Mobile Device and Applications Key Laws Chart

by Charles R. Macedo, Amster, Rothstein & Ebenstein LLP and Richard P. Zemsky, Aimcast Edge Corp., with Practical Law Data Privacy & Cybersecurity

Maintained • USA (National/Federal)

A Chart outlining key US federal and state laws applicable to mobile applications (apps). This resource is designed for mobile app developers, operators, and other businesses to help assess their legal compliance obligations in the evolving digital landscape. This Chart covers a wide range of regulatory areas, addressing rules for financial data under the Gramm-Leach-Bliley Act (GLBA), health information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and children's data under the Children's Online Privacy Protection Act (COPPA). It also covers regulations for emerging AI features, state-specific consumer privacy laws like the California Consumer Privacy Act of 2018 (CCPA), and federal laws such as the Federal Trade Commission Act (FTC Act). For each law, this Chart identifies the covered entities, triggering events, and a summary of the core requirements or restrictions, helping users navigate compliance.

This Chart provides a high-level overview of key federal and state statutes applicable to providing mobile applications. Developers, operators, and other stakeholders, including businesses that offer mobile apps, can use this information to assess their legal compliance obligations. This Chart does not comprehensively address every law, regulation, industry standard, or agency guidance that may apply to mobile apps.

Generally Applicable Federal Laws

Statute or Regulation	Covered Entities and Information	Events that Trigger Consideration	Key Requirements or Restrictions
Federal Trade Commission Act (FTC Act) (15 U.S.C. §§ 41 to 58)	Entities whose business affects commerce, except regulated financial institutions and common carriers. The FTC Act prohibits unfair trade practices, which the Federal Trade Commission (FTC) and courts have broadly	The FTC Act applies broadly to mobile apps and devices to protect consumers and also applies to a variety of practices that may implicate unfair trade practices and privacy concerns. The FTC	Developers and operators may not engage in deceptive marketing or other anti-consumer practices and must adopt reasonable privacy practices. For more, see Practice Notes:

	interpreted to include consumer privacy concerns. Similar state unfair practices laws, known as State Mini-FTC Acts, also apply to mobile devices and apps.	provides guidance for developers and businesses offering an app covering a wide range of topics including truth-in-advertising, data security, transparency, and consumer privacy. For a directory of the FTC's mobile guidance, including information on enforcement actions, see the FTC's Mobile Technology Issues page.	• FTC Consumer Protection Investigations and Enforcement. • US Privacy and Data Security Law: Overview: FTC Act.
Sarbanes-Oxley (SOX) (Pub. L. 107–204)	Public companies and accounting firms and their confidential business information.	Accessing or transmitting corporate data from a mobile device or storing corporate data on a mobile device.	Covered entities must implement effective internal controls over mobile devices to protect corporate data.
Electronic Communications Privacy Act (ECPA) (Pub. L. 99–508) (As codified, key sections include the Wiretap Act (18 U.S.C. §§ 2510 to 2523) **Stored Communications Act** (18 U.S.C. §§ 2701 to 2713) Video Privacy Protection Act (VPPA) (18 U.S.C. § 2710))	All persons and communications when electronic or mechanical devices are involved in either transmitting or intercepting them. The VPPA applies to information that identifies a person as having requested or obtained specific video materials or services.	Receiving, accessing, or storing wire, oral, or electronic communications or records of consumer video viewing or rental activity, or when a party accesses such information stored on a device.	• Wiretap Act. Prohibits intercepting communications while in transit using a mobile device and prohibits using or disclosing the contents of any communication obtained illegally. • Stored Communications Act. Prohibits knowingly disclosing communications by certain parties and prohibits unauthorized access to a system used to transmit wire or electronic communications and through that unauthorized access, obtaining, altering, or preventing another's authorized access to a wire or electronic communication stored on the system. • Video Privacy Protection Act. Prohibits disclosure

			of video viewing or rental activity records. For more, see Practice Note, US Privacy Litigation: Overview: Video Privacy Protection Act (VPPA).

