NAI website.
- The international mobile industry group GSMA's Internet of Things (IoT) privacy and data security guidelines targeted at mobile device developers, manufacturers, and service providers (see Legal Update, Mobile Industry Group Issues Internet of Things Privacy and Data Security Guidelines).

Comply with App Store Guidelines and Agreements

Review the privacy-related terms of each applicable platform provider's app store developer guidelines and agreements to ensure compliance:

- When the app is submitted for approval after development.
- At the time of each app update.
- When the platform provider's terms of use or other relevant documents change.

(See Practice Note, Mobile App Development and Distribution: The App Store-App Developer Relationship.)

Develop Internal and Customer-Facing Privacy Policies

Develop separate written user information policies for:

- Internal business use, setting out required practices for employees (see Internal User Information Policy).
- Online disclosure, setting out the privacy promises the company makes to its end users (see Long-Form and Short-Form Privacy Disclosures).
- Special or "just-in-time" notices, which are shorter privacy statements and privacy controls designed to draw users' attention to data practices that may be unexpected.

For more information on drafting effective privacy notices, see Practice Note, Drafting Privacy Notices.

Internal User Information Policy

- Develop a comprehensive internal customer information policy that sets out, among other things:
  - the person or group with custody over user information and responsibility for safeguarding it;
  - organizational permissions for accessing and using the information;
  - proper chain-of-custody for user information;
  - procedures for requesting and approving access to and use of information; and
  - requirements for disclosing information.

- Ensure the internal policy is at least as restrictive as the company's external statements.
- Regularly review the policy to ensure it reflects developments in both the business and technology.

For a sample internal data protection policy, see Standard Document, Personal Information Protection Policy (Internal).

Long-Form and Short-Form Privacy Disclosures

Taking into account regulatory guidance favoring shorter and understandable privacy policies, develop both short- and long-form privacy policies. The short-form policy should:

- Provide a succinct overview of the information collection and sharing practices of the app.
- Disclose collection and sharing of any personal information, including:
  - geolocation data;
  - hardware identifiers;
  - photos;
  - address book data;
  - audio and video files; and
  - text messages.

  (See Broadly Consider both Traditional and Non-Traditional Types of Personal Information.) For a sample short-form mobile app privacy disclosure, see Standard Document, Mobile Application Short-Form Privacy Disclosure.
- Link to a longer policy that provides additional detail for the end user. For a model long-form mobile app privacy policy, see Standard Document, Mobile Application Privacy Policy.

US Privacy and Data Security Law: Overview

by Ieuan Jolly, Linklaters LLP, with Practical Law Data Privacy Advisor

Maintained • California, Maine, Massachusetts, Nevada, USA (National/Federal)

This Note provides an overview of prominent US privacy and data security laws relating to the collection, use, processing, and disclosure of personal information. It summarizes key federal privacy and data security laws, certain state laws, with a focus on California and Massachusetts, and the Mobile Marketing Association and Payment Card Industry Data Security Standards.

Privacy and Data Security Risks

Federal Laws

FTC Act

GLBA

Dodd-Frank Wall Street Reform and Consumer Protection Act

HIPAA

Other Federal Laws

State Laws

California Laws

Massachusetts Data Security Regulation

Other State Internet Privacy Laws

Industry Guidelines and Standards

Mobile Marketing Association Guidelines

PCI DSS

Cross-Border Issues

While each Congressional term brings proposals to standardize laws at the federal level, the US currently does not have a single, comprehensive federal law regulating privacy and the collection, use, processing, disclosure, and security of **personal information**. Instead, there is a system of federal and state laws and regulations, and common law principles that overlap, dovetail, and sometimes contradict one another. Government agencies have also developed guidelines and industry groups have undertaken self-regulatory efforts that do not have the force of law but are considered best practices. These self-regulatory programs often have accountability components that regulators increasingly use as enforcement tools.

Recent increases in data security breaches have led to an expansion of this patchwork system, which is becoming one of the fastest growing areas of legal regulation. The growth in interstate and cross-border data flow, together with new privacy and data security-related statutes and regulations, heightens the risk of privacy violations and creates a significant compliance challenge.

This Note provides an overview of key US privacy and data security laws, including:

- The consequences of failing to comply with privacy and data security laws.
- Key federal laws in this area, with an explanation of the entities and data the law covers, the obligations and requirements under the legislation, and potential sanctions and liability.
- State laws in California, Massachusetts, and several other states where rigorous privacy and data security laws have been adopted.
- Industry guidelines and standards.

Privacy and Data Security Risks

Failure to comply with privacy and data security laws can result in significant adverse consequences, including:

- Government-imposed civil and criminal sanctions, including fines and penalties.
- Significant fines and damages awards resulting from private lawsuits, including class actions, which some privacy and data security laws permit.
- Damage to the company's reputation and customers' confidence and trust, resulting in lost sales, market share, and brand and stockholder value.

Federal Laws

There are many federal laws that regulate privacy and the collection, use, processing, and disclosure of personal information, including:

- Broad federal consumer protection laws, such as the **Federal Trade Commission Act** (FTC Act), that are not specifically privacy and data security laws, but are used to prohibit unfair or deceptive practices in the collection, use, processing, protection, and disclosure of personal information.
- Laws that apply to particular sectors, such as:
    - the **Gramm-Leach-Bliley Act** (GLBA), which applies to financial institutions; and

    - the **Health Insurance Portability and Accountability Act** (HIPAA), which applies to most health care providers, health plans, and their service providers.

- Laws that apply to types of activities that use personal information or might otherwise affect individual privacy, such as:
    - the Telephone Consumer Protection Act (TCPA) for telemarketing activities; and
    - the **Controlling the Assault of Non-Solicited Pornography and Marketing Act** (CAN-SPAM Act) for commercial email.

There are also many federal national security and law enforcement-related laws that regulate the use of personal information such as the **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001** (USA PATRIOT Act), and federal and state wiretapping laws. A discussion of these laws is outside the scope of this Note.

This section examines the following key federal privacy laws in more detail:

- The FTC Act.
- GLBA.
- The **Federal Trade Commission's** Red Flags Rules issued under the Fair and Accurate Credit Transactions Act (FACTA), which require financial institutions and creditors to implement and maintain written identity theft prevention programs.
- HIPAA, as amended by the **Health Information Technology for Economic and Clinical Health Act** (HITECH Act).
- Other prominent federal laws, including:
    - the **Children's Online Privacy Protection Act** (COPPA), which regulates the online collection of information from children under 13;
    - the **Fair Credit Reporting Act** (FCRA), as amended by FACTA, which regulates consumer credit and other information;
    - CAN-SPAM, which regulates commercial email;
    - the TCPA, which regulates telemarketing;
    - the **Electronic Communications Privacy Act** (ECPA), which regulates electronic communications;

- the **Computer Fraud and Abuse Act** (CFAA), which regulates unauthorized computer use and computer tampering;
- the Communications Act, which regulates telecommunications and network service providers; and
- the **Video Privacy Protection Act** (VPPA), which regulates consumers' video service usage data.

For information on the progress of select federal privacy-related bills that Congress is currently considering, see Practice Note, Federal Privacy-Related Legislation Tracker.

FTC Act

The FTC Act (15 U.S.C. §§ 41-58) is a federal consumer protection law that prohibits unfair or deceptive commercial practices. The FTC has long applied it to business practices that affect consumer privacy and data security. Under its broad consumer protection enforcement authority, the FTC has emerged as the primary federal regulator in this area. It has brought enforcement actions against companies for:

- Failing to comply with statements in their posted privacy policies.
- Making material changes to their privacy policies without adequate notice to consumers.
- Failing to provide reasonable and appropriate security measures for sensitive consumer information they hold.

