Mobile Device and Applications Key Laws Chart

CHARLES R. MACEDO AND RICHARD P. ZEMSKY, AMSTER, ROTHSTEIN & EBENSTEIN LLP
WITH PRACTICAL LAW INTELLECTUAL PROPERTY & TECHNOLOGY

A chart listing key statutes and regulations that apply to mobile devices and mobile applications (apps). It provides an overview of the circumstances that trigger application of each statute or regulation as well as key requirements and restrictions.

This Chart provides a high-level overview of key statutes that mobile app developers, operators and other stakeholders, including businesses that use mobile devices, should consider when assessing their legal compliance obligations. This Chart does not address every law that may apply to mobile devices or apps or industry standards or guidance.

Statute or Regulation	Covered Entities and Information	Events that Trigger Consideration	Key Requirements or Restrictions
GENERALLY APPLICABLE LAWS			
Federal Trade Commission Act (FTC Act) (*15 U.S.C §§ 41-58*)	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 interpreted to include consumer privacy concerns. Similar state unfair practices laws, known as State Mini-FTC Acts, also apply to mobile devices and apps.	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 provides guidance for developers covering a wide range of topics including truth-in-advertising, data security 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.	Developers and operators may not engage in deceptive marketing or other anti-consumer practices and must adopt reasonable privacy practices (see *Practice Notes, FTC Consumer Protection Investigations and Enforcement (http://us.practicallaw.com/4-549-3090)* and *US Privacy and Data Security Law: Overview (http://us.practicallaw.com/6-501-4555)*).
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.

Courtesy of Amster, Rothstein & Ebenstein, LLP

Statute or Regulation	Covered Entities and Information	Events that Trigger Consideration	Key Requirements or Restrictions
Electronic Communications Privacy Act (ECPA) (*Pub. L. 99–508*) (As codified, key sections include the **Wiretap Act** (*18 U.S.C. §§ 2510-2522*) **Stored Communications Act** (*18 U.S.C. §§ 2701-2709*); and **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 records.

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;
			  ■ a protected computer used by or for the federal government or a financial institution, or used in interstate or foreign commerce or communication.
			■ Knowingly trafficking in device passwords and extortion involving a threat to damage a protected computer.

CONTENT RESTRICTION LAWS			
Digital Millennium Copyright Act (DMCA) (*Pub. L. 105-304*)	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 (see *Practice Note, Digital Millennium Copyright Act (DMCA): Safe Harbors for Online Service Providers (http://us.practicallaw.com/1-518-6907))*. For a form of DMCA takedown notice, see *Standard Document, DMCA Complaint (Takedown Notice) (http://us.practicallaw.com/3-502-6258).*
Communications Decency Act (CDA) (*Pub. L. No. 104-104*)	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.

Statute or Regulation	Covered Entities and Information	Events that Trigger Consideration	Key Requirements or Restrictions
LAWS THAT APPLY TO FINANCIAL INFORMATION			

Restore Online Shoppers' Confidence Act (ROSCA)
 	
(*Pub. L. 111–345*)
	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*)
	Financial institutions (which is 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;
			  ■ appointing a person to be in charge of security of NPI; and
			  ■ conducting a risk assessment.
			
			(See *Practice Note, GLBA: The Financial Privacy and Safeguards Rules (http://us.practicallaw.com/4-578-2212).*)

Statute or Regulation	Covered Entities and Information	Events that Trigger Consideration	Key Requirements or Restrictions
LAWS THAT APPLY TO HEALTH OR MEDICAL INFORMATION			

Health Insurance Portability and Accountability Act of 1996 (HIPPA) and **Health Information in Technology for Economic and Clinical Health Act (HITECH)**
 	
(*Pub. L. 104-191* and *Pub. L. 111–5*)
	HIPAA covered entities, which are:
	■ 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.
		Collecting, creating, using, storing, maintaining or 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.	Covered entities and their BAs must implement 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.
			