Computer Fraud and Abuse Act (CFAA)
 	
(18 U.S.C. § 1030)
	All persons and all information stored on protected computers, which includes mobile devices.	Accessing or damaging a mobile device or engaging in password trafficking or extortion relating to a protected computer.	Prohibits:
			
			• The unauthorized access of:
			  • devices to obtain certain types of prohibited information; and
			  • a protected computer used by or for the federal government or a financial institution, or used in interstate or foreign commerce or communication or is part of a voting system or used for federal elections.
			
			• Knowingly trafficking in device passwords and extortion involving a threat to damage a protected computer.
			
			For more, see Practice Note, Key Issues in Computer Fraud and Abuse Act (CFAA) Civil Litigation.

Generally Applicable State Consumer Privacy Laws

Statute or Regulation	Covered Entities and Information	Events that Trigger Consideration	Key Requirements or Restrictions

California Consumer Privacy Act of 2018 (CCPA) (Cal. Civ. Code §§ 1798.100 to 1798.199.100) The voter-approved California Privacy Rights Act of 2020 (CPRA), amended and expanded the CCPA on January 1, 2023.	Entities that do business in California and meet certain revenue or consumer **personal information** collection thresholds. Entities that control or are controlled by a business meeting the above thresholds and share common branding with that business, such as a shared name, **service mark**, or **trademark**.	Collecting a California resident's personal information. The statute broadly defines personal information to include any information that identifies, relates to, describes, references, is reasonably capable of being associated with, or could reasonably be linked to, directly or indirectly, a particular consumer or household (Cal. Civ. Code §1798.140(v)).	Comprehensive data protection legislation for California residents. Provides specific notice requirements and establishes certain rights regarding personal information, including access, deletion, and opt-out of personal information sales. It also contains anti-discrimination requirements. For more, see: • California Privacy Toolkit (CCPA and CPRA). • Practice Note, Understanding the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA). • Practice Note, California Consumer Privacy Act (CCPA/CPRA) Quick Facts: Overview.
Colorado Privacy Act (CPA) (SB 21-190; Colo. Rev. Stat. Ann. §§ 6-1-1301 to 6-1-1313)	Data controllers conducting business in Colorado or intentionally targeting Colorado residents with goods or services, that also meet certain consumer data processing thresholds.	Collecting a Colorado resident's personal data.	Comprehensive data protection legislation for Colorado residents acting in individual or household contexts. Provides specific notice requirements, requires consent to process sensitive personal data, and establishes certain personal data rights including access, correction, deletion, data portability, and opt-out of personal data sales, targeted advertising,

			or profiling with legal or similarly significant effects. It also contains data minimization, purpose specification, and anti-discrimination requirements. For more, see: • Practice Note, Understanding the Colorado Privacy Act (CPA). • Practice Note, Colorado Privacy Act (CPA) Quick Facts: Overview.
Texas Data Privacy and Security Act (TDPSA) (Tex. Bus. & Com. Code Ann. §§ 541.001 to 541.205).	Persons conducting business in Texas or producing products or services that Texas residents consume.	Processes a Texas resident's personal data.	Comprehensive data protection legislation for Texas residents acting in individual or household contexts. Provides specific notice requirements, requires consent to process sensitive personal data, and establishes certain personal data rights including access, correction, deletion, data portability, and opt-out of personal data sales, targeted advertising, or profiling with legal or similarly significant effects. It also contains data minimization, purpose specification, and anti-discrimination requirements. For more, see Practice Note, Texas Data Privacy and Security Act (TDPSA) Quick Facts: Overview.

Several other states have also passed comprehensive data protection legislation. For more information, see:

- US State Consumer Privacy Laws Toolkit.
- US State Consumer Privacy Laws Chart.
- Quick Compare Chart, State Consumer Privacy Laws - Overview.
- Practice Note, US Privacy and Data Security Law: Overview: State Consumer Privacy Laws.

