U.S. Senator John Hickenlooper

Senate Committee on Commerce, Science, and Transportation Committee
Subcommittee on Consumer Protection, Product Safety, and Data Security

Subcommittee Hearing: Strengthening Data Security to Protect Consumers

May 8, 2024

Opening Statement

We're at a pivotal moment in the age of technologies that rely on increasing amounts of consumers' data. Obviously, Artificial Intelligence has gotten the lion's share of publicity but that's nowhere near the limit!

Businesses collect or process data ranging from personally identifiable information: name, address, likeness – as they say in college these days. Obviously, sensitive Data like Physical locations and browsing history.

The threats to consumers' data that companies face is complex and, in almost every way, daunting.

As companies collect more data, they become more attractive targets for data breaches. And, by that I mean criminal activity. Each breach costs companies nearly $4.2 million per incident. And consumers shoulder the financial burden and reputational harm of each incident.

How many more consumers need to be victims of identity theft for us to take action? How much longer should we allow personal data to be sold on the dark web for profit?

When will cyber criminals be stopped – or at least deterred – from preying on our data?

These data breaches hurt small businesses, large corporations, and everything in between.

In 2023 alone, there were 3,205 data breaches in the U.S. – and that's what we know of or were reported. 353,000 individuals were severely impacted. 10 percent of publicly traded companies reported a data breach impacting, in total, 143 million individuals.

These data breaches can have devastating effects. A nationwide wireless carrier's data breach exposed the data of 70 million customers. A large health insurer, this was recently widely reported, saw their system grind to a halt, which delayed important healthcare payments and exposed critical health data.

This is why we need strong requirements for how companies collect and protect our data, are conducting routine risk assessments, and establishing strong internal & external safeguards for data.

We need a strong national privacy standard that includes 'data minimization' and 'data security'.

Obviously, 'data minimization' establishes specific categories to 'turn off the spigot' as it were. 'Turn off the spigot' of data that companies collect from consumers so that companies aren't just collecting everything they can.

"Data security' establishes clear requirements for how companies should safeguard the data that they do collect – so breaches are less common.

We need to give consumers meaningful control over how their data is used. This will restore consumers' confidence in the technology that powers our economy.

And, I think states clearly are not waiting for the federal government to act.

Already 16 states, including Colorado, have passed – or are in the process of passing – their own state privacy laws. Other states are talking about it.

There are lessons we can learn from these state laws. For example, Colorado's law has a temporary 'right to cure' for businesses to comply or adapt to privacy requirements.

There are also areas where the federal government has to step in to issue rules and apply enforcement, consistent definitions for key terms like 'sensitive data', or to issue nationwide rules.

The draft American Privacy Rights Act is an important, bipartisan, compromise framework for Congress to build upon. I commend Chair Cantwell and Chair McMorris Rodgers in the House for their efforts to bring this proposal forward.

We're committed here to listening to all perspectives on data minimization and data security. Minimization and security are obviously interconnected, interrelated.

Together, they represent the foundation of a strong data privacy framework on which we can build.

We have an opportunity right now – and an obligation right now – to build meaningful, bipartisan consensus around these complex issues.