



How will scrapping of US internet privacy rules affect me?

29 March 2017



GETTY IMAGES

The Trump administration is poised to nullify Obama-era regulations designed to protect internet users' private data. What does this mean for users in the US?

On Tuesday, the US House of Representatives passed a bill that effectively tears up a 2016 internet privacy rule from the Federal Communications Commission (FCC) called, "Protecting the Privacy of Customers of Broadband and Other Telecommunication Services".

The rule said that internet service providers (ISPs) must obtain permission from their users before harvesting personal data and selling it to advertisers or other third-party entities. It also required ISPs to adopt security practices to help prevent large-scale data breaches, and to notify users, the FCC and the FBI in case of a major hack.

The bill to scrap all these regulations now heads for President Donald Trump's desk and his administration has already pledged to sign it.

Which parts of the Internet will this rule affect?

Thanks to this law, big-name internet service providers like AT&T, Verizon, Charter Communications and Comcast will not have to ask their users for permission to collect, share

or sell their data.

Other services like Google and Facebook already harvest this kind of information - a fact that ISP companies use to argue they were being unfairly singled out by the FCC.

"The phone and cable companies have always had Google envy," says Jeffrey Chester, executive director of the Center for Digital Democracy, a privacy rights advocacy group.

Chester says that while users can easily opt-out of using Facebook or switch to another search engine, many Americans have little if any choice about where they buy their internet access. In some places, there is only a single provider.

ISPs are also capable of collecting even more information than a web browser or social network.

"They know what you watch on cable television, they know what you stream," Chester says.



What kind of data will my ISP be able to collect and sell?

The original FCC rule sought to protect customer proprietary information including, "financial information, health information, Social Security numbers, precise geo-location information, information pertaining to children, content of communications, web browsing history, application usage history, and the functional equivalents of web browsing history or application usage history".

Now that data is conceivably up for grabs to ISPs.

However, Ryan Radia, regulatory counsel at the pro-business think tank Competitive Enterprise Institute, says he doesn't think that ISPs will be able to retain their customer base if they're selling off highly personal or de-anonymised information.

"No self-respecting ISP is ever going to do anything to let that happen intentionally," he says. "[It'll be] what domain names you visited, what broad interest category, maybe detailed URLs - certainly demographics."



GETTY IMAGES

How will my user experience change?

It likely won't change much at all for the average user in the US.

Had the FCC regulations gone into effect later this year as originally planned, logging on to the web via your phone, tablet, smart TV or laptop might have brought up a request from your ISP for permission to access and share your information.

"Consumers would have had to have some process where they click on something or check a box," says Neema Singh Guliani, legislative counsel with the American Civil Liberties Union.

"On the most basic level it's going to make it much more difficult to fully understand how their information is being shared and used."

At minimum, users may notice that the advertisements they are being shown on their devices gets more targeted - a pregnant woman may see more ads for baby products, or a house-hunting couple will start seeing ads from banks.

"I think most people won't really notice a difference," says Radia.



Why should I care?

Guliani worries that personal data could be used for discriminatory advertising practices, like showing ads for high-interest loans only to low-income consumers, or prices for products that vary based on the user's income information. Super targeted ads "don't always benefit the consumer," she says.

But business advocates and critics of federal oversight argue consumers ought to be free to make their own decisions.

"I reject the idea that we should protect people from buying things that they might actually want because their preferences were revealed by their browsing history," says Radia.

Chester says that there is a two-fold risk when it comes to data breaches. Not only are ISPs no longer required to notify consumers about major hacking incidents, they've also put a big target on their backs as repositories for new, proprietary information about Americans.

"This is a data breach in the waiting," Chester says. "They'll get to it."

The advocacy group Fight for the Future also put out a statement saying that bypassing consumer consent will "enable more unconstitutional mass government surveillance".



ANDREW BURTON

What can I do to protect my information?

Some experts recommend using a virtual private network (VPN) service, which can encrypt data leaving your computer or phone, and make it impossible for your ISP to collect.

It is also possible to contact your ISP to find out more about the kind of data they collect, and to ask if you can opt out.

Companies like Facebook have backed off of unpopular data collection practices after outcry for their users.

"There will be an ISP in the next few years that does something outrageous and hopefully someone will notice, and it'll be reported and stopped," Radia says.

"That's probably what will stop the bad practices more than any regulatory body."

But Guliani says that puts all the onus on the consumer, and most people rarely read the fine print on their contracts, much less take the time to grill their internet companies about how their data is being used.

"There is this growing concern that companies are going to make consenting to using your information a condition of using their service," she says.

"The system as it is today is just not working. People care about how their data is shared - they would like more control."

Share this story About sharing