The FTC also issues privacy and data security guidelines that are not legally binding but are considered best practices. For example:

- The FTC issued a report on consumer privacy protection in March 2012 with recommendations for best privacy practices for companies, including use of privacy-by-design principles (see Protecting Consumer Privacy in an Era of Rapid Change).
- The FTC published Self-Regulatory Principles for Behavioral Advertising (Behavioral Advertising Principles) in 2009, which set out non-binding guidelines for conducting behavioral advertising, including tracking an individual's online activities to deliver tailored advertising. The FTC expanded the self-regulatory program to the mobile environment in 2015.
- In 2017, the FTC issued a report on cross-device tracking, which occurs when online platforms, publishers, and ad companies track a consumer's activity across different devices such as smartphones, tablets, computers, or other connected devices. The FTC recommends that companies engaging in cross-device tracking:
  - be transparent;
  - give consumers choice to control their data;

    - provide higher protections for sensitive data such as health, financial, and children's information; and
    - maintain reasonable security measures.

- The FTC regularly publishes data security guidance, including its Start with Security: A Guide for Business and its Stick with Security blog posts. For more information on the FTC's data security standards, see Practice Note, FTC Data Security Standards and Enforcement.

Entities Subject to the FTC Act

The FTC Act and related FTC-issued rules and guidelines apply to most companies and individuals doing business in the US. Companies that are primarily regulated by other federal agencies, such as certain transportation, telecommunications, and financial companies, are not subject to the Act.

The Behavioral Advertising Principles apply to online service providers, including website operators and mobile app developers, that engage in behavioral advertising, which in various forms is also called contextual advertising or targeted advertising. Compliance with these principles is voluntary, although many companies adopt them as best practices.

Regulated Data

The FTC Act does not regulate specific categories of personal information. Instead, it prohibits unfair or deceptive acts or practices that fail to safeguard consumers' personal information.

The Behavioral Advertising Principles apply to entities that track a consumer's online activity to deliver advertising targeted to the consumer's interests. They focus on any data that could reasonably be associated with a particular:

- Consumer.
- Computer.
- Other device.

The Principles are not limited to personal information that can be directly linked to a specific individual, such as an individual's name, address, email address, Social Security number, or driver's license number.

Notice and Disclosure Requirements

The FTC Act does not expressly require companies to have or disclose a privacy policy. The FTC has taken the position, however, that:

- If a company discloses a privacy policy, it must comply with it.
- It is a violation of the FTC Act for a company to make material changes to its privacy policy without providing consumers with:
    - notice of those changes; and
    - the opportunity to opt out.

The FTC also enforces COPPA, which requires websites, online services, and mobile apps directed to children, or that knowingly collect personal information from children, to provide a privacy policy (see COPPA).

The FTC's Behavioral Advertising Principles suggest that companies engaging in behavioral advertising:

- Disclose to consumers their data collection practices tied to online behavioral advertising.
- Disclose that consumers can opt out of these practices.
- Provide an opt-out mechanism to consumers such as an electronic checkbox or a means to send an email to the operator.

Consent Requirements

The FTC Act does not expressly address consent. However, organizations that revise their privacy policies should obtain consumers' consent before using their data in ways that are materially different from the policy that was in effect when they collected it.

The FTC also enforces COPPA, which requires websites, online services, and mobile apps directed to children, or that knowingly collect personal information from children, to obtain verifiable parental consent before collecting, using, or sharing children's personal information (see COPPA).

The FTC's Behavioral Advertising Principles suggest that website operators and mobile app developers obtain affirmative express consent, which can be provided online, from consumers before collecting or using sensitive consumer data for online behavioral advertising. Under the Behavioral Advertising Principles, sensitive data includes:

- Financial data.
- Children's data.
- Health information.
- Precise geographic location (geolocation) information.

- Social Security numbers.

Individual Access to Collected Data and Right to Correct or Delete Data

The FTC Act and most US federal and state privacy laws generally do not provide individuals with specific rights to access or correct their personal information. Some notable exceptions include HIPAA and some California laws (see HIPAA and California Laws).

However, the FTC enforces COPPA, which requires operators of websites and other online services directed to children, or that knowingly collect personal information from children, to allow parents to:

- View the personal information the operator collects about their child.
- Delete and correct that information.

(See COPPA.)

Data Security Requirements

The FTC Act does not specifically address data security. However, the FTC has brought enforcement actions alleging that the failure to take reasonable and appropriate steps to protect personal information is an unfair act or practice. For example, the FTC has found violations of the FTC Act where a company:

- Failed to encrypt information while it was in transit or stored on in-store networks.
- Stored personally identifiable information in a file format that permitted anonymous access.
- Did not use readily accessible security measures to limit access to customer data.
- Failed to employ sufficient measures to detect unauthorized access or conduct security investigations.
- Created unnecessary business risks by storing information longer than necessary, in violation of bank rules.

(See *In re BJ's Wholesale Club, Inc.,* 140 F.T.C. 465 (FTC Consent Order, Sept. 20, 2005).)

The FTC has taken the position that inadequate data security practices can form the basis for a deceptive practices claim where a privacy policy states that the business has implemented reasonable and appropriate security measures (see Complaint, *Federal Trade Comm'n v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602 (D.N.J. 2014), ***aff'd***, 799 F.3d 236 (3d Cir. 2015) (see Enforcement)).

The FTC's Behavioral Advertising Principles suggest that website and mobile app operators that collect or store consumer data for behavioral advertising purposes should:

- Provide reasonable security for that data, according to:
    - the data's sensitivity;
    - the nature of the company's business operations;
    - the types of a risks a company faces; and
    - reasonable protections that are available.
- Retain data for only the time necessary to fulfill a legitimate business or law enforcement need.

Restrictions on Sharing Data with Third Parties

The FTC Act does not expressly prohibit sharing personal information with third parties. However, the FTC takes the position that if a company's privacy policy includes statements regarding the company's information sharing practices, it must comply with them. This includes situations where the privacy policy states that the company will not rent, sell, or otherwise disclose personal information to third parties.

The FTC may also bring enforcement actions against companies that have unfair or deceptive information sharing practices, even if those companies do not have a privacy policy or have not violated their privacy policies.

Important Exemptions

The FTC's privacy rules and guidelines provide exemptions from privacy requirements for law enforcement purposes.

Enforcement

The FTC is the primary enforcer of the FTC Act and other federal privacy laws, including COPPA, the FCRA, and FACTA. Actions the FTC can take include:

- Starting an investigation.
- Issuing a cease and desist order.
- Filing a complaint in court.

The FTC also reports to Congress on privacy issues and recommends the enactment of privacy-related legislation.

Sanctions and Other Liability

The FTC Act provides:

- Monetary penalties.
- Criminal penalties, including imprisonment for up to ten years.

The FTC can also:

- Obtain injunctions.
- Provide restitution to consumers.
- Require repayment of investigation and prosecution costs.

Settlements with the FTC and other government agencies also often result in significant reporting requirements, audits, and third-party monitoring.

