Committee on Energy and Commerce

Opening Statement as Prepared for Delivery
of
Ranking Member Frank Pallone, Jr.

Innovation, Data, and Commerce Subcommittee Hearing on "Addressing America's Data Privacy Shortfalls: How a National Standard Fills Gaps to Protect Americans' Personal Information."

April 27, 2023

For decades, we've sought to safeguard Americans' fundamental right to privacy with a series of fragmented, sector-by-sector laws. Anyone with a smartphone, laptop, or tablet can tell you that we're not getting the job done.

The alphabet soup of well-intentioned federal privacy laws – HIPAA, COPPA, FERPA, GLBA – have failed to rein-in the collection, use, and transfer of Americans' sensitive data. That's partly because they were not designed for our modern online economy. FERPA, or the Federal Educational Rights and Privacy Act, passed in 1974. HIPAA, or the Health Insurance Portability Accountability Act, passed in 1996. GLBA, or the Gramm-Leach-Bliley Act, which addresses privacy within the financial sector, passed in 1999. And COPPA, or the Childrens Online Privacy Protection Act, became law in 2000. The iPhone wasn't released until 2007. In internet years, these laws are dinosaurs.

Today, health information is no longer confined to the relative safety of a doctor's filing cabinet. Fitness trackers monitor our heart rates, sleep patterns, and oxygen saturation levels. Health information websites provide diagnosis and treatment information on every possible medical condition. Mobile applications track dietary, mental, and reproductive health.

But the HIPAA privacy rules only restrict the use and sharing of health information by health care providers, clearinghouses, and health plans. As a result, some of the most commonly used websites, apps, and devices have the green light to mine and use Americans' health information without meaningful limitations.

The lack of strong privacy protections threatens Americans' financial information as well. Existing financial privacy laws largely do not apply to retailers and online marketplaces. Nor do they provide protection from discriminatory algorithms.

Likewise, existing children's privacy laws leave vast amounts of children and teens' sensitive information unprotected.

FERPA, the privacy law protecting educational records, does not apply to private and parochial elementary and secondary schools. It also does not apply to EdTech downloaded and used at home or in after school programs to supplement or complement children's schoolwork.

COPPA only restricts "online operators" from collecting data from children under the age of 13 without obtaining verifiable parental consent, but only under limited circumstances. Children's data collected on sites like TikTok, Instagram, Google, Facebook, and Snapchat is not protected unless the site knows it is collecting information from kids under 13.

This honor system has become a get out of jail free card for Big Tech companies, which often claim that their services are intended for users 13 or older. But we know children are on these sites and apps. Sixty-four percent of children between eight- and twelve-years-old report watching online videos on platforms like TikTok and YouTube every day. Nearly one in five say they use social media every day.

Simply tweaking current child privacy laws will not sufficiently protect our nation's youth. That's because age verification is notoriously challenging and has proven to be ineffective. After all, children today are digital natives. They know how to bypass popups asking for their age or birthdate and can enter these virtual playgrounds with little parental supervision and meager privacy protections.

We also know that parents' use of the internet routinely provides information about their children, either directly or by inference. When a parent or guardian goes online to research and sign up for summer camps, family vacations, little league teams, gymnastics classes, or a broad variety of other activities, they share data about their children. That information is then used and shared for targeted marketing and other purposes. As a result, protecting kids and teens' privacy requires us to protect everyone's privacy.

That's why we must pass a comprehensive privacy bill that closes the gaps and enshrines Americans' right to privacy in law. We need a bill that reins-in the overcollection of information by mandating data minimization. We need a bill that puts all Americans back in control of how their data is collected, used, and shared.

Last Congress, this Committee overwhelmingly passed such a bill with broad bipartisan support. I'm committed to getting a bill over the finish line and look forward to continuing to work with Chair Rodgers on that effort.