Content Restriction Laws

Statute or Regulation	Covered Entities and Information	Events that Trigger Consideration	Key Requirements or Restrictions
Digital Millennium Copyright Act (DMCA) (Pub. L. 105-304; 17 U.S.C. § 512)	Requires internet service providers to provide mechanisms for content owners to object to the posting of their copyrighted material on the internet.	Whenever app users can upload content into or by way of a mobile app.	Service providers must provide a mechanism for content owners to submit a notice of objection and must have procedures in place to take down content after a verified objection. For more, see Practice Note, Digital Millennium Copyright Act (DMCA): Safe Harbors for Online Service Providers. For a DMCA takedown notice form, see Standard Document, DMCA Complaint (Takedown Notice).
Communications Decency Act (CDA) (Pub. L. 104-104; 47 U.S.C. § 230)	Internet service providers. Regulates the transmission of obscene and defamatory content.	Knowingly distributing obscene material.	Covered parties must provide notice to recipients of the option to block obscene material. The statute prevents service providers and users from being treated as the publisher or speaker of information provided by another information content provider.

Laws that Regulate AI

Statute or Regulation	Covered Entities	Events that Trigger Consideration	Key Requirements or Restrictions
California AI Transparency Act (SB 942, as amended by AB 853; Cal. Bus. & Prof. Code §§ 22757 to 22757.6, effective August 2, 2026)	• Large AI systems providers (entities that create, code, or otherwise produce a publicly accessible generative AI system with over 1,000,000 monthly visitors or users). • Internet websites and applications that provide AI systems, including source code downloads.	Make AI systems available to consumers.	Large AI systems providers must: • Provide a free, publicly accessible AI detection tool for users that meets specific requirements, including identifying whether the provider's AI system created or altered the submitted content. • Enable users to make a disclosure that the user's content is AI-generated. • Include a "latent" disclosure that meets specific criteria, including the AI system provider's name and the AI system name and version. Large AI systems providers cannot: • Collect or retain detection tool users' personal information. • Retain content submitted to the AI detection tool for

			longer than needed to operate the tool. • Retain personal data embedded into content submitted to the AI detection tool or its metadata for purposes of verifying content authenticity, origin, or modification history. Beginning January 1, 2027, internet websites and apps cannot knowingly provide AI systems without the required disclosures.
Colorado AI Regulation (SB 24-205, delayed by SB 25-004; C.R.S.A. § 6-1-1701 to 1707, effective June 30, 2026)	Developers and deployers of an AI system that it intends to interact with consumers.	Deploying, selling, offering, leasing, giving, or otherwise making available an AI system intended to interact with consumers.	Must disclose to consumers that they are interacting with an AI system. Additional obligations and requirements apply to high-risk AI systems. See Legal Update, Colorado Enacts Comprehensive AI Legislation Targeting Discrimination.
Maine Act to Ensure Transparency in Consumer Transactions Involving Artificial Intelligence (HP 1154)	Entities using an AI chatbot or other computer technology to engage in trade and commerce with a consumer.	Using an AI chatbot or other computer technology to engage in trade and commerce with a consumer in a manner that may mislead or deceive a reasonable consumer into believing they are engaging with a human being.	Must notify the consumer that they are **not** engaging with a human being.
Texas Responsible Artificial Intelligence Governance Act (HB 149; Tex. Bus. & Com. Code Ann. §§ 554.001 to 554.102)	Entities that deploy AI systems for use in Texas (deployers) and persons who develop an AI system to offer, sell, lease, give, or otherwise provide the system in Texas (developer).	• Developing or deploying an AI system. • A governmental entity making available an AI system intended	Requires informing consumers when an AI system is used in relation to health care service or treatment.