Notable examples of recent FTC enforcement actions include:

- In September 2021, the FTC announced a proposed settlement with Support King LLC dba Spyfone for allegedly failing to ensure purchasers of its "stalking" app used the app for legitimate purposes. The app allowed purchases with physical access to another person's mobile device to install the app and surreptitiously monitor photos, texts, web histories, physical locations, and other personal information. Spyfone also allegedly harvested and shared personal information. The settlement bans Spyfone from selling surveillance apps and also requires it to delete all personal data collected by the app (for more, see Legal Update, FTC Announces Settlement Banning "StalkerApp" SpyFone and Ordering Deletion of All Data).
- In January 2021, the FTC announced a proposed settlement with Tapjoy, Inc. for allegedly failing to provide users with in-game rewards they were promised for completing tasks that appeared on an "offerwall" where Tapjoy displayed third-party advertisements. The settlement requires Tapjoy to monitor its advertisers to ensure they are following through on promised rewards, investigate complaints from consumers who say they did not receive their rewards, and discipline advertisers who deceive consumers (for more, see Legal Update, FTC Prohibits Mobile Advertising Company From Misleading Users About In-Game Rewards).
- In January 2021, the FTC settled with Everalbum, Inc. for allegedly deceiving customers about its use of facial recognition technology and its retention of photos and videos of users who deactivated their accounts. The settlement requires Everalbum to delete facial recognition data derived from users who did not expressly consent to the use of that technology and obtain users' express consent before using their biometric information (for more, see Legal Update, FTC Announces Settlement with Photo Storage App Company Over Improper Facial Recognition Use Allegations).

- In December 2020, the FTC announced a proposed settlement with Ascension Data & Analytics, LLC for allegedly violating the GLBA by failing to ensure that its vendor secured mortgage holders' personal data. The FTC alleged that the vendor stored sensitive information, including social security numbers, on a cloud-based server in plain text without any protections. The proposed consent order requires Ascension to contractually require vendors to implement and maintain safeguards for personal information (for more, see Legal Update, FTC Agrees to Settle with Ascension Over Alleged Vendor Oversight Failures).

- In November 2020, the FTC settled with Zoom Video Communications, Inc. for alleged unfair and deceptive practices related to its user security and end-to-end encryption practices. The settlement imposes specific information security program and monitoring requirements on the company, and requires it to refrain from making misrepresentations about its privacy and security practices (for more, see Legal Update, FTC Settlement Requires Zoom to Enhance Information Security Program).

- In June 2020, the FTC announced a settlement with Kohl's Department Stores, Inc. for alleged violations of the Fair Credit Reporting Act (FCRA), which requires mandatory disclosures to identity theft victims (15 U.S.C.A. § 1681g(e)). From 2017 to 2019, Kohl's policy for handling FCRA information requests was to send relevant records to law enforcement or a victim's attorney on their request, rather than directly to the victim, as required by law (for details, see Legal Update, FTC Settles Claims Kohl's Failed to Give Identity Theft Victims FCRA Required Information).

- In January 2020, the FTC settled with mortgage broker, Mortgage Solutions FCS, Inc., for responding to negative Yelp.com reviews with customer's personal information, including their credit histories, family relationships, and names. Mortgage Solutions agreed to pay a $120,000 civil penalty and refrain from using customers' personal information without consent (for more, see Legal Update, FTC and Mortgage Broker Reach Settlement Over Personal Information Disclosures in Yelp Review Responses).

- In September 2019, the FTC announced its largest to-date COPPA settlement of $170 million, including $34 million to New York, with YouTube, LLC and its parent, Google LLC, over allegations that YouTube collected personal information from children under 13 without proper notice and verifiable parental consent (for more, see COPPA and Legal Update, FTC and NY AG Announce $170 Million YouTube Settlement Over Alleged COPPA Violations).

- In mid-2019, the FTC settled charges against Facebook, Inc. for violating a 2012 FTC order prohibiting the company from deceiving users about how much control they have over their privacy. Under the settlement terms, Facebook must pay a record-setting five billion dollar penalty and make sweeping changes to its corporate structure and privacy practices (for details, see Legal Update, Facebook Agrees to Settle Privacy Claims with the FTC and SEC).

For more information on FTC enforcement actions, see Practice Note, FTC Data Security Standards and Enforcement.

GLBA

The GLBA's (15 U.S.C.A. §§ 6801 to 6809) privacy and data security provisions regulate the collection, use, protection, and disclosure of nonpublic personal information (NPI) by financial institutions.

Entities Subject to GLBA

The GLBA applies to:

- Financial institutions, which the law broadly defines to include a range of institutions that engage in financial activities. The FTC considers a business to be a financial institution if it significantly engages in financial activities, which is a flexible standard that takes into account all of the facts and circumstances. Examples of financial institutions include:
  - banks;
  - securities firms;
  - insurance companies; and
  - other businesses that may not traditionally be thought of as financial institutions but provide financial services and products, such as mortgage lenders or brokers, credit counseling services and other financial advisors, collection agencies, and retailers that issue their own credit cards.
- Affiliated and unaffiliated third parties that receive NPI from financial institutions.
- Persons who obtain or attempt to obtain NPI from financial institutions through false or fraudulent means.

Regulated Data

The GLBA applies to NPI that a financial institution collects. It also applies to NPI provided by, resulting from, or otherwise obtained in connection with consumers and customers who obtain financial products or services primarily for personal, family, or household purposes.

NPI under the GLBA generally is any personally identifiable financial information that is:

- Not publicly available.
- Capable of personally identifying a consumer or customer.

Consumers are individuals who have obtained a financial product or service from a financial institution, but do not necessarily have an ongoing relationship with the entity. An example of a consumer is someone who cashes a check with a check-cashing company, makes a wire transfer, or applies for a loan.

Customers are a subset of consumers and include anyone with an ongoing relationship with a financial institution.

General Obligations

The GLBA regulates the collection, use, protection, and disclosure of NPI. The GLBA requires that financial institutions:

- Notify customers about their information sharing practices.
- Provide customers with a right to opt out if they do not want their information shared with certain unaffiliated third parties, as detailed in the GLBA Financial Privacy Rule.
- Implement a written information security program, including specific safeguards to protect NPI from unauthorized disclosure, as detailed in the GLBA Safeguards Rule.

GLBA requirements may also restrict entities that receive consumer financial information from a financial institution from reusing or redisclosing that information.

Notice and Disclosure Requirements

The GLBA requires a financial institution to provide notice of its privacy practices to customers and consumers in certain situations. The notice's timing and content depends on whether the subject of the data is a consumer or customer. For example, a financial institution must provide notice of its privacy practices to:

- A customer, both:
  - when the relationship is created; and
  - annually thereafter.
- A consumer, if the financial institution intends to share the consumer's NPI.

The privacy notice must be a clear, conspicuous, and accurate statement of the financial institution's privacy practices. It should:

- Describe the categories of information that the financial institution collects and discloses.
- Identify the categories of affiliated and non-affiliated entities with which it shares information.
- State that the consumer or customer has the right to opt out of some disclosures.
- Explain how the consumer or customer can opt out, if an opt-out right is available.

An affiliated entity is any company that controls, is controlled by, or is under common control with another company and includes both financial and non-financial institutions.

In 2009, the FTC issued a form model privacy notice with the federal banking regulators responsible for enforcing the GLBA (12 C.F.R. pt. 1016, App.). Using the form is not mandatory, but financial institutions that use it obtain a safe harbor and satisfy the GLBA disclosure requirements for privacy notices (12 C.F.R. § 1016.2(a)).

Consent Requirements

Although the GLBA does not require any affirmative consent from a customer or consumer, it requires a financial institution to:

- Notify customers of the institution's privacy policy and practices at the time of setting up a customer relationship, and at least annually thereafter.
- Notify consumers, if they are not also customers, of the institution's privacy policy and practices before it discloses NPI to a non-affiliate, unless a statutory exception applies.
- Provide customers and consumers with reasonable means to opt out of certain uses and disclosures of their NPI. The means can be written, oral, or electronic.

