ASPEN TECH POLICY HUB

aspen institute

Policy 101: Data Privacy

What is data privacy?

Data privacy refers to a person's right to control the collection, storage, and sharing of digital information related to them. As data becomes increasingly easy to capture and lucrative to leverage, policymakers are grappling with the extent to which the right to data privacy should be codified into law.

Why does it matter?

The widespread availability of digital information has prompted myriad questions about what uses of data should be allowed and who should get to decide. In recent years, companies have found tremendous value in leveraging, exchanging, and selling user data. Depending on the perspective of the beholder, the net result may be one of the most successful pro-consumer developments in history, or a terrifying trap of "surveillance capitalism."

User data allows companies to individualize their services more than ever before, and has enabled a new category of services that are powered by aggregate data sets from millions of users. Companies have powerful incentives in this context to sell data to each other. While a user might be comfortable with providing their information to a particular site for a particular service, they may not be comfortable with that same information being passed onto another service without their approval, or even used by the same company for a different purpose. Restrictions on these types of data exchanges have been central to data privacy debates.

Many privacy frameworks propose requirements based on whether personally identifiable information (PII) is involved. But the scope of PII – sensitive data that can reveal an individual's identity – is constantly changing. Anonymized information has been shown to be deanonymizable. Data that is non-identifiable on its own can be pieced together with other sources to deduce someone's identity anyway. Any effort to regulate the disclosure of PII is working with a moving target. These tensions are particularly stark, to give one example, in the ongoing debates over facial recognition technology.

Where does data privacy regulation stand in the US?

In the US, there is currently no comprehensive federal rule on data privacy and data collection. However, there are federal laws that cover data privacy for specific types of information (see box). The Federal Trade Commission holds general authority to prevent consumer fraud, and has wielded this power in the past to penalize companies (notably Facebook) for privacy violations.

At the state level, the California Consumer Protection Act (CCPA) became the first comprehensive commercial privacy act in the United States in 2018. The CCPA states that consumers should have transparency into collection of their data, greater access to and the right to delete the collected data, and the ability to opt out of the sale of their personal data.

Colorado and Virginia are the only other states with fully-enacted data privacy laws. Though these laws share many of the transparency and choice themes of the CCPA, they vary in significant ways, including the businesses to which they apply, the amount of time businesses have to "cure" mistakes, and how users are able to delete data and opt out of collection. Several other states – most notably Massachusetts, New York, Pennsylvania, and North Carolina – also have comprehensive privacy bills under consideration.

How does the United States compare to other countries?

Given the relative newness of data privacy, most other jurisdictions do not have comprehensive data privacy laws. The exception is the European Union's General Data Protection Regulation of 2018 (GDPR), which sets as a default that data cannot be collected or used without legal justification, limits the effectiveness of consent to specific contexts of data usage, grants citizens the right to access data collected about them, imposes steep penalties on companies that fail to comply, and much more. The GDPR has inspired other countries, including India and Kenya, to adopt similar privacy efforts.

WHAT PERSONAL DATA IS PROTECTED AT THE FEDERAL LEVEL?

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) protects health data from being shared without patient consent.

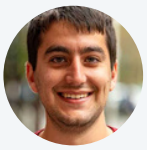
The Family Education and Rights and Privacy Act of 1974 (FERPA) gives students the right to scrutinize their school records and control the sharing of that information.

The Gramm-Leach-Bliley Act of 1999 requires financial institutions to inform consumers how their personal financial information is used.

The Fair Credit Reporting Act of 1970 protects information in consumer credit reports, restricting how these reports can be assembled and who can view them.

OUR EXPERTS


Barbara Cohn


Aloni Cohen


Ginny Fahs


Steve Weis


Sharon Zezima

To contact the fellows for media inquiries, please visit: aspentechpolicyhub.org.

The Aspen Tech Policy Hub is a West Coast policy incubator, training a new generation of STEM policy entrepreneurs. Our Policy 101s offer quick and to-the-point overviews of the key tech policy issues of the day. For more information, visit www.aspentechpolicyhub.org.

The Aspen Institute
2300 N St. NW, Suite 700
Washington, DC 20037
202 736 5800