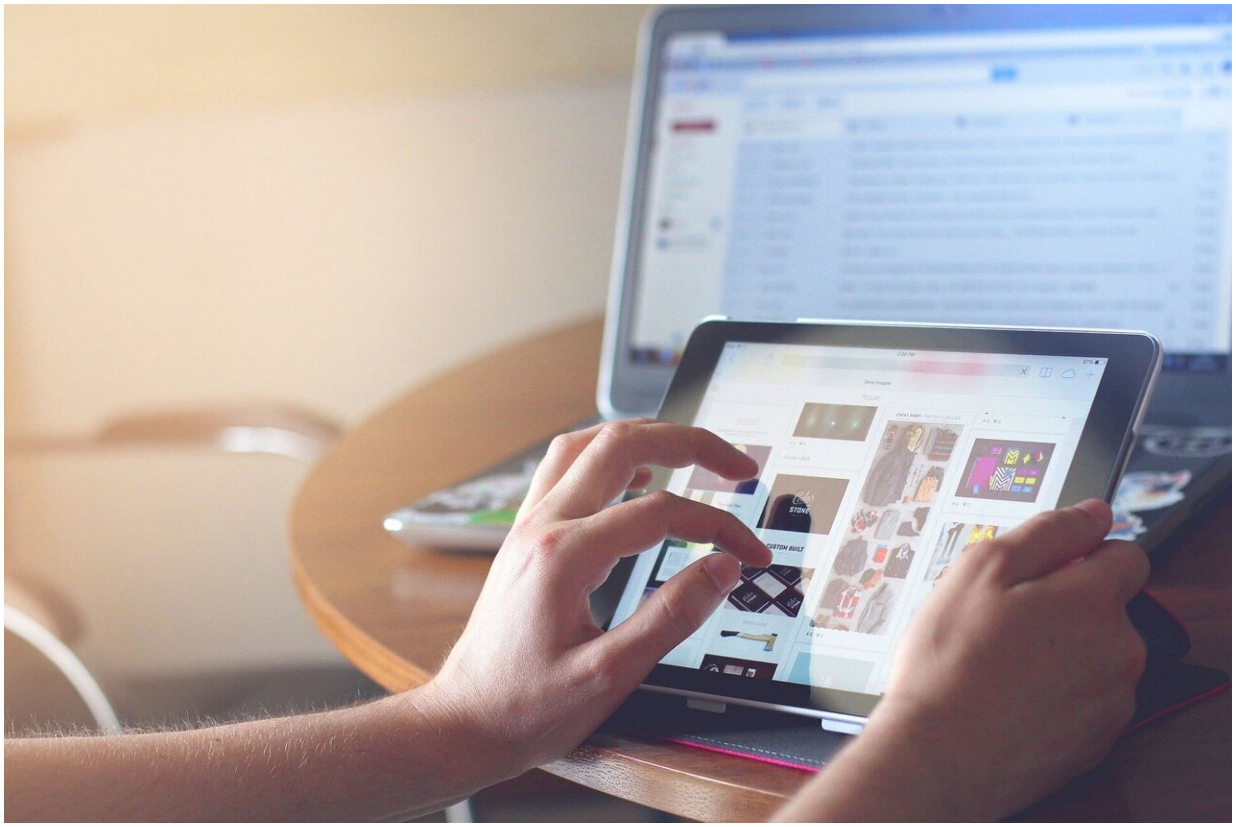
TechXplore

Cyberspace is critical infrastructure, and it will take effective government oversight to make it safe

August 10 2020, by Francine Berman



Credit: CC0 Public Domain

A famous 1990s New Yorker cartoon showed two dogs at a computer and a caption that read "On the Internet, nobody knows you're a dog."

The cartoon represents a digital past when people required few safeguards on the internet. People could explore a world of information without having every click tracked or their personal data treated as a commodity.

The New Yorker cartoon doesn't apply today. Not only do your browser, service provider and apps know you're a dog, they know what breed you are, what kind of dog food you eat, who your owner is and where your doghouse is. Companies are parlaying that information into profit.

Legal and regulatory protections in cyberspace have not kept up with the times. They are better suited to the internet of the past than the present. Today's dependence on the internet has thrust society into a new era, making effective public protections critical for a healthy cyberspace.