Under the GLBA, a financial institution does not need to provide an opt-out right to:

- Share NPI for the purpose of administering or enforcing a transaction that a customer or consumer requests or authorizes (see Practice Note, GLBA: The Financial Privacy and Safeguards Rules: Exceptions to Notice and Opt Out Rights).
- Share NPI with outside companies that provide the financial institution with essential services, such as data processing or servicing accounts, if certain conditions are met. Those conditions include contractually binding the outside company to protect the confidentiality and security of the data.

Individual Access to Collected Data

The GLBA allows consumers or customers to opt out of certain disclosures, but generally does not provide affirmative access rights.

Restrictions on Disclosing Personal Information to Third Parties

Restrictions under the GLBA on disclosing personal information to third parties depend on whether the third party is an affiliate or unaffiliated third party:

- **Disclosures to affiliates.** A financial institution can disclose a consumer's NPI to an affiliated entity if it provides notice of this practice. The financial institution does not need to obtain affirmative consent or provide an opt-out right for this disclosure.

- **Disclosures to unaffiliated third parties.** Generally, a financial institution must provide notice and a right to opt out of disclosures of NPI to unaffiliated parties. However, a financial institution can disclose an individual's NPI to an unaffiliated entity without allowing the individual to opt out if all of the following conditions are met:
    - the third party uses the information to perform services for the financial institution;
    - the financial institution provides notice of this practice to the individual before sharing the NPI; and
    - the financial institution and the third party enter into a contract that requires the third party to maintain the NPI's confidentiality and to use the information only for the prescribed purposes.

Financial institutions may also disclose NPI to unaffiliated third parties without providing an opt-out right under certain circumstances, including when the disclosure is:

- Necessary to effect, administer, or enforce a transaction or made with the customer's consent.
- For compliance purposes.
- For law enforcement purposes.

Data Security Requirements

The GLBA Safeguards Rule requires companies to develop a written information security program that sets out how they protect customer information and implement reasonable technical, administrative, and physical safeguards to:

- Ensure the security and confidentiality of customer information.
- Protect against any anticipated threats or hazards to the security or integrity of customer information.
- Protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to the customer.

The written information security program must be appropriate to:

- The company's size and complexity.
- The nature and scope of the company's activities.
- The sensitivity of the customer information the company handles.

On December 9, 2021, the FTC published a final rule amending the Safeguards Rule to clarify and strengthen data security obligations and expand its application to additional entities (16 C.F.R § 314; see Legal Update, FTC Amends Safeguards

Rule to Strengthen Data Security Obligations). For more information on elements of an information security program and the specific safeguards that companies are required to implement under the Safeguards Rule, see Practice Note, GLBA: The Financial Privacy and Safeguards Rules: The Safeguards Rule.

Data Breach Notification Requirements

Neither GLBA itself nor the FTC regulation currently require data breach notification, though in late October 2021 the FTC issued a supplemental notice of proposed rulemaking on additional amendments to the Safeguards Rule that would require entities to report data breaches and other security events.

Several of the federal banking regulators, such as the **Office of the Comptroller of the Currency** (OCC) and the **Federal Reserve Board** (FRB), have issued guidance that requires financial institutions subject to their authority to notify the regulator, and sometimes affected customers, when there has been unauthorized access to sensitive customer information.

Sensitive customer information generally includes a customer's name, address, or telephone number combined with one or more of the following items:

- Social Security number.
- Driver's license number.
- Account number.
- Credit or debit card number.
- Personal identification number or password that would permit access to the customer's account.

In late November 2021, the OCC, Board of Governors of the FRB, and the Federal Deposit Insurance Corporation (FDIC) also issued a final rule requiring banking organizations to notify their primary federal regulator within 36 hours of determining that a material computer-security incident has occurred. For more information, see Legal Update, Federal Banking Agencies Issue Cyber Incident Notification Requirements.

Enforcement

Multiple federal regulators enforce the GLBA, including:

- The **Consumer Financial Protection Bureau** (CFPB).
- The FTC.
- Federal banking regulators.
- The **Securities and Exchange Commission**.

- The **Commodity Futures Trading Commission**.

These agencies have jurisdiction over banks, **thrifts**, credit unions, brokerage firms, and **commodity** traders. State insurance agencies also enforce the GLBA. The enforcing agency depends on the enforcement target and whether the Financial Privacy Rule or Safeguards Rule is at issue.

The GLBA does not include a right for individuals to bring private actions.

Sanctions and Other Liability

Penalties for GLBA violations vary based on the authorizing statute of the agency that brings the enforcement action. Possible sanctions and other liability for FTC enforcement actions include:

- Civil monetary penalties.
- Fines and imprisonment for those who obtain or attempt to obtain, or cause or attempt to cause, the disclosure of a financial institution's customer information through means that are:
  - false;
  - fictitious; or
  - fraudulent.
- Enhanced criminal penalties, if the acts are committed or attempted:
  - while violating another US law; or
  - as part of a pattern of illegal activity.

For more information on the GLBA, see Practice Note, GLBA: The Financial Privacy and Safeguards Rules.

Dodd-Frank Wall Street Reform and Consumer Protection Act

In 2010, the **Dodd-Frank Wall Street Reform and Consumer Protection Act** created the CFPB. The Dodd-Frank Act grants the CFPB financial privacy rulemaking and enforcement authority under the GLBA (see GLBA). The Dodd-Frank Act also gives the CFPB enforcement authority against covered organizations that engage in acts or practices related to consumer financial products and services that are:

- Unfair.

- Deceptive.
- Abusive.

(12 U.S.C. §§ 5531(a), 5536(a)(1).)

The CFPB interprets this authority broadly to take data security actions against consumer financial product and service providers. For example, in March 2016, the CFPB announced its first data security action against Dwolla, Inc. for deceptive practices related to representations about its online payment service. In addition to paying a $100,000 monetary penalty, the CFPB's consent order required Dwolla to:

- Stop misrepresenting its data security practices.
- Develop, implement, and maintain a comprehensive written information security program.
- Properly train employees and fix security flaws.
- Annually obtain and submit to the agency an independent data security program audit.

(See Legal Update, CFPB's First Data Security Action Imposes $100,000 Penalty.)

HIPAA

HIPAA (Pub. L. No. 104-191 (1996)) governs **individually identifiable health information**. It applies broadly to certain health care entities and their service providers. The **Department of Health and Human Services** (HHS) promulgates related regulations, which include:

- The HIPAA Privacy Rule, also known as the Standards for Privacy of Individually Identifiable Health Information, which applies to the collection, use, and disclosure of **protected health information** (PHI). For more information on the Privacy Rule, see Practice Note, HIPAA Privacy Rule.
- The HIPAA Security Rule, also known as the Security Standards for the Protection of Electronic Protected Health Information, which provides standards for protecting PHI. For more information on the Security Rule, see Practice Note, HIPAA Security Rule.
- The HIPAA Transactions Rule, also known as the Standards for Electronic Transactions, which applies to some forms of electronic transmissions of health data, especially between health care providers and health plans.

HIPAA includes a Breach Notification Rule (45 C.F.R. Part 164) which requires covered entities to provide notice of a PHI breach. Under the rule, a covered entity must provide notice if PHI is acquired, accessed, used, or disclosed in a manner not permitted under the Privacy Rule, unless the covered entity demonstrates that there is a low probability that the PHI has been compromised. For more details, see Practice Note, HIPAA Breach Notification Rules.

Entities Subject to HIPAA

HIPAA applies to covered entities and their business associates. Covered entities include:

- Health plans.
- Health care clearinghouses.
- Most health care providers, specifically those that conduct HIPAA standard financial and administrative transactions electronically.

