

The Consumer Privacy Protection Act of 2015

Data breaches continue to plague corporations and compromise the privacy of millions of Americans by exposing their sensitive personal and financial information. At the same time data breaches are increasing in number and scope, so too is the amount of information we share with companies who are the target of these breaches. Companies collect and store our social security numbers, our bank account information, and our email addresses. They collect information about our private health and medical conditions. They know what routes we take to and from work. They can replicate our fingerprints, and they store our family photographs in the cloud.

The Consumer Privacy Protection Act of 2015 strengthens protections for American consumers by requiring that companies who collect and store such information take reasonable measures to ensure it remains private and secure. The bill also requires that companies notify affected individuals if their sensitive personal or financial information has been breached. Specifically the bill:

- Requires companies who store sensitive personal or financial information on 10,000 customers or more meet consumer privacy and data security standards to keep this information safe, and notify the customer within 30 days in event of a breach.
- Establishes a broad definition of information that must be protected, including (1) social security numbers and other government-issued identification numbers; (2) financial account information, including credit card numbers and bank accounts; (3) online usernames and passwords, including email addresses and passwords; (4) unique biometric data, including fingerprints; (5) information about a person's physical and mental health; (6) information about a person's geolocation; and (7) access to private digital photographs and videos.
- Creates civil penalties for companies that fail to meet the required consumer privacy and data security standards or fail to notify customers of a breach of covered data. The Department of Justice, the Federal Trade Commission, and the State Attorneys General each have a role in enforcement.
- Requires companies to inform federal law enforcement, such as the Secret Service and the FBI, of all large data breaches, as well those involving federal government databases, or databases that contain information about federal employees involved in law enforcement or national security.
- Guarantees a federal baseline of strong consumer privacy protections for all Americans by preempting weaker state laws, while leaving stronger state laws in place.

This bill is supported by a wide range of consumer and privacy advocacy organizations, including: Center for Democracy & Technology, Consumers Union, Consumer Federation of America, National Consumers League, New America's Open Technology Institute, and Privacy Rights Clearinghouse.