Applicable law[edit]

United States[edit]

Main article: Privacy laws of the United States

While no generally applicable law exists, some federal laws govern privacy policies in specific circumstances, such as:

- The Children's Online Privacy Protection Act (COPPA)[13] affects websites that knowingly collect information about or targeted at children under the age of 13.[14] Any such websites must post a privacy policy and adhere to enumerated information-sharing restrictions[15] COPPA includes a "safe harbor" provision to promote Industry self-regulation.[16]
- The Gramm-Leach-Bliley Act[17] requires institutions "significantly engaged"[18] in financial activities give "clear, conspicuous, and accurate statements" of their information-sharing practices. The Act also restricts use and sharing of financial information.[19]
- The Health Insurance Portability and Accountability Act (HIPAA) privacy rules[20] requires notice in writing of the privacy practices of health care services, and this requirement also applies if the health service is electronic.[21]

Some states have implemented more stringent regulations for privacy policies. The California *Online Privacy Protection Act of 2003 – Business and Professions Code sections 22575-22579* requires "any commercial websites or online services that collect personal information on California residents through a web site to conspicuously post a privacy policy on the site".[22] Both Nebraska and Pennsylvania have laws treating misleading statements in privacy policies published on websites as deceptive or fraudulent business practices.[23]

Canada[edit]

Canada's federal Privacy Law applicable to the private sector is formally referred to as Personal Information Protection and Electronic Documents Act (PIPEDA). The purpose of the act is to establish rules to govern the collection, use, and disclosure of personal information by commercial organizations. The organization is allowed to collect, disclose and use the amount of information for the purposes that a reasonable person would consider appropriate in the circumstance.[24]

The Act establishes the Privacy Commissioner of Canada as the Ombudsman for addressing any complaints that are filed against organizations. The Commissioner works to resolve problems through voluntary compliance, rather than heavy-handed enforcement. The Commissioner investigates complaints, conducts audits, promotes awareness of and undertakes research about privacy matters.[25]

European Union[edit]

Main articles: General Data Protection Regulation and Data Protection Directive

The right to privacy is a highly developed area of law in Europe. All the member states of the European Union (EU) are also signatories of the European Convention on Human Rights (ECHR). Article 8 of the ECHR provides a right to respect for one's "private and family life, his home and his correspondence", subject to certain restrictions. The European Court of Human Rights has given this article a very broad interpretation in its jurisprudence.

In 1980, in an effort to create a comprehensive data protection system throughout Europe, the Organisation for Economic Co-operation and Development (OECD) issued its "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data".[26] The seven principles governing the OECD's recommendations for protection of personal data were:

1. Notice—data subjects should be given notice when their data is being collected;

2. Purpose—data should only be used for the purpose stated and not for any other purposes;
3. Consent—data should not be disclosed without the data subject's consent;
4. Security—collected data should be kept secure from any potential abuses;
5. Disclosure—data subjects should be informed as to who is collecting their data;
6. Access—data subjects should be allowed to access their data and make corrections to any inaccurate data; and
7. Accountability—data subjects should have a method available to them to hold data collectors accountable for not following the above principles.[27]

The OECD guidelines, however, were nonbinding, and data privacy laws still varied widely across Europe. The US, while endorsing the OECD's recommendations, did nothing to implement them within the United States.[27] However, all seven principles were incorporated into the EU Directive.[27]

In 1995, the EU adopted the Data Protection Directive, which regulates the processing of personal data within the EU. There were significant differences between the EU data protection and equivalent U.S. data privacy laws. These standards must be met not only by businesses operating in the EU but also by any organization that transfers personal information collected concerning a citizen of the EU. In 2001 the United States Department of Commerce worked to ensure legal compliance for US organizations under an opt-in Safe Harbor Program.[28] The FTC has approved a number of US providers to certify compliance with the US-EU Safe Harbor. Since 2010 Safe Harbor is criticised especially by German publicly appointed privacy protectors because the FTC's will to assert the defined rules hadn't been implemented in a proper even after revealing disharmonies.[29]