A business associate is a person or entity that performs services, functions, or activities for or on behalf of a covered entity involving the use or disclosure of PHI. These services, functions, and activities include, for example:

- Claims processing and administration.
- Data analysis and processing.
- Quality assurance.
- Billing.
- Benefits management.
- Practice management.
- Re-pricing.

HIPAA's jurisdictional scope is limited to covered entities and business associates over which the US government has enforcement authority. However, business associates of covered entities may have contractual obligations to safeguard PHI, including those operating outside of US jurisdiction.

Regulated Data

HIPAA regulates PHI, which is defined as individually identifiable health information that a covered entity or business associate maintains or transmits.

General Obligations

HIPAA regulates the use and disclosure of PHI and the collection, use, maintenance, or transmission of electronic PHI.

HIPAA requires that covered entities, with some exceptions:

- Provide notice of their privacy practices and individuals' rights under HIPAA.
- Use, request, and disclose only the minimum amount of PHI necessary to complete a transaction, as detailed in the HIPAA Privacy Rule.
- Implement data security procedures, protocols, and policies at administrative, technical, physical, and organizational levels to protect PHI, as detailed in the HIPAA Security Rule.
- Comply with uniform standards for certain electronic transactions, as defined in the HIPAA Transactions Rule.
- Notify individuals if there is a security breach of PHI. Business associates must notify affected covered entities if a security breach occurs. In late 2009, the FTC issued a similar breach notification rule for companies that are not subject to HIPAA regulations but that develop and distribute online and offline software applications that process personal health records (16 C.F.R. §§ 318.1-318.9).

Notice and Disclosure Requirements

The HIPAA Privacy Rule requires each covered entity to provide notice to individuals of its privacy practices and of individuals' rights under HIPAA. For health care providers, this requirement generally applies on the first visit for treatment. The rule sets out specific requirements for the contents and method of the notice. For a sample provider notice and acknowledgment form, see Standard Documents, HIPAA Notice of Privacy Practices for Health Care Providers and HIPAA Notice of Privacy Practices Acknowledgment Form.

Consent Requirements

HIPAA generally requires covered entities to obtain consent from an individual before using or disclosing that individual's PHI to third parties, with certain exceptions. Consent must generally:

- Be in writing.
- Contain the individual's signature and the date.

The HIPAA Privacy Rule provides specific statements that must be included in the consent. For an example form, see Standard Document, HIPAA Authorization to Use and Disclose PHI.

With some exceptions, HIPAA allows a covered entity to use and disclose PHI under certain circumstances without first obtaining consent. For example, a covered entity need not obtain consent before using or disclosing PHI for purposes of:

- Treatment.

- Payment.
- Healthcare operations.

Special Rules for Certain Categories of Data

There are specific rules under HIPAA governing the disclosure of psychotherapy notes. In general, a covered entity must obtain written authorization before disclosing psychotherapy notes, even for purposes of treatment, operations, or payment.

Individual Access to Collected Data

Under HIPAA, individuals have the right, with some exceptions, to:

- Request access to their PHI.
- Make corrections to their PHI.
- Request an accounting of the manner in which a covered entity has used or disclosed their PHI.

Restrictions on Sharing Data with Third Parties

HIPAA generally requires covered entities to obtain an individual's consent in writing before using or disclosing that individual's PHI to third parties.

Covered entities may disclose PHI to business associates if the parties enter into an agreement that requires the business associate to:

- Use the information only for the purposes the covered entity requires or permits.
- Safeguard the information from misuse.
- Help the covered entity comply with its duties under the Privacy Rule.

When a covered entity has knowledge that its business associate has materially breached or violated the applicable agreement, the covered entity must take reasonable steps to cure the breach or end the violation. If such steps are unsuccessful, the covered entity must terminate the contract. For an example business associate agreement, see Standard Document, HIPAA Business Associate Agreement.

Data Security Requirements

The HIPAA Security Rule requires covered entities to implement data protection policies and reasonable security procedures, including:

- Administrative safeguards, which generally include activities such as assigning responsibility for the security program to the appropriate individuals and requiring security training for employees.
- Physical safeguards, which include mechanisms to protect electronic systems and electronic PHI, such as limiting access to facilities to authorized individuals.
- Technical safeguards, which include automated processes designed to protect data and control access, such as using authentication controls and encryption technology.

For more information on the HIPAA Security Rule, see Practice Note, HIPAA Security Rule.

Data Breach Notification Requirements

The HHS also requires covered entities to notify individuals when their unsecured PHI has been breached. For more information on the HIPAA breach notification rules, see Practice Note, HIPAA Breach Notification Rules.

Important Exemptions

HIPAA does not apply to health information that:

- Is not individually identifiable, for example, aggregate data.
- Individuals or entities that do not fall within the definitions of covered entities or business associates collect or use. For example:
    - some educational and employment records, such as a report about an individual's fitness for duty that is used to make an employment decision, do not fall within HIPAA's scope; and
    - consumer-oriented apps, devices, and online services that collect health-related information but do not meet HIPAA criteria for covered entities or business associates.

There are many exemptions from the restrictions on disclosure of PHI. For example:

- For law enforcement purposes.
- To avert a serious public health threat.

Enforcement

The HHS Office for Civil Rights (OCR) actively enforces the HIPAA rules (for more details, see Practice Note, HIPAA Enforcement: Penalties and Investigations). For example, the OCR:

- Initiates investigations into covered entities' and business associates' information handling practices to determine whether they are complying with the HIPAA regulations.
- Allows individuals to file complaints about privacy violations. HIPAA does not, however, allow individuals to bring private actions.

Sanctions and other Liability

HIPAA authorizes the HHS to impose civil penalties ranging from $100 - $1.5 million based on a framework that examines whether the covered entity or business associate:

- Knew of the violation.
- Was willfully negligent.
- Timely corrected the violation.

In assessing the amount of civil penalties, the HHS will also examine certain mitigating or aggravating factors, such as:

- The nature and extent of the violation.
- The nature and extent of the harm.
- The organization's compliance history.

HIPAA also allows for criminal penalties of up to $250,000 and ten years' imprisonment if the offense was committed under false pretenses or with intent to sell the data for commercial gain (see Enforcement).

Other Federal Laws

COPPA

COPPA (15 U.S.C. §§ 6501-6506) applies to commercial websites, mobile apps, or other online services that:

- Are directed to and collect personal information from children under 13.

- Have actual knowledge that they are collecting personal information from children.

Under the COPPA Rule, personal information is defined as individually identifiable information about a child that is collected online, such as:

- A full name.
- A home address.
- Online contact information.
- A telephone number.
- A Social Security number.
- A persistent identifier that an operator can use to recognize a user over time and across different websites or online services.
- A photo, video, or audio file that contains a child's image or voice.
- Geolocation information sufficient to identify a street name and name of a city or town.
- Information concerning a child or a child's parent or legal guardian that an operator collects online from the child and combines with an identifier described above.

COPPA requires that these websites or online services:

- Provide a privacy notice on the site, including a clear and prominent link to the notice from the home page and at each area where the site collects personal information from children, which states certain required information to inform parents about their information practices.
- Before collecting, using, or disclosing children's personal information:
    - provide direct notice to parents or legal guardians with the same information required in the website notice; and
    - obtain, with some exceptions, verifiable parental consent. The acceptable methods for obtaining consent vary depending on how the operator uses children's personal information.
- On request, provide parents of children who have given personal information with:
    - a description of the types of personal information collected;

    - an opportunity to prevent any further use or collection of information; and
    - reasonable means to obtain the specific information collected.