	Texas state governmental entities, except hospital districts created under Texas's health and safety code and higher education institutions.	to interact with consumers.	Prohibits developing or deploying an AI system that intentionally aims to: • Encourage or cause a person to harm themselves or others or commit criminal activity. • Violate an individual's constitutional rights. • Discriminate against a protected class in violation of state or federal law. • Produce or distribute explicit images or sexual text-based conversations. Prohibits governmental entities from certain social scoring that results in infringing a US or Texas constitutional right or law, identifying specific individuals using biometric data, or collecting images of an individual in violation of US or Texas constitutional right or law.
Utah Artificial Intelligence Consumer Protection Amendments (SB 226; 2025 Utah Laws Ch. 465)	• Individuals providing services in certain regulated professions, including, but not limited to, architects, engineers, plumbers, physicians, nurses, dentists, pharmacists, real estate, mortgage brokers, investment advisors, social workers, inspectors,	Using generative AI to interact with an individual in connection with a consumer transaction.	Requires regulated occupations to prominently disclose any generative AI use in connection with a consumer transaction if either: • The AI use constitutes a high-risk use case, such as collecting sensitive personal information (health,

	interior designers, and accountants (regulated occupations). • Other sellers, lessors, offerors, brokers, assignors, and other entities that regularly engage in consumer transactions but are not providing services in regulated occupations (non-regulated occupations).		financial, or biometric data). • The AI use provides personalized recommendations or information that a consumer could reasonably rely on to make significant personal decisions, such as financial advice or services, legal advice or services, or mental health advice or services. • Other use cases that the Utah Division of Consumer Protection sets out in a rule. Requires that non-regulated occupations disclose any generative AI use in connection with a consumer transaction, if asked by the consumer.

For more information on AI regulation, see AI Toolkit (US) and Practice Note, AI Key Legal Issues: Overview (US).

Laws that Apply to Financial Information

Statute or Regulation	Covered Entities and Information	Events that Trigger Consideration	Key Requirements or Restrictions
Restore Online Shoppers' Confidence Act (ROSCA) (Pub. L. 111-345; 15 U.S.C. §§ 8402(b) and 8403))	Merchants that obtain financial information through processing online transactions.	Employing negative option marketing on the internet or facilitating third-party post-transaction sales.	Requirements include: • A merchant may not disclose customer billing information to any third-party seller for use in an internet-

			based sale from that third-party seller.
			• Before attempting to charge a customer through a negative option feature, the seller must:
			  • clearly disclose all material terms of the transaction before obtaining billing information;
			  • obtain the customer's express informed consent before charging the customer; and
			provide mechanisms for the customer to stop recurring charges.

Gramm-Leach-Bliley Act (GLBA) (Pub. L. 106-102) (15 U.S.C. §§ 6801 to 6827; 12 C.F.R. §§ 1016.1 to 1016.17; 70 Fed. Reg. 15,736 (March 29, 2005))	Financial institutions (broadly defined to include virtually any entity that provides consumer financial products or services) that hold non-public **personally identifiable information** (NPI). Service providers to financial institutions also have compliance obligations.	Disclosing NPI about a consumer to a nonaffiliated third party. The Financial Privacy Rule covers the use, collection and disclosure of NPI. The Safeguards Rule covers security measures financial institutions must take to protect NPI.	• The Financial Privacy Rule. The covered entity must provide notice of its privacy policies and practices initially and on an annual basis and allow the consumer to opt out of the disclosure of consumer information. • The Safeguards Rule. The covered entity must implement appropriate administrative, technical, and physical

			safeguards to protect NPI, including, for example: • implementing a written information security program; • notifying the SEC in the event of notification event that affects at least 500 customers; • appointing a person to be in charge of security of NPI; and • conducting a risk assessment. Covered entities report to the SEC certain security events that affect at least 500 customers. For more, see Practice Note, GLBA: The Financial Privacy and Safeguards Rules.

Laws that Apply to Health or Medical Information

Statute or Regulation	Covered Entities and Information	Events that Trigger Consideration	Key Requirements or Restrictions
Health Insurance Portability and	HIPAA covered entities, which are:	Collecting, creating, using, storing, maintaining, or	Covered entities and their Bas must implement

Accountability Act of 1996 (HIPAA) and **Health Information in Technology for Economic and Clinical Health Act** (HITECH)
 	
(Pub. L. 104-191 and Pub. L. 111–5)
 	
(42 U.S.C. §§ 1320d-2(d), 17921 to 17953; 45 C.F.R. §§ 164.302 to 164.534)
	• Health plans.
	• Health care clearinghouses.
	• Health care providers.
	
