Selected Important Privacy Laws for Businesses

Federal Laws

Cable Communications Policy Act
47 U.S.C. § 551

Requires that cable television operators provide their subscribers with a written statement describing the nature of personally identifiable information it collects; the use, disclosure and maintenance of such information; and the subscribers' ability to access such information. Permits cable television operators to collect personally identifiable information from subscribers only to render services to the subscriber or detect unauthorized reception of cable communications, or with the subscriber's consent, and limits the disclosure of such information. Permits subscribers to bring civil actions in federal court, and provides for actual damages (of not less than $100/day or $1000, whichever is higher), punitive damages and reasonable attorneys' fees and other litigation costs.

Children's Online Privacy Protection Act of 1998
15 U.S.C. § 6501-6506; 16 C.F.R. § 312.1-312.12

Applies to the collection of personal information from children under the age of thirteen. Generally, it prohibits the operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting information from children, from collecting personal information without meeting certain requirements (e.g., obtaining verifiable parental consent, providing information about what information is collected and how it is used, etc.). Also requires that these operators post a notice of their information practices with regard to children.

Computer Fraud and Abuse Act
18 U.S.C. §1030

Among other things, prohibits (1) intentionally accessing a computer without authorization (or in excess of any authorization) to obtain information, (2) knowingly, and with intent to defraud, accessing a computer without authorization (or in excess of any authorization), where such conduct furthers the intended fraud and obtains anything of value, and (3) intentionally causing damage to a computer, or intentionally accessing a computer without authorization and causing damage. Creates a private cause of action (generally, for losses at least $5,000 in value) and provides for criminal penalties.

CFAA claims have been used in the following contexts, among others:

- Trade secret misappropriation
- Unfair competition and online misconduct
  - *Register.com Inc. v. Verio, Inc.*, 126 F. Supp. 2d 238 (S.D.N.Y. 2000), and *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001) – use of robots to obtain information from public websites
- Click fraud
- Improper use of cookies
- Improper collecting and sharing of information by social network
  - Alleged in *Hibrick v. Google*, involving Google Buzz
- Cyberbullying
  - The CFAA theory was ultimately rejected in the Lori Drew case, *United States v. Drew,* 257 F.R.D. 449 (C.D. Cal. 2009).

Electronic Communications Privacy Act
18 U.S.C. § 2701 et seq.

Protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers. Generally prohibits communications providers from disclosing customer information except via legal processes. Applies to email, telephone conversations, and data stored electronically. Consists of three titles:

> (1) The Wiretap Act addresses the interception and disclosure of communications content in transit;
>
> (2) The Stored Communications Act regulates access and disclosure of communications content and records in electronic storage; and
>
> (3) The Pen Register and Trap and Trace Device Act regulates the interception and access of non-content identifying information.

Depending on the type of conduct, violations (both interception and wrongful disclosures) may result in criminal penalties and/or civil actions.

Some exceptions exist to the general rule that communications providers may not intercept or disclose information except under warrant and court order:

- Service Provider exception. Providers may intercept communications as "necessarily incident" to "rendition of service" or to "protection of [provider's] rights or property"
- Business use exception. Permits actions taken in "ordinary course of business"; court decisions split as to coverage on this exception
- Consent exception. One-party consent permitted, except for criminal or tortious purposes

Because the ECPA was last significantly amended before widespread use of the Internet began, and because of the difficulty of applying it to new technologies (e.g., cloud computing), Congress and various interest groups have begun considering possible reform or rewriting of the act.

Gramm-Leach-Bliley Act
15 U.S.C. § 6801 et seq.

Requires that financial institutions provide notices to their customers about their information-collection and sharing practices, and restricts their ability to disclose a consumer's personal financial information to nonaffiliated third parties. Requires financial institutions to provide consumers with a notice and opt-out opportunity before they may disclose information to nonaffiliated third parties. Provides specific exceptions under which a financial institution may share customer information with a third party and the consumer may not opt out.

Health Insurance Portability and Accountability Act
Pub. Law No. 104-191 §§ 262, 264; 45 C.F.R. §§160-164

Regulates the use and disclosure of protected health information by "covered entities" (i.e., health care providers, health plans, and health care clearinghouses). Generally, requires that covered entities protect the privacy of protected health information; regulates how covered entities can use and disclose such information; provides patients the ability to receive a copy of the records that covered entities keep about them, and to amend their personal health information; and allows patients to obtain an accounting of personal health information disclosures, and to request that covered entities restrict the use and disclosure of such information. Requires that covered entities have a Privacy Officer, enter agreements with business associates that provide services on their behalf, and punish employees that violate their privacy policies and procedures. Provides for criminal penalties and civil fines up to $1.5 million/year.