- Maintain procedures to ensure the confidentiality, security, and integrity of the personal information collected.

The FTC is the primary enforcer of COPPA. In 2017, the FTC updated its COPPA guidance to include internet-connected toys and other devices, as part of the growing internet of things (IoT). The updated guidance also:

- Discusses how new business models and ways of collecting data, like voice-activated toys and IoT devices that collect children's personal information, may affect a company's COPPA obligations.
- Describes additional approved methods for obtaining parental consent.

COPPA includes limited exceptions allowing operators to collect certain information without obtaining parental consent in advance. For example, an operator need not obtain parental consent in advance to:

- Provide the required privacy notice to the child's parent or guardian and seek consent.
- Respond to a one-time request from a child, if the operator then deletes the information.
- Respond more than once to a specific request such as a subscription to a newsletter. However, the operator must:
    - notify a parent or legal guardian that it is communicating regularly with the child; and
    - give a parent the opportunity to stop the communication before sending or delivering a second communication to the child.
- Protect the safety of a child who is participating on the site, online service, or mobile app. The provider must notify the parent or legal guardian and give them an opportunity to prevent further use of the information.
- Protect the security or avoid liability of the site, online service, or mobile app or to respond to law enforcement.

For more information, see Practice Note, Children's Online Privacy: COPPA Compliance.

FCRA and FACTA

The FCRA (15 U.S.C. §§ 1681 to 1681x), as amended by FACTA, limits how consumer reports and credit card account numbers can be used and disclosed. The FCRA applies to:

- **Consumer reporting agencies**.
- Those who use consumer reports, such as lenders and employers.
- Those who provide consumer credit information to reporting agencies, such as credit card companies.

The FCRA defines a consumer report as any communication a consumer reporting agency issues or uses to evaluate a consumer's eligibility for credit or insurance that relates to a consumer's:

- Credit worthiness.
- Credit history.
- Credit capacity.
- Character.
- General reputation.

FACTA amended the FCRA to:

- Allow consumers to:
  - receive on request a free credit report annually from a consumer credit reporting company; and
  - place fraud alerts on their credit histories to reduce identity theft.
- Restrict businesses, with some exceptions, from printing more than five digits of a consumer's payment card number on receipts.
- Create the Red Flags Rule (see The Red Flags Rule).

Rules implemented under FACTA also:

- Require consumer reporting agencies and any other businesses that use consumer reports to adopt procedures for properly disposing of consumer information under the Disposal Rule.
- Prohibit companies from using certain credit information received from an affiliate to market goods or services to a consumer, unless they provide consumers with:
  - notice;

- a reasonable opportunity to opt out; and
- a simple and reasonable method for opting out.

The Red Flags Rule

The FTC's Red Flags Rule requires financial institutions and creditors with covered accounts to develop a written program that identifies and detects relevant warning signs, or red flags, of identity theft. These can include:

- Unusual account activity.
- Fraud alerts on a consumer report.
- Attempted use of suspicious account application documents.

The program must describe appropriate responses to prevent and mitigate the crime and detail a plan to update the program. (16 C.F.R. §§ 681.1-681.2.)

The FTC provides further Red Flags Rule guidance. For a sample written identity theft prevention program, see Standard Document, Red Flags Rule Identity Theft Prevention Program Master Policy.

CAN-SPAM Act

The CAN-SPAM Act (15 U.S.C. §§ 7701-7713) regulates the collection and use of email addresses for commercial purposes. CAN-SPAM prohibits senders of commercial emails from using:

- Any false or misleading header information.
- Subject lines that would likely mislead a recipient about a material fact regarding the message's contents or subject matter.

Senders of commercial emails must also follow certain requirements, including providing in each email, a clear and conspicuous:

- Identification that the message is an advertisement or solicitation.
- Notice of the opportunity to opt out of receiving further commercial email messages from the sender and instructions on how to do so.

For more information on CAN-SPAM, see Practice Note, Email Marketing: CAN-SPAM Act Compliance.

TCPA

The TCPA (47 U.S.C. § 227) regulates the collection and use of telephone numbers for commercial purposes. It applies to both telephone calls and text messages. The TCPA and the regulations promulgated under it set out rules governing, for example:

- Times during the day when telephone solicitations can be made.
- Use of automated telephone equipment for solicitations.
- Maintenance of a do not call registry.
- Information the solicitor must give to the consumer.

The Federal Communication Commission (FCC) makes and enforces the TCPA regulations. For more details, see Practice Note, Telephone Consumer Protection Act (TCPA): Overview.

The TCPA permits private rights of action and provides for recovery of either actual or statutory damages ranging from $500 to $1,500 per unsolicited call or message. Because of these statutory damages, TCPA class action litigation is a key issue for businesses, and the terms of the statute are frequently litigated (see Practice Note, TCPA Litigation: Key Issues and Considerations).

ECPA

ECPA (18 U.S.C. §§ 2510-2522) governs the interception of electronic communications. It applies to anyone who improperly accesses, intercepts, or discloses electronic communications whether stored or in transit that affect interstate or foreign commerce. Violations of ECPA can result in fines and sometimes, imprisonment.

CFAA

The CFAA (18 U.S.C. § 1030) governs computer hacking and makes unauthorized access to protected computers a criminal offense when the offender:

- Knowingly accesses a computer without authorization to obtain national security data.
- Intentionally accesses a computer without authorization to obtain information:
    - contained in a financial institution's financial records or a consumer reporting agency's consumer files;
    - from any US government department or agency; or

- from any protected computer if the conduct involves an interstate or foreign communication.

The CFAA defines a protected computer as a computer that is used in interstate or foreign commerce, which may include any internet-connected laptop or computer. For more information on the CFAA and related litigation, see Practice Notes, Cyberattacks: Prevention and Proactive Responses and Key Issues in Computer Fraud and Abuse Act (CFAA) Civil Litigation.

Communications Act

The Communications Act (47 U.S.C. § 222) regulates telecommunications carriers and services and requires carriers to protect the privacy of customer proprietary network information (CPNI). The FCC's CPNI regulations obligate carriers to report certain data breaches.

VPPA

The VPPA (18 U.S.C. § 2710) prohibits video tape service providers from disclosing consumer's personally identifiable records without consent. The VPPA defines a video service provider as one who rents, sells, or delivers:

- Prerecorded video.
- Similar audio visual materials.

Congress originally passed the VPPA in reaction to the disclosure of a Supreme Court candidate's video rental records in a local newspaper. However, courts have extended it to internet-based service providers. In *In re Hulu Privacy Litigation*, for example, the court held that an online streamer of television shows was a video tape service provider because it sold prerecorded "audio visual materials" (2014 WL 1724344 (N.D. Cal. Apr. 28, 2014)).

The VPPA allows service providers to disclose personal information without consent in limited circumstances, including:

- To law enforcement agencies on a showing of probable cause and under a valid warrant, grand jury subpoena, or court order.
- The names and addresses of consumers to any person, if:
  - the service provider provides the consumer with the opportunity to opt out; and
  - the disclosure does not identify the title, description, or subject matter of any audio visual material. Service providers may disclose the subject matter solely for direct marketing purposes.

The VPPA also:

- Requires service providers to destroy personal information as soon as practicable but no later than one year after it is no longer needed for its collection purposes.
- Provides a private right of action and civil liability for violations, including awards of:
  - actual and punitive damages;
  - legal costs and reasonable attorneys' fees; and
  - equitable relief.

