

**Oral Statement of
Commissioner Rohit Chopra**

As Prepared for Delivery

**Before the US House of Representatives
Committee on Energy and Commerce
Subcommittee on Digital Commerce and Consumer Protection**

**Hearing on
Oversight of the Federal Trade Commission**

July 18, 2018

Chairman Latta, Ranking Member Schakowsky, and members of the Subcommittee, thank you for the opportunity to testify today about data security and privacy.

According to survey data, 91% of adults believe they have lost control over how companies are collecting and using their personal information. News reports of data breaches and disclosure of sensitive data have become routine. On the dark web, stolen credit card and Social Security numbers and social media profiles can be bought and sold.

For many Americans, the situation seems hopeless, and they feel powerless. I'm concerned that Washington is sitting on the sidelines.

We must confront the risks to our economy, society, and national security of inadequate data security and privacy. The cost of inaction is growing.

According to an industry study, over 15 million Americans were the victim of identity theft in 2016, leading to \$16 billion of losses. The majority of these Americans had their records accessed in a data breach in the years prior to their identity theft.

When we talk about data security, we typically focus on protecting power grids, payment networks, and other critical infrastructure to avoid a crippling attack. But we also know that the infiltration of commercial holdings of consumer data can also cause chaos. Large-scale breaches of unencrypted data are increasing these risks. We must do more to secure personal data from falling into the wrong hands.

Chairman Simons is right. The FTC cracks down on illegal practices when we can. But our existing toolkit will not do the trick. In too many situations, our resolution is to tell a law-breaking company to stop breaking the law.

To truly make a difference when it comes to data protection, we need the ability to deter misconduct through financial penalties and sensible safeguards that can evolve with the marketplace.

When it comes to privacy, the United States should lead. New privacy protections from Europe and California are advancing. But we shouldn't feel we have to simply copy and paste. That's not leadership.

Privacy and competition can go hand in hand, especially when consumers can access their data in portable and interoperable formats. We can increase privacy protections without crowning corporate royalty.

We don't need to start from scratch. Congress can build upon existing privacy laws, such as the Children's Online Privacy Protection Act. Twenty years ago, industry incumbents warned that the bipartisan effort to protect children online would end in utter disaster for our information economy, and boy were they wrong.

COPPA has common sense ideas. Data collected for one purpose shouldn't be used for another purpose without your permission. You should have the ability to review the information collected about you. Companies should be upfront and honest about who they are sharing your data with. And strong protections should be backed by an enforcement regime that can hold companies and their operators accountable.

Over the past decade, the FTC has produced scores of studies and reports. But now it is time for Congress to act.

I'm confident that if Congress entrusts the FTC with the authority and resources to do more to protect families and businesses, we will deploy them efficiently and effectively, while continuing to promote a dynamic digital economy that truly benefits all of us.