COMPREHENSIVE FEDERAL PRIVACY LEGISLATION

Data Security Requirements

CENTER FOR DEMOCRACY & TECHNOLOGY

Data security is one of the foundational Fair Information Practices which undergird privacy laws across the country, including existing federal health and financial privacy rules. Federal legislation must require entities that collect and use personal information to adopt reasonable policies, practices, and procedures to protect personal data. What is "reasonable" should be tailored to the activities of the company, the type and amount of data at issue, and the costs of implementing state of the art safeguards.

Companies continue to mishandle information and fail at basic security processes

In 2017, Equifax demonstrated how even multi-billion dollar companies whose entire business is the collection and protection of sensitive personal information can give basic data security short-shrift and then have no plan when things go wrong. While 2018 saw fewer breaches than 2017, major data security lapses compromised passport numbers, and a data broker no one had ever heard of leaked people's contact information—along with whether they believed you were a smoker or drinker, and even the interests and habits of children—onto the public internet.

Companies are challenging the FTC's authority to police data security lapses

Following serious data breaches and security lapses, Wyndham hotels challenged the FTC's data security authority under current law. Medical testing firm LabMD and router company D-Link have also argued the FTC's data security requirements are not clear. Writing more explicit data security baselines into statute and regulation will provide companies like these with the notice of appropriate behavior they assert they do not have.

Reasonable data security protections can address many longstanding security problems

Most data security investigations involve "basic, fundamental security missteps," according to the FTC. The California Attorney General's Office concurs, noting that most publicly reported data breaches could be prevented by companies employing reasonable security measures. Such measures can build on existing security regulations, like those in Massachusetts and New York, and include widely accepted best practices like updating software, implementing access controls, and maintaining written information security plans, and having data retention and deletion policies like those that already exist in 35 states.

Rulemaking authority can permit the FTC to appropriately tailor data security requirements

A bipartisan collection of FTC commissioners and staff have long called for Congress to pass comprehensive data security legislation, specifically asking for APA-rulemaking authority for data security generally. CDT agrees. Data security standards evolve rapidly and regulators must be empowered to establish requirements that can change over time and adapt to new security threats. Any data security requirements enacted into federal law should provide general instructions to the FTC and other data security regulators as to what reasonable data security to strive towards.

For more info on CDT's efforts to create comprehensive federal privacy legislation, visit http://bit.ly/CDTfedpriv or contact Michelle Richardson at mrichardson@cdt.org.