State Laws

Hundreds of privacy and data security laws governing the collection, use, protection, and disclosure of personal information exist at the state level. State privacy and data security laws include, for example:

- **Baby FTC Acts and other consumer protection statutes.** Like the FTC Act, many states have adopted broad consumer protection statutes that prohibit unfair or deceptive business practices.
- **GLBA and HIPAA add-ons.** The GLBA and HIPAA do not preempt more protective state laws concerning the privacy of consumer financial information or personal health information if these state laws are not inconsistent with federal mandates.
- **Social Security number laws.** Many states have adopted specific laws governing the collection, use, protection, and disclosure of Social Security numbers. For details on various state-level requirements to protect Social Security numbers, see Practice Note, State Social Security Number Protection Laws Chart: Overview.
- **Records disposal laws.** Many states, including California, New Jersey, and New York, have enacted laws requiring proper disposal of records containing personal information. For example, California requires businesses to dispose of records containing personal information by shredding, erasing, or otherwise modifying the personal information in these records to make it unreadable (Cal. Civ. Code § 1798.81). For more information on state-level records disposal requirements, see Practice Note, State Data Disposal Laws Chart: Overview.
- **Card transaction laws.** Several states, including California, New York, and Massachusetts, have enacted laws that limit the collection of personal information in connection with payment card transactions.
- **Health information laws.** Many states, including California, have adopted statutes specifically aimed at protecting health or medical information.
- **General data security laws.** A growing set of states, including California and Massachusetts, have enacted laws requiring companies to take reasonable measures and, sometimes, specific steps to protect the security of the personal information that they collect, use, and maintain. For more information on the requirements under various state-level data security laws, see Practice Note, State Data Security Laws: Overview.

- **Financial services and insurance data security laws.** An initial group of states has adopted some form of the National Association of Insurance Commissioners (NAIC) Model Insurance Data Security Law (MDL-668), applying risk-based security standards to state-regulated licensees (see Practice Note, NAIC Model Data Security Law and State-Specific Implementations). New York imposes detailed data security standards on licensed financial services and insurance entities, predating the model law's development (see Practice Note, The NYDFS Cybersecurity Regulations and Complying with the NYDFS Cybersecurity Regulations Checklist).

- **Breach notification laws.** California was the first state to enact a data security breach notification law, dramatically changing the privacy landscape in the US. Currently, all 50 states and the District of Columbia, Guam, Puerto Rico, and the US Virgin Islands have enacted laws requiring notification of security breaches involving personal information. For more information on US data breach notification laws and practical tips on how to prepare for and respond to a data security breach, see Practice Note, Breach Notification and State Q&A Tool: Data Breach Notification Laws.

- **Telephone call recording laws.** Most states have longstanding wiretapping laws that limit telephone call recording without the consent of one or all involved parties. For details on state telephone call recording laws, including consent requirements and various exceptions, see Practice Note, State Telephone Call Recording Laws Chart: Overview.

A growing number of states have laws that govern social media privacy and the privacy of student records. Conflicting federal privacy laws preempt some of these laws, compounding the challenge for companies trying to find a road map for privacy compliance in the US.

California and Massachusetts were early adopters of some of the most rigorous state-level privacy and data security laws. California continues to lead the states in general data protection and sector-specific laws, influencing business practices and policymaking nationwide because of its large market and extensive economic impact (see Other State Internet Privacy Laws).

For information on the progress of select in-progress state privacy-related bills, see Practice Note, State Omnibus Privacy Legislation Tracker.

California Laws

California privacy and data security laws:

- Broadly protect the personal information that businesses collect through the California Consumer Privacy Act of 2018 (CCPA) (Cal. Civ. Code §§ 1798.100 to 1798.199.95; Cal. Code Regs. tit. 11, §§ 7000 to 7102) by granting consumers certain rights regarding their information and imposing various notice and consumer choice duties on businesses. On November 3, 2020, California voters amended the CCPA by passing ballot Proposition 24 to enact the California Privacy Rights Act of 2020 (CPRA), which expands consumers' rights and establishes the California Privacy Protection Agency. The CPRA takes full effect on January 1, 2023. For more on the CCPA and CPRA, see California Privacy Toolkit (CCPA and CPRA).

- Require commercial website and online service providers to conspicuously post and abide by their online privacy policies under the California Online Privacy Protection Act (CalOPPA) (Cal. Bus. & Prof. Code § 22577).

- Impose disclosure requirements and other restrictions on businesses regarding how they share personal information for marketing purposes through the Shine the Light law (Cal. Civ. Code §§ 1798.83-1798.84).

- Specifically protect children and students online under the Student Online Personal Information Protection Act (SOPIPA) (Cal. Bus. & Prof. Code § 22584(i)) and Privacy Rights for California Minors in the Digital World Act (Eraser Law) (Cal. Bus. & Prof. Code §§ 22580-22582).

- Demand reasonable information security practices and data breach notification.

- Address data protection for other specific business sectors and forms of personal information.

For details on California's wide-ranging privacy and data security legal regime, see Practice Note, California Privacy and Data Security Law: Overview. For a California-specific legislation tracker, see CCPA Proposed Amendments and Other California Privacy-Related Legislation Tracker.

Massachusetts Data Security Regulation

The Massachusetts Data Security Regulation (201 Mass. Code Regs. §§ 17.01-17.05) contains some of the most rigorous state-level general data security requirements.

Specifically, Massachusetts's extensive data security regulations:

- Apply to all businesses, whether located in or outside of Massachusetts, that own, license, store, or maintain personal information about Massachusetts residents, whether consumers or employees.

- Define personal information to include first name or initial, and last name in combination with any one or more of:
    - Social Security number;
    - driver's license number or state-issued identification card number; or
    - financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password that would permit access to a resident's financial account.

- Require businesses to develop, implement, and maintain a comprehensive, written information security program that addresses specified safeguards in a way that is appropriate to their:
    - size;
    - scope;
    - resources;

- amount of stored personal information; and
- risks.

For more details on data security requirements in Massachusetts, including specified safeguards, see Practice Note, Written Information Security Programs: Compliance with the Massachusetts Data Security Regulation.

For information on the progress of selected privacy-related bills in Massachusetts, see Practice Note, State Omnibus Privacy Legislation Tracker: Massachusetts.

Other State Internet Privacy Laws

Maine

Maine's Act to Protect the Privacy of Online Consumer Information (Internet Privacy Law) is the strictest state internet service provider (ISP) privacy law to date. The Internet Privacy Law prohibits broadband ISPs from using, selling, disclosing, or permitting access to a customer's personal information without the customer's express opt-in consent, unless an exception applies.

Under the Internet Privacy Law, customer personal information includes:

- Personally identifying information, such as a customer's:
  - name;
  - Social Security number;
  - billing address; or
  - demographic data.
- Information about service use, such as a customer's:
  - web browsing history;
  - geolocation information;
  - financial or health information or information about the customer's children;
  - communication contents; or

- device identifier or internet protocol (IP) address.

The Internet Privacy Law requires ISPs to:

- Provide customers with a notice at the point of sale and on the ISP's website regarding the provider's obligations and customers' rights under the law.
- Secure customer personal information by implementing reasonable security measures to protect it from unauthorized use, disclosure, or access.
- Not treat customers differently based on whether they consent to the use, disclosure, sale, or access of their personal information, for example by:
  - refusing to serve a customer;
  - charging a penalty; or
  - offering a discount if the customer consents.

The law takes effect on July 1, 2020.

Nevada

Nevada's Online Privacy Law, Nev. Rev. Stat. 603A (as amended), provides consumers with a new right to opt out of the sale of their personal information.