	Covered entities' business associates (BAs), for example service providers, must also comply with HIPAA. HIPAA applies to **protected health information** (PHI), which generally includes health and medical information.
		transmitting PHI. The HIPAA Privacy Rule governs the privacy of PHI, and the HIPAA Security Rule imposes obligations specific to the security of electronic PHI.	appropriate administrative, technical, and physical safeguards to protect PHI.
			• Privacy Rule. Requirements include:
			  • notifying individuals about their privacy rights and how their information can be used;
			  • adopting and implementing privacy procedures;
			  • designating a privacy officer; and
			  • securing PHI.
			• **Security Rule.** Requirements include:
			  • ensuring that workforce complies with the Security Rule; and
			  • protecting against reasonably anticipated threats or hazards to the security or integrity of ePHI or uses or disclosures of ePHI that are

			not permitted or required. For more, see Practice Notes: • HIPAA Privacy Rule. • HIPAA Security Rule: Overview and Administrative Safeguards. • HIPAA Privacy and Security (Individual Rights): Right of Access to PHI. • HIPAA Privacy and Security (Individual Rights): Right of Accounting and Other Rights. • HIPAA Enforcement: Penalties and Investigations. • HIPAA Breach Notification Rules.
Food and Drug Administration Act (Mobile Medical Applications) (21 U.S.C. § 360c)	Health and medical information maintained by mobile apps that meet the definition of a medical device and all entities other than those that are HIPAA-regulated.	A mobile app that is used as an accessory to a medical device or as medical device software.	Apps may be required to obtain **Food and Drug Administration** (FDA) approval under a risk-based approach in certain circumstances. For more, see: • FDA: Device Software Functions Including Mobile Medical Applications.

			• FDA Report, Policy for Device Software Functions and Mobile Medical Applications. (September 2019). • The FTC's Mobile Health Apps Interactive Tool, produced in cooperation with the FDA and other federal agencies.
FTC's Health Breach Notification Rule (16 C.F.R. §§ 318.1 to 318.9)	Vendors of personal health records (PHR), which are electronic records of identifiable health information on an individual that can be drawn from multiple sources and that are managed, shared, and controlled by or primarily for the individual. The rule covers vendors' service providers but does not apply to HIPAA covered entities.	An unauthorized acquisition of unsecured individually identifiable PHR information.	Covered party must notify: • Each affected person who is a US citizen or resident. • The FTC. • The media, if the breach affects at least 500 residents of a particular state or US territory. For more, see Practice Note, US Privacy and Data Security Law: Overview: Entities Subject to the FTC Act and Legal Update, FTC Warns Health Apps to Comply with its Health Breach Notification Rule; FTC: Complying with the FTC's Health Breach Notification Rule.
Washington's My Health My Data Act	Entities that both: • Conduct business in Washington or provide products or services targeted	Either: • Collecting consumer health data (defined broadly as personal information, including	Health data privacy protections for Washington residents acting in individual or household contexts. Provides specific notice requirements, requires consent to process or

	to Washington consumers. • Alone or with others, determine the purpose and means of collecting, processing, sharing, or selling consumer health data.	a persistent unique identifier, that is linked or reasonably linkable to a consumer and identifies the consumer's past, present, or future physical or mental health status). Geofencing around an entity that provides in-person health care services to identify or track consumers, collect consumer health data, or send consumers health care service-related notification or messages, including ads.	disclose health data, and establishes certain personal data rights including access and deletion. It also contains data minimization and purpose specification requirements. For more, see Practice Note, Understanding the Washington My Health My Data Act.
Nevada's Consumer Health Data Privacy Law (NRS 603A.400 to 603A.550)	Entities that both: • Conduct business in Nevada or provide products or services targeted to Nevada consumers. • Alone or with others, determine the purpose and means of collecting, processing, sharing, or selling consumer health data.	Either: • Collecting consumer health data (defined broadly as personal information, including a persistent unique identifier, that is linked or reasonably linkable to a consumer and identifies the consumer's past, present, or future health status). • Geofencing around an entity that provides in-person health care services to identify or track consumers, collect consumer health data, or send consumers health care service-related notification or messages, including ads.	Health data privacy protections for Nevada residents acting in individual or household contexts. Provides specific notice requirements, requires consent to process or disclose health data, and establishes certain personal data rights including access and deletion. It also contains data minimization and purpose specification requirements.

