A new US data privacy bill aims to give you more control over information collected about you

August 24 2022, by Anne Toomey McKenna

Credit: CC0 Public Domain

Data privacy in the U.S. is, in many ways, a legal void. While there are limited protections for health and financial data, the cradle of the world's largest tech companies, like Apple, Amazon, Google, and Meta

(Facebook), lacks any comprehensive federal data privacy law. This leaves U.S. citizens with minimal data privacy protections compared with citizens of other nations. But that may be about to change.

With rare bipartisan support, the American Data and Privacy Protection Act moved out of the U.S. House of Representatives Committee on Energy and Commerce by a vote of 53–2 on July 20, 2022. The bill still needs to pass the full House and the Senate, and negotiations are ongoing . Given the Biden administration's responsible data practices strategy, White House support is likely if a version of the bill passes.

As a legal scholar and attorney who studies and practices technology and data privacy law, I've been closely following the act, known as ADPPA. If passed, it will fundamentally alter U.S. data privacy law.

ADPPA fills the data privacy void, builds in federal preemption over some state data privacy laws, allows individuals to file suit over violations and substantially changes data privacy law enforcement. Like all big changes, ADPPA is getting mixed reviews from media, scholars and businesses. But many see the bill as a triumph for U.S. data privacy that provides a needed national standard for data practices.

Who and what will ADPPA regulate?

ADPPA would apply to "covered" entities, meaning any entity collecting, processing or transferring covered data, including nonprofits and sole proprietors. It also regulates cellphone and internet providers and other common carriers, with potentially concerning changes to federal communications regulation. It does not apply to government entities.

ADPPA defines "covered" data as any information or device that identifies or can be reasonably linked to a person. It also protects

biometric data, genetic data and geolocation information.

The bill excludes three big data categories: deidentified data, employee data and publicly available information. That last category includes social media accounts with privacy settings open to public viewing. While research has repeatedly shown deidentified data can be easily reidentified, the ADPPA attempts to address that by requiring covered entities to take "reasonable technical, administrative, and physical measures to ensure that the information cannot, at any point, be used to re-identify any individual or device."

How ADPPA protects your data

The act would require data collection to be as minimal as possible. The bill allows covered entities to collect, use or share an individual's data only when reasonably necessary and proportionate to a product or service the person requests or to respond to a communication the person initiates. It allows collection for authentication, security incidents, prevention of illegal activities or serious harm to persons, and compliance with legal obligations.

People would gain rights to access and have some control over their data. ADPPA gives users the right to correct inaccuracies and potentially delete their data held by covered entities.

The bill permits data collection as part of research for public good. It allows data collection for peer-reviewed research or research done in the public interest—for example, testing whether a website is unlawfully discriminating. This is important for researchers who might otherwise run afoul of site terms or hacking laws.

The ADPPA also has a provision that tackles the service-conditioned-on-consent problem—those annoying "I Agree" boxes that force people to

accept a jumble of legal terms. When you click one of those boxes, you contractually waive your privacy rights as a condition to simply use a service, visit a website or buy a product. The bill will prevent covered entities from using contract law to get around the bill's protections.

Looking to federal electronic surveillance law for guidance

The U.S.'s Electronic Communications Privacy Act can provide federal law makers guidance in finalizing ADPPA. Like the ADPPA, the 1986 ECPA legislation involved a massive overhaul of U.S. electronic privacy law to address adverse effects to individual privacy and civil liberties posed by advancing surveillance and communication technologies. Once again, advances in surveillance and data technologies, such as artificial intelligence, are significantly affecting citizens' rights.

ECPA, still in effect today, provides a baseline national standard for electronic surveillance protections. ECPA protects communications from interception unless one party to the communication consents. But ECPA does not preempt states from passing more protective laws, so states can choose to provide greater privacy rights. The end result: Roughly a quarter of U.S. states require consent of all parties to intercept a communication, thus providing their citizens increased privacy rights.

ECPA's federal/state balance has worked for decades now, and ECPA has not overwhelmed the courts or destroyed commerce.

National preemption

As drafted, ADPPA preempts some state data privacy legislation. This affects California's Consumer Privacy Act, although it does not preempt the Illinois Biometric Information Privacy Act or state laws specifically regulating facial recognition technology. The preemption provisions, however, are in flux as members of the House continue to negotiate the

bill.

ADPPA's national standards provide uniform compliance requirements, serving economic efficiency; but its preemption of most state laws has some scholars concerned, and California opposes its passage.

If preemption stands, any final version of the ADPPA will be the law of the land, limiting states from more firmly protecting their citizens' data privacy.

Private right of action and enforcement

ADDPA provides for a private right of action, allowing people to sue covered entities who violate their rights under ADPPA. That gives the bill's enforcement mechanisms a big boost, although it has significant restrictions.

The U.S. Chamber of Commerce and the tech industry oppose a private right of action, preferring ADPPA enforcement be restricted to the Federal Trade Commission. But the FTC has far less staff and far fewer resources than U.S. trial attorneys do.

ECPA, for comparison, has a private right of action. It has not overwhelmed courts or businesses, and entities likely comply with ECPA to avoid civil litigation. Plus, courts have honed ECPA's terms, providing clear precedent and understandable compliance guidelines.

How big are the changes?

The changes to U.S. data privacy law are big, but ADPPA affords much-needed security and data protections to U.S. citizens, and I believe that it is workable with tweaks.

Given how the internet works, data routinely flows across international borders, so many U.S. companies have already built compliance with other nations' laws into their systems. This includes the E.U.'s General Data Protection Regulation—a law similar to the ADPPA. Facebook, for example, provides E.U. citizens with GDPR's protections, but it does not give U.S. citizens those protections, because it is not required to do so.

Congress has done little with data privacy, but ADPPA is poised to change that.

Provided by The Conversation