The Amended Online Privacy Law applies to operators that:

- Own or operate an internet website or online service for commercial purposes.
- Collect or maintain personal information from a consumer who resides in Nevada and uses or visits their internet website or service.
- Are sufficiently tied to the state of Nevada.

Under the Amended Online Privacy Law, each operator must:

- Continue to comply with the existing requirement to post a notice that:
  - identifies the categories of information it collects and the categories of third parties with which it shares information;

    - identifies the process for users to review and request changes to their information;
    - describes how it will notify users of changes to the notice;
    - discloses whether third parties may collect information about a user's activities across the web; and
    - states the effective date of the notice.

- Establish a designated request address through which consumers can submit verified requests directing the entity not to sell the covered information they collect.
- Verify and act on consumer opt-out requests within 60-days of receiving them.

The opt-out requirements apply whether a business currently sells information or not.

Industry Guidelines and Standards

Many industry groups issue guidelines that are generally considered best practices or are common contract requirements in those industries, but do not have the force of law. Some industry organizations have also implemented enforcement programs (for example, see Legal Update, Digital Advertising Alliance Will Enforce Mobile Self-Regulatory Program). Significant examples of self-regulatory regimes include:

- Mobile Marketing Association Guidelines.
- The Payment Card Industry Data Security Standard (PCI DSS).

Mobile Marketing Association Guidelines

The Mobile Marketing Association's Code of Conduct for Mobile Marketing (registration required), suggests that companies advertising on mobile or wireless devices:

- Ask for and obtain an explicit opt in for all mobile messaging programs.
- Implement a simple opt-out process and reasonable technical, administrative, and physical procedures to protect user information from unauthorized use, disclosure, or access.

More information on the Code of Conduct for Mobile Marketing is available from the Mobile Marketing Association.

PCI DSS

PCI DSS requires all entities that process, store, or transmit cardholder data to comply with 12 basic security requirements, including:

- Implementing firewalls.
- Maintaining access controls.
- Monitoring and testing networks.
- Avoiding vendor-supplied default passwords.
- Maintaining an information security policy.
- Supporting encryption.

PCI DSS is not law. It is an industry standard created and enforced by a group of major credit card brands through contractual obligations. While the individual card companies maintain their own security programs, these programs are consistent with the PCI DSS.

The PCI DSS applies to all payment card system participants that store or transmit cardholder data or sensitive authentication data, including:

- Merchants.
- Merchant or acquiring banks that process merchant payments.
- Issuing banks that issue payment cards.
- Third-party service providers and processors.

Failure to comply with the PCI DSS can result in significant fines and penalties.

For more information on the card payment system and the PCI DSS requirements, see Practice Notes, The Card Payment System and PCI DSS Compliance.

Cross-Border Issues

There are few limits on the transfer of personal information to countries outside the US. While several US states have enacted laws that limit or discourage outsourcing of data processing beyond US borders, these laws typically apply only to state government agencies and their private contractors. The position of the FTC and other US regulators is that:

- US laws and regulations still apply to personal information after it leaves the US. For example, see the FTC's enforcement action against GMR Transcription Services, Inc., which alleged a medical and legal transcription company outsourced services to independent typists in India without adequately checking to make sure they could implement reasonable security measures (*In re GMR Transcription Serv., Inc.*, No. C-4482, 2014 WL 4252393 (F.T.C. Aug. 14, 2014)). The FTC has cited this case in subsequent reports and guidance to illustrate the strong need for appropriate service provider oversight.

- Regulated entities in the US remain responsible for exported personal information and for the processing of personal information overseas by subcontractors.

- Entities should use the same protections, such as security safeguards, protocols, audits, and contractual provisions, whether the regulated data is located in the US or elsewhere.

However, US businesses that operate multinationally must also comply with the data protection laws in each jurisdiction in which they operate. For example, in contrast to US law, privacy is a fundamental individual right in many European countries. The EU has comprehensive data protection requirements under its **General Data Protection Regulation** (GDPR). For more information on the GDPR, see Practice Note, Overview of EU General Data Protection Regulation.

EU laws provide EU residents with greater data privacy protection and rights to access and control the use of their personal information. EU laws also restrict the transfer of EU personal information to countries outside of the EU that are not deemed to offer adequate protections for data privacy, unless the transfer is made under an approved transfer mechanism. The EU regards the US as a country that does not offer adequate protections.

Before October 2015, many companies relied on the now defunct US-EU Safe Harbor self-certification program as the approved transfer mechanism under which they could transfer data to the US. In part to address issues raised by EU regulators over the Safe Harbor program, Congress enacted the Judicial Redress Act in 2016. That Act gives citizens of certain ally nations, and EU member states in particular, the right to seek redress in US courts for privacy violations when their personal information is shared with law enforcement agencies. Subsequently, the EU and US Department of Commerce agreed to the updated EU-US Privacy Shield self-certification program.

However, on July 16, 2020, the European Court of Justice (ECJ) decision in *Data Protection Commissioner v Facebook Ireland and Maximillian Schrems* (Case C-311/18) EU:C:2020:559, 16 July 2020) (Schrems II) invalidated the EU-US Privacy Shield framework's use as a personal data transfer mechanism under the GDPR and required case-by-case evaluations on whether a recipient country's laws enable or prevent controller-to-processor Standard Contractual Clauses (SCCs) from providing the GDPR's required level of adequate protection for transferred personal data before a controller can rely on that mechanism for specific transfers. For more, see Legal update, Schrems II: controller to processor standard contractual clauses valid but EU-US Privacy Shield invalid (ECJ).

On June 4, 2021, the European Commission adopted an Implementing Decision and Annex with new SCCs for personal data transfers from the EEA to third countries under GDPR Articles 28(7) and 46(2)(c). From June 27, 2021, organizations can use the SCCs for controller-to-controller, controller-to-processor, processor-to-controller, and processor-to-processor transfers. The SCCs include examples of supplementary measures to safeguard personal data transfers to third countries in response to the Schrems II decision. For more information, see Legal Updates:

- European Commission publishes new standard contractual clauses for feedback.

- EDPB and EDPS adopt joint opinions on European Commission's draft sets of standard contractual clauses.
- European Commission adopts final versions of standard contractual clauses under EU GDPR.

On June 18, 2021 the European Data Protection Board (EDPB) adopted its Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, which aim to assist controllers in identifying and implementing supplementary measures to ensure personal data protection that is essentially equivalent to the EU's protections following the Schrems II decision. For more information, see Legal Update, EDPB adopts final version of recommendations on supplementary measures for data transfers to third countries in response to Schrems II (50th Plenary).

On November 19, 2021, the EDPB published draft Guidelines on the Interplay between the application of Article 3 and the provisions on international transfers as per Chapter V of the GDPR (EDPB 05/2021) (Territorial Scope and International Data Transfer Guidelines) which clarify what constitutes an international data transfer under the GDPR. The Territorial Scope and International Data Transfer Guidelines establish criteria to determine if a processing activity qualifies as an international data transfer and provides examples. The public consultation closes on January 31, 2022. For more, see Legal Update, EDPB publishes guidance on interplay between GDPR territorial applicability and international transfers (57th Plenary).

The FTC regularly takes enforcement action against companies that misrepresent their participation in the Privacy Shield and other cross-border data transfer programs, including the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR) system. Despite the Schrems II decision, organizations must continue to meet their publicly stated Privacy Shield obligations for previously transferred EU personal data unless and until they formally withdraw from the framework (see Privacy Shield: Withdrawal from Privacy Shield).

A discussion of data protection laws in other jurisdictions is outside the scope of this Note. For more information on data protection and privacy laws in various jurisdictions, see Country Q&A Tool: Data Protection.

