Senate votes to repeal FCC internet privacy regulations

Bryan Dyne
27 March 2017

With virtually no public discussion, the US Senate voted Thursday to repeal a set of internet privacy regulations passed by the Federal Communications Commission (FCC) last October.

If passed by the House of Representatives and signed into law by President Donald Trump, the legislation will allow internet service providers such as AT&T, Comcast, Time Warner and Verizon to sell private communications information to the advertising industry and any other buyers, unimpeded by any sort of regulatory oversight.

The repeal was passed by the Senate using powers outlined in the Congressional Review Act (CRA), which gives Congress the authority to eliminate rules and guidelines passed by federal agencies before they go into effect. The use of the CRA will also prevent the FCC from passing "substantially similar" regulations in the future, essentially giving these companies free reign in regards to the data they collect from their users.

While the CRA had only been used once before 2017, early in the George W. Bush era, it has been used multiple times by the new Congress and the Trump administration to attack other federal regulations.

The FCC ruling, set to go into effect at the end of this year, requires companies that provide internet access to receive explicit consent from their customers in order to use and share any personal information they collect, including things like financial information, browsing history and location. It would also allow customers to revoke their permission for companies to use what was deemed "non-personal" information, such as the level or types of service a given individual receives.

In theory, the ruling was designed to uphold the idea of net neutrality, that no company should have the capability to dictate what users do on the internet or to use information collected by virtue of supplying internet access for profits. However, the exceptions clause put in by the FCC was vague enough to make the measure largely toothless. In addition, without intimate access to each company's own infrastructure, the FCC has no way to monitor and enforce what policies it adopted.

Despite this, however, the regulations were denounced by groups like the Direct Marketing Association and others in the media and advertising business for stifling growth opportunities in these various industries. They claim that since websites like Google and Facebook already collect consumer data and use it to generate advertising revenue that other telecommunications companies should be able to do the same.

Rather than being a democratic demand, this is an attempt by what were once largely phone or television companies to cash in on the revenue stream that companies like Google and Facebook make through targeted advertising. For example, Google made $17.3 billion in revenue in 2015, of which $15.5 billion was from advertising sales.

The reason Google, along with Facebook, Twitter and other social media platforms have made such huge amounts of money from advertising is that they are able to take the information they collect about a person's online habits and generate ads that target said person's interests. While the algorithms that make targeted ads are not always correct, they are far more lucrative than serving the same ads to everyone and the algorithms are constantly being improved.

A company like Comcast, however, has an advantage that a website like Google does not. Google is only able to collect data when a person is using a Google device (like an Android or Chromebook) or using an internet browser. In contrast, Comcast is able to collect every

bit of someone's internet activity. This includes if someone is using an email client, logging on to a private network, playing an online video game, getting updates to programs or operating systems, using an instant messenger and the myriad other ways people use the internet.

Moreover, Comcast also provides phone, television and even home security services. Phone calls can be recorded, and voicemails are recorded, stored and converted into text. Television viewing habits are noted. It is even possible, with the sort of data Comcast collects, to figure out someone's work schedule. Given that it is likely that the FCC rules will be fully struck down, these companies will be able to sell all of this information, allowing advertisers to escalate targeted advertising from internet browsing to television and beyond.

What will happen to all this information if one of these companies is hacked? The amount of information they are poised to start selling is even more invasive and private than what is collected by Google, et. al. What are the guarantees that this information will not be compromised or leaked and exposed for all to see?

More importantly, however, is the relationship between these companies and the state. As exposed by the Snowden revelations, organizations like the National Security Administration collect internet traffic both by tapping into the physical infrastructure of the internet as well as asking the various Silicon Valley companies to share the data they collect. Once the FCC ruling is struck down, the US intelligence agencies will have access to even more ways to spy on the population.

Of course, such invasive surveillance by the US government could already be occurring, though the leaks of the past five years have not yet indicated this. However, knowing the history and relationships between these companies and the US government, such collusion is no doubt at least being planned