Telephone Consumer Protection Act
47 U.S.C. § 227

Restricts telemarketing calls and the use of automatic telephone dialing systems and artificial or prerecorded voice messages, and the sending of unsolicited advertisements by fax. Requires that telemarketers maintain a list of people that request not to receive future telephone solicitations, and that the telemarketers honor such requests for 5 years. Creates a private cause of action, including statutory damages.

Video Privacy Protection Act
18 U.S.C. § 2710

Generally prohibits video sale and rental companies from disclosing personally identifiable information regarding consumers, unless the disclosure is required by law or the consumer has provided consent. Disclosure of the names and addresses of consumers is permitted if the video sale/rental company gave consumers the opportunity to prohibit such disclosure, and the disclosure does not identify the title, description or subject matter of the videos (though the disclosure may include the subject matter of such materials if the disclosure is for the exclusive use of marketing goods and services directly to the consumer). Also requires the destruction of personally identifiable information as soon as practicable after it is no longer needed for the purpose for which it was collected. Creates a private cause of action, including the possibility of actual damages of not less than $2500, punitive damages, reasonable attorneys' fees and other litigation costs, and other equitable relief.

State Laws

Common Law Causes of Action

Possible causes of action for invasion of privacy, public disclosure of private facts, defamation, and breach of duty of confidentiality. Remedies may include monetary damages, injunctive relief, and other damages.

- "Public disclosure of private facts" claims can be brought whenever facts that are highly offensive to a reasonable person are published, without the subject's consent, unless the publication relates to a matter of legitimate public concern.

Computer Hacking Statutes

Prohibit tampering with computers or accessing certain computerized records without authorization. May provide criminal penalties and/or civil damages.

Missouri Statutes:

- Mo. Rev. Stat. § 569.095-569.099: Broadly defines crime of tampering with computer data. Covered acts include accessing, modifying, disclosing, receiving or using computer data or programs.
- Mo. Rev. Stat. § 537.525: Civil remedy provision.

Illinois Statutes:

- 720 ILCS 5/16D-1 et seq.: Creates crime of computer tampering for access to a computer or network in excess of authorization; creates civil remedy.

Data Breach Statutes

Require businesses to notify consumers when a data breach has occurred. A breach is generally defined as the unauthorized acquisition of personal information, which is often defined as a name in combination with certain other data (e.g., a social security or account number). May also specify the manner in which notice is to be given (e.g., written, electronic, etc.). Select state statutes are summarized below:

California Statute:

- Cal. Civ. Code § 1798.29: Generally, must provide notice without delay, in most expedient time possible. Depending on the circumstances, may provide written notice, electronic notice, conspicuous posting on entity's website, or notification to major statewide media.
- California Office of Privacy Protection published Recommended Practices on Notice of Security Breach Involving Personal Information, which summarizes applicable laws and provides a sample notice letter. Available at www.privacyprotection.ca.gov/res/docs/pdf/COPP_Breach_Reco_Practices_6-09.pdf.

Illinois Statute:

- 815 ILCS 530/1 to 530/30: Must notify affected Illinois residents of breach in most expedient time possible, without delay and at no charge to the resident. Depending on the circumstances, may provide written notice, electronic notice, conspicuous posting on entity's website, or notification to major statewide media.

Missouri Statute:

- Mo. Rev. Stat. § 407.1500: Must notify affected consumers of the security breach without unreasonable delay and consistent with needs of law enforcement unless, after appropriate investigation or consultation with law enforcement, the entity determines that a risk of identity theft or other fraud to consumer is not reasonably likely to occur.
- Requires a clear and conspicuous notice that includes a description of the following:
  - the incident in general terms;
  - the type of personal information that was obtained as result of breach;
  - a phone number that consumer may call for further information and assistance, if one exists; and
  - contact information for consumer reporting agencies.
- Depending on the circumstances, may provide written notice, electronic notice, telephonic notice, conspicuous posting on entity's website, or notification to major statewide media.

Online Privacy Policy Laws

Require website operators to post online privacy policies.

California's Online Privacy Protection Act:

- Cal. Bus. & Prof. Code §§ 22575-22579: Requires operators of commercial websites that collect personal information from California residents through the Internet to conspicuously post a privacy policy on their website. The privacy policy must identify the categories of personally identifiable information collected, the categories of third parties with whom the operator may share the information, the process by which consumers may review and request changes to any of his/her personally identifiable information, and its effective date.