U.S. Data Privacy Protection Laws: A Comprehensive Guide

Conor Murray ⋮ 6-7 minutes ⋮ 4/21/2023

Topline

Here are some of the most important data privacy laws in the United States and their purposes, explained.

> Social medias applications are displayed on the screen of an iPhone. (Photo Illustration by ... [+] Chesnot/Getty Images)
>
> Getty Images

Key Facts

The United States has various federal and state laws that cover different aspects of data privacy, like health data, financial information or data collected from children.

Data privacy in the United States is notably different than in the European Union, which has a comprehensive data privacy law—General Data Protection Regulation—though some states have passed their own comprehensive data privacy laws that have drawn comparisons to the EU system.

Since data collected by many companies is unregulated in most states, these companies can use, sell or share your data without notifying you.

Privacy Act Of 1974

The Privacy Act of 1974 governs how federal agencies can collect and use data about individuals in its system of records. The act prohibits agencies from disclosing personal information without written consent from the individual, subject to limited exceptions including to the Census Bureau for statistical purposes. Individuals reserve the right to request their records, request a change to their records if they are inaccurate or incomplete, and to be protected against unwarranted invasion of their privacy.

Health Insurance Portability And Accountability Act (hipaa)

President Bill Clinton signed HIPAA into law in 1996, creating standards for how healthcare providers can use a patient's personal health data. HIPAA regulations only apply to "covered entities," which encompasses providers (like doctors, nurses, psychologists and dentists), a health plan (including healthcare insurance companies and government plans like Medicare) and healthcare clearinghouses, which process medical information. Under HIPAA guidelines, covered entities must comply with an individual's right to see their health information, correct their health information and covered entities cannot use or share health information without the individual's written consent. HIPAA is sometimes erroneously thought to be a more sweeping health privacy law that covers all of an individual's health data, *Vox* reported, but health information not shared with a covered entity is not subject to HIPAA regulation, meaning health data you share with a nutrition app or on social media would not be covered. Other institutions not considered covered entities that handle health information, like schools and employers, are not subject to HIPAA regulation but may be regulated by other laws.

The Gramm-Leach-Bliley Act

The GLBA, signed into law by Clinton in 1998, covers data privacy for financial institutions. The law requires these institutions, including "companies that offer consumers financial products or services like loans, financial or investment advice, or insurance," according to the Federal Trade Commission, to safeguard sensitive data and explain how it uses customer data. The law requires these institutions to have a policy in place to protect consumer data from security threats, and institutions must provide consumers with a privacy notice explaining what information is collected about the consumer and where it is shared, and it must inform the consumer of their right to opt out of the information being shared with unaffiliated parties.

Children's Online Privacy Protection Act

Signed into law in 1998, COPPA places limits on what companies can do with data collected about children under 13 years of age. Companies and websites that may collect data from children under 13 must post an online private policy that details their data practices and must obtain parental or guardian consent before collecting personal information from children. Parents must have the opportunity to access their child's data, review or delete it and prevent the company from collecting further data about their child. Companies must also maintain the confidentiality of data collected from children and must only keep it as long as necessary to fulfill the purpose for which it was collected. Because of COPPA's limits on data collection for children, some companies—notably, social media sites like Facebook and Twitter—require their users to verify they are 13 years of age or older when signing up.

California Consumer Privacy Act

Passed in 2018 and known as the strictest data privacy law in the country, the CCPA applies to a business that collects personal information about consumers and outlines specific rights consumers have. The CCPA allows consumers the right to know what personal information a business collects and to whom it is sold, the right to delete personal information collected by the business, the right to opt-out of the sale of personal information and the right to nondiscriminatory treatment for exercising privacy rights. The CCPA was updated with a second act—the California Privacy Rights Act—which was passed in 2020 and took effect in 2023. This extended the rights of consumers to include the right to correct inaccurate data a business collected about them and the right to limit the use and disclosure of sensitive data.

Other State Data Privacy Laws

Virginia became the second state after California to implement its own comprehensive state-level data privacy law this year, and similar laws in Colorado, Connecticut and Utah will go into effect later this year.

Further Reading

The State of Consumer Data Privacy Laws in the US (And Why It Matters) (New York Times)

CCPA vs CPRA: What's the Difference? (Bloomberg Law)

States' long-awaited data privacy laws are going into effect (Axios)