			(See *Practice Notes, HIPAA Enforcement: Penalties and Investigations (http://us.practicallaw.com/2-519-1055)*, *HIPAA Privacy Rule (http://us.practicallaw.com/4-501-7220)*, *HIPAA Security Rule (http://us.practicallaw.com/5-502-1269)* and *HIPAA Breach Notification Rules (http://us.practicallaw.com/1-532-2085).*)

Food and Drug Administration Act (Mobile Medical Applications)	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 FDA approval under a risk-based approach in certain circumstances (see the FDA's *Mobile Medical Applications: Guidance for Industry and Food and Drug Administration Staff.*)
FTC's Health Breach Notification Rule (*16 C.F.R. §§ 318.1 - 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. (See the FTC's *Complying with the FTC's Health Breach Notification Rule.*)

Statute or Regulation	Covered Entities and Information	Events that Trigger Consideration	Key Requirements or Restrictions
LAWS THAT APPLY TO COMMERCIAL MESSAGES			

Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act)
 	
(*15 U.S.C. §§ 7701-13*)
	Commercial e-mails and anyone who sends them.	Sending a commercial e-mail message.	■ Prohibits the transmission of commercial e-mails that contain false or misleading transmission information or deceptive subject headings.
			■ Commercial e-mails must include:
			  ■ that the message is an advertisement or solicitation, plus the sender's physical postal address;
			  ■ an unsubscribe mechanism; and
			  ■ the sender's postal address.
			■ Includes restrictions on initiations of commercial e-mails containing sexually oriented material.
			■ Prohibits the sending of commercial messages to certain e-mail addresses provided by wireless carriers specifically for mobile messaging services.
			
			(See *Practice Note, CAN-SPAM Act Compliance (http://us.practicallaw.com/0-503-5278).*)

Telephone Consumer Protection Act (TCPA) (*47 U.S.C. § 227* and regulations at *47 C.F.R. § 64.1200(a)*)	Subject to certain exceptions, to 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.
LAWS THAT APPLY TO INFORMATION OF MINORS AND STUDENTS			

Children's Online Privacy Protection Act (COPPA)
 	
(*15 U.S.C. §§ 6501-6506*)
	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:
			  ■ the ability to review and change their children's personal information;
			  ■ prevent its further use; and
			  ■ require its deletion.
			
			(See *Practice Note, Children's Online Privacy: COPPA Compliance (http://us.practicallaw.com/1-555-6526), Children's Online Privacy Protection Act (COPPA) Compliance Checklist (http://us.practicallaw.com/0-528-7426)* and *Standard Document, Children's (COPPA) Privacy Policy Notice (http://us.practicallaw.com/8-551-3350).*)

Statute or Regulation	Covered Entities and Information	Events that Trigger Consideration	Key Requirements or Restrictions
OTHER PRIVACY AND SECURITY LAWS			
The California Online Privacy and Protection Act (CalOPPA) (*Cal. Bus. & Prof. Code §§ 22575-22579*)	Operators of commercial websites and online services that collect California residents' 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. (See *California Privacy and Data Security Laws: Overview: Online and Mobile Privacy (http://us.practicallaw.com/6-597-4106).*)
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. PII varies by state, but typically consists of an individual's name plus one or more data elements, such as: ■ Social Security number. ■ Driver's license or state identification number. ■ Financial account information sufficient to access an individual's account. ■ Health or medical information.	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, in the event of an incident that compromises the security or confidentiality of PII (see *Practice Note, Breach Notification (http://us.practicallaw.com/3-501-1474)* and *Data Breach Notification Laws: State Q&A Tool (http://us.practicallaw.com/3-578-0925)*). ■ **Data security laws.** Require data holders to take certain actions to protect PII. ■ **Records disposal laws.** Require certain records to be securely disposed of under specified circumstances.
FCC's Customer Proprietary Network Information (CPNI) Breach Notification Rule (*47 C.F.R.§§ 64.2011*)	Telecommunications carriers when they experience a breach of certain phone record information such as call logs, call duration and phone numbers.	A breach of data collected on wireless devices, including location information about where a call starts and ends.	Carrier must: ■ Notify law enforcement. ■ Notify customers or disclose the breach, but not until after law enforcement is notified. ■ Maintain records of any breaches.

06-15