The State of Data Privacy

Center Forward Basics

June 2024

Overview

Data privacy, sometimes known as information privacy, pertains to the proper handling of sensitive data, including personal data, along with other confidential information such as financial and intellectual property data. It ensures compliance with regulations and safeguards the confidentiality and integrity of the data. Data privacy involves individuals' ability to control the sharing of personal information, such as name, location, contact details, one's online behavior, and much more. Just as someone might want to keep conversation private, online users often seek to manage or prevent certain types of data collection. Practically speaking, data privacy generally involves controlling data sharing with third parties, determining storage methods, and adhering to relevant regulations.

As Internet usage has grown, so has the significance of data privacy. Websites, apps, and social media platforms frequently gather and store user data to deliver services. However, some platforms may exceed user expectations in data collection, potentially compromising their users' privacy. Additionally. insufficient safeguards around collected data can lead to data breaches, further compromising user privacy. Protecting sensitive and personal data is a fundamental aspect of data privacy and security, aiming to maintain the availability and integrity of critical business data. Security plays a vital role in safeguarding data from external and internal threats and in determining data-sharing practices. In this Basic, the aim is to look at what data privacy is and what role state and federal governments play.

Center Forward Basics

Center Forward brings together members of Congress, not-for profits, academic experts, trade associations, corporations and unions to find common ground. Our mission: to give centrist allies the information they need to craft common sense solutions, and provide those allies the support they need to turn those ideas into results.

In order to meet our challenges we need to put aside the partisan bickering that has gridlocked Washington and come together to find common sense solutions.

For more information, please visit www.center-forward.org

Key Concepts of Data Privacy

Data privacy is a critical concern in today's digital age, and it encompasses several vital aspects. It pertains to safeguarding sensitive information collected by individuals, organizations, or governments, ensuring it is handled securely and used appropriately. It involves the practices, regulations, and technologies employed to protect personal information from unauthorized access, misuse, or exploitation. Well-crafted privacy regulations can help businesses adapt and respond to consumer trends and demands while ensuring consumers are confident that their data is being protected. Having data privacy and security laws that create clear protections for Americans, while allowing businesses to serve their customers in the ways they have come to rely upon, is the balance that businesses, governments, and consumers hope to strike.

Here are some key concepts of data privacy:

- **Personal Information**: Data privacy primarily concerns personal information, encompassing any data that can identify an individual. This ranges from primary identifiers like name, address, and phone number to more sensitive data like financial information, health records, and biometric data.
- **Consent**: The belief that individuals have the right to control how their personal data is collected, used, and shared. Obtaining explicit consent from individuals before collecting their data is fundamental to data privacy regulations. It is

important for consumers to be aware of and understand what they consent to, specifically when it comes to personal data.

- **Data Collection**: Organizations should be transparent about the purpose of collecting data and limit data collection to what is necessary for those purposes. They should also ensure data-processing activities comply with relevant privacy laws and regulations.
- **Processor & Controller Distinction:** Throughout the world, data protection laws and regulations recognize the need to distinguish between companies that decide how and why to collect and process personal data (controllers of that data), and companies that provide services and process data on behalf of controllers (processors).
- **Data Minimization**: Collecting only the minimum amount of personal data necessary for a specific purpose could reduce the risk of data breaches and protect individuals' privacy. Data collection practices should be regularly reviewed, and no longer needed data should be disposed of properly.
- **Data Subject Rights**: Privacy regulations grant individuals certain rights over their personal data, such as the right to access, rectify, or delete their data. Many organizations have mechanisms to facilitate these rights and promptly respond to data subject requests.
- **Regulatory Compliance**: Data privacy regulations vary across jurisdictions. Organizations that handle personal data must comply with the relevant regulations applicable to their operations.
- **Cross-Border Data Transfers**: When transferring personal data across borders, organizations should ensure adequate safeguards are in place to protect the privacy and security of the data, particularly when transferring data from regions with strict privacy regulations to areas with less stringent regulations and laws.
- **Security Measures**: Proper security measures are crucial to protecting data from unauthorized access, data breaches, and cyberattacks. These include encryption, access controls, regular security audits, and employee training on data handling best practices.

State Laws

While some U.S. data protection laws are enacted at the federal level, several states have ratified and enacted data privacy laws. These laws provide consumers with a combination of fundamental and comprehensive protections that grant rights to individuals pertaining to the collection, use and disclosure of data.

Examples of some of these state-level data privacy laws include:

- California Consumer Privacy Act (CCPA)
- California Privacy Rights Act (CPRA)
- Colorado Privacy Act (CPA)
- Connecticut Personal Data Privacy and Online Monitoring Act (CPDPA)
- New York SHIELD Act (SHIELD)
- Utah Consumer Privacy Act (UCPA)
- Virginia's Consumer Data Protection Act (VCDPA)

California was the first state in the nation to pass a comprehensive data privacy law. This law allows consumers to directly sue tech and online companies over data breaches that involve personal information such as names, social security numbers, and email addresses. The current data privacy laws in Colorado, Connecticut, Delaware, Indiana, Iowa, Florida, Montana, New Hampshire, New Jersey, Oregon, Texas, Tennessee, Utah, and Virginia do not allow individuals to sue tech companies for data breaches. In the absence of nationwide federal policy, these fifteen states have enacted their own laws. In the coming years, more states will likely implement privacy laws to protect consumers from cyber risks and stay competitive with international data regulation.

Federal Involvement

Earlier this year, federal lawmakers unveiled a first draft of the American Privacy Rights Act (APRA), an attempt to legislate national data privacy protections. Along with establishing a framework of data privacy rights for Americans, this bill also promises to eliminate the patchwork of state data privacy laws that have been passed in the absence of a federal mandate. Complying with this patchwork of state regulations poses a challenge for many large and small companies. The American Privacy Rights Act of 2024 is the successor to the American Data Privacy and Protection Act, or ADPPA, which was introduced in 2021.

While some data privacy experts have called for a federal law to regulate the practices of online data brokers, some say eliminating the patchwork of state privacy laws might do more harm than good. If the "choice of law" amendment is added to APRA and passed, it would allow states to maintain their privacy laws and prevent federal law from preempting state authority. Businesses would then be allowed to choose which state's privacy law they will adhere to. This patchwork approach to privacy legislation could pose compliance and liability risks for businesses and companies with multi-state operations.

Other federal laws that have been implemented are:

- **Children's Online Privacy Protection Act** (COPPA) - aims to protect the privacy of children under the age of 13 by requiring parental consent for the collection or use of any personal information of users.
- **Electronic Communications Privacy Act** (ECPA) - aims to protect wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers. The Act applies to email, telephone conversations, and data stored electronically.
- **Fair Credit Reporting Act** (FCRA) - aims to promote the accuracy, fairness, and privacy of consumer information contained in the files of consumer reporting agencies.
- **Gramm-Leach-Bliley Act** (GLBA) - requires financial institutions to explain how they share and protect their customers' private information.
- **Health Insurance Portability and Accountability Act** (HIPAA) - requires national standards to protect sensitive patient health information from disclosure.
- **Video Privacy Protection Act** (VPPA) - aims to protect the collection, use, and disclosure of personal video rental information.

Members of Congress from both parties have pledged to pursue federal data privacy legislation in the current session. They are under pressure to act because of the rapid onset of artificial intelligence systems that use large volumes of data, threatening privacy protections for Americans. As the November election nears, Congress stands on the brink of finalizing a law that has been the subject of intense debate for years.

Links to Other Resources

- Bloomberg Law - Which States Have Consumer Data Privacy Laws?
- CloudFare - What is data privacy?
- Congressional Research Service - Data Protection and Privacy Law: An Introduction
- Legal 500, GC Magazine - The State of Privacy: Does the US need a federal privacy law?
- Main Street Privacy Coalition - Legislative Solutions to Protect Kids Online & Ensure Americans' Data Privacy Rights
- SNIA - What is Data Privacy?
- RollCall - Push for federal data privacy law grows as rights vary by state

- State Scoop - The American Privacy Rights Act could undercut state privacy efforts
- TechTarget - What is Data Privacy?