Laws that Apply to Commercial Messages

Statute or Regulation	Covered Entities and Information	Events that Trigger Consideration	Key Requirements or Restrictions

Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act)
 	
(15 U.S.C. §§ 7701 to 7713)
	Commercial emails and anyone who sends them.	Sending a commercial email message.	• Prohibits the transmission of commercial emails that contain false or misleading transmission information or deceptive subject headings.
			
			• Commercial emails must:
			  • state that the message is an advertisement or solicitation;
			  • include an unsubscribe mechanism; and
			  • disclose the sender's physical postal address.
			
			• Includes restrictions on initiations of commercial emails containing sexually oriented material.
			
			• Prohibits the sending of commercial messages to certain email addresses provided by wireless carriers specifically

			for mobile messaging services. For more, see Practice Note, CAN-SPAM Act Compliance.
Telephone Consumer Protection Act (TCPA) (47 U.S.C. § 227; 47 C.F.R. § 64.1200(a))	Subject to certain exceptions, any person or entity that initiates a call: • Using an automated telephone dialing system or artificial or prerecorded voice. • For advertising or marketing purposes.	Sending a commercial message that will be received on a mobile device.	Requires prior express written consent of person being called. For more, see Practice Notes: • Telephone Consumer Protection Act (TCPA): Overview. • TCPA Litigation: Key Issues and Considerations.

Laws that Apply to Information of Minors and Students

Statute or Regulation	Covered Entities and Information	Events that Trigger Consideration	Key Requirements or Restrictions
Children's Online Privacy Protection Act (COPPA) (15 U.S.C. §§ 6501 to 6506)	Website and online service operators, including mobile app operators that operate child-directed services or have reason to know that children use their services.	Collecting personal information from children under age 13.	• Must make available a privacy policy that identifies how the collected information is used. • Obtain verifiable parental consent. • Provide parents with the opportunity to: • review and change their children's personal information;

			• prevent its further use; and • require its deletion. For more, see: • Practice Note, Children's Online Privacy: COPPA Compliance. • Children's Online Privacy Protection Act (COPPA) Compliance Checklist. • Standard Document, Children's (COPPA) Privacy Policy Notice.
Federal Education Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 C.F.R. §§ 99.1 to 99.67)	Schools receiving federal funding. For a full description of covered educational institutions, see 34 C.F.R. § 99.1. Some FERPA provisions apply to education service providers that receive student educational records or personally identifiable information (PII) from a covered educational institution.	Collecting or maintaining students' education records, including: • Grades and transcripts. • Class rosters. • Biographical information, including date of birth, Social Security number, and address. • Medical or health records. • Financial information. • Disciplinary records.	• Requires prior written consent for disclosure, subject to specific exceptions. • Provides rights to parents and eligible students regarding their education records and PII, including: • access, inspection, and review; • correction; and • prevent disclosure absent prior

			written consent in most cases. • Designates a subset of education record information, called directory information, for special treatment, including permitting disclosure without prior written consent (20 U.S.C. § 1232g(a)(5); 34 C.F.R. § 99.37). For more, see Practice Note, Student Privacy: Education Service Provider Requirements.
State Student Privacy Laws	Varies by state.	Varies by state.	For more, see: • Practice Note, Student Privacy: Education Service Provider Requirements. • Practice Note, Student Privacy State Laws for Education Service Providers Chart: Overview.
Children's and Teens' Data and Social Media Safety Laws	Varies by state; typically applies to social media platforms.	Varies by state.	Varies by state; requirements include prohibiting account creation by minors without parental consent, verifying account creator age, and deleting minors' data. For more, see: • Children's and Student Privacy Laws Toolkit.

			• Practice Note, US Children's Privacy Legislation Tracker. • Article, Trends in Data Privacy and Cybersecurity: 2024: Children's and Teens' Data and Social Media Safety Laws.
California Digital Age Assurance Act (AB 1043; Cal. Civ. Code §§ 1798.500 to 1798.505, effective January 1, 2027)	Operating system (OS) providers. App distributors (app stores). App developers.	User creates an account on an app store. User downloads a developer's app.	OS providers must provide user age bracket data (under 13 years; 13 to 15 years; 16 to 17 years; 18 years and older) to app stores via API. Developers must request user age bracket from OS providers and app stores when a user downloads their app.
Texas App Store Accountability Act (SB 2420; Tex. Bus. & Com. Code Ann. §§ 121.001 to 121.102 (was to go into effect January 1, 2026, but enactment, implementation, and enforcement enjoined by preliminary injunction on Dec. 23, 2025 (*Computer & Communications Industry Ass'n v. Paxton*, 2025 WL 3754045 (W.D. Tex. 2025)))	App distributors (app stores).	User creates an account on an app store.	App stores must: • Verify user age by age bracket (under 13 years; 13 to 15 years; 16 to 17 years; 18 years and older). • Require that each minor's account be linked with a parent or legal guardian's account. • Obtain parental or legal guardian consent for any minor to download or purchase an app and for any in-app purchases. • Notify app developers when a parent or legal

			guardian revokes consent. • Use industry-standard encryption protocols to ensure personal data integrity and confidentiality.

Other Privacy and Security Laws

Statute or Regulation	Covered Entities and Information	Events that Trigger Consideration	Key Requirements or Restrictions
The California Online Privacy and Protection Act (CalOPPA) (Cal. Bus & Prof. Code §§ 22575 to 22579)	Operators of commercial websites and online services that collect California residents' personally identifiable information (PII), including any identifier that permits the online or physical contacting of a specific individual, through a website or mobile app. Other similar state laws may also apply to mobile devices and apps.	Collecting California residents' PII.	Requires: • Conspicuous posting of privacy policies. • Disclosures regarding how the operator responds to do-not-track signals and third-party access to PII. For more, see Practice Note, California Privacy and Data Security Law: Overview: Online and Mobile Privacy.
State Data Breach Notification, Data Security and Records Disposal Statutes	Those doing business within the state that collect or otherwise have in their possession, PII. The definition of PII varies by state, but typically consists of an individual's name plus one or more data elements, such as: • Social Security number.	Collecting, storing, maintaining, or transmitting PII.	• Data breach laws. Require notice to consumers, entities on whose behalf a breached entity holds PII, and sometimes regulators or consumer reporting agencies, in the event of an incident that compromises the security or

	• Driver's license or state identification number. • Financial account information sufficient to access an individual's account. • Health or medical information. (See State Data Breach Laws Protected Personal Information Chart: Overview.)		confidentiality of PII. For more, see: • Practice Note, Cyber Incident and Data Breach Notification; and • Data Breach Notification Laws: State Q&A Tool. • Data security laws. Require data holders to take certain actions to protect PII. • Records disposal laws. Requires secure disposal of certain records under specified circumstances.
State Biometric Privacy Laws	Those doing business within the state that collect or otherwise have in their possession biometric data.	Collecting, storing, or disclosing biometric data.	Provides specific notice and consent requirements and establishes restrictions on disclosures and sales. For more, see: • Practice Note, Biometric Data Laws: Overview. • Quick Compare Chart, State Biometric Laws - Biometric Data Obligations.
FCC's Customer Proprietary Network Information (CPNI) Breach Notification Rule	Telecommunications and interconnected Voice over Internet Protocol (VoIP) carriers and	A breach, including an inadvertent breach, of data collected on wireless devices, including location	Carrier must:

(47 C.F.R. § 64.2011)	telecommunications relay services (TRS) providers when they experience a breach of personally identifiable information (PII) or certain phone record information such as call logs, call duration, and phone numbers.	information about where a call starts and ends.	• Notify law enforcement. • Notify customers or disclose the breach. • Maintain records of any breaches. For more, see Practice Note, Cyber Incident and Data Breach Notification: The FCC CPNI Breach Rule.