The COVID-19 pandemic has made cyberspace critical infrastructure. When schools, stores, restaurants and community gathering places closed, the U.S. went online and digital technologies became the primary platform for education, grocery delivery, services and many workplaces.

In the last four months, I've attended a Zoom funeral, a Zoom wedding and taken ballet classes online. This fall I'll teach online. Many of the shifts from on-site to online are here to stay, and I predict the "new normal" will put much more emphasis on interacting in cyberspace.

This creates new urgency for public protections. As former head of a national Supercomputer Center and a data scientist, I've seen that digital exploitation of personal information is the pandemic in cyberspace. It puts individuals and society at risk.

The need for government action

Public leadership is needed to solve this public problem. But for the most part, the federal government has left the private sector to regulate itself. Today, data is a commodity, and relying on the fox to guard the henhouse has not brought the needed protections.

Evidence of digital exploitation is everywhere. Online dating services Grindr, Tinder and OKCupid share personal data on sexual orientation and location with advertisers. Commercial data brokers sell lists of "dementia sufferers" and "Hispanic payday loan responders" to predators and others. Cambridge Analytica used personal information to manipulate a presidential election. Before public outcry, Zoom handed over user information to Facebook. High school students, peaceful protesters and others have become targets of mass surveillance and facial recognition.

Experiences with data protection regulation in Europe and California demonstrate that getting protections right is complicated and politically fraught, and many people have little confidence in government protection or effectiveness. But with cyberspace serving as public infrastructure, I believe safeguards must come from the public sector.

Regulating protections

So what needs to be done? Political leaders can initiate digital reforms by enacting effective legislation and empowering independent oversight agencies. Federal efforts to safeguard Americans in other areas provide a blueprint: The Health Insurance Portability and Accountability Act protects private health information. The Occupational Safety and Health Administration mandates protective gear to keep workplaces safe. The Food and Drug Administration works to ensure that drugs are safe to ingest.

In these instances, government stepped in because industry could or would not, and companies in these sectors conform to government expectations for public protections or pay a price.

Cyberspace needs the same strategies. Multiple bills in the 116th Congress could provide a baseline for federal digital reforms.

The most comprehensive of the bunch, according to the Electronic Privacy Information Center, is Reps. Eshoo and Lofgren's Online Privacy Act. This bill would promote individuals' rights to access, control and delete personal data. Sen. Gillibrand's Data Protection Act would create an independent Data Protection Agency, needed to monitor and enforce public protections. Sen. Markey's Facial Recognition and Biometric Technology Moratorium Act would ban federal use of facial recognition technology.

Despite the urgency of enacting privacy protections in the wake of COVID-19, Congress has yet to hold hearings, invite experts or seek public comment on these bills.

First steps

Passing legislation now is important because building healthy digital infrastructure takes time. Legislation and policy are only the first step. When digital reforms are enacted, technology companies will need to design new protections into existing and next-generation digital products, services, protocols and algorithms. This could change the software architectures of everything from baby monitors to Fitbits to Facebook.

Digital protections will need to be monitored and effectively enforced by independent federal agencies. They will impact business models in Silicon Valley and the marketplace for information. They will constrain the way the private sector deploys surveillance technologies, accumulates huge personal digital profiles and exploits data.

With unconstrained digital exploitation, the privacy and safety of cyberspace will continue to erode and with it the social fabric. Digital reform is the basis for a healthy cyberspace where users control what personal data is collected and how it is used, where digital products and services meet standards for privacy, safety and security, and where individuals can opt out and still function without commercial penalty.

Cyberspace can function as critical infrastructure only when it's safe for everyone. Federal digital reforms are stuck in committee; redesigning cyberspace for protections later will limit effectiveness. Safeguards must be incorporated into today's and tomorrow's digital products now, including new surveillance technologies and AI. Congress must take the lead to effectively contain the digital exploitation pandemic and make cyberspace safe for the public.

Provided by The Conversation

Citation: Cyberspace is critical infrastructure, and it will take effective government oversight to make it safe (2020, August 10) retrieved 2 May 2024 from https://techxplore.com/news/2020-08-cyberspace-critical-infrastructure-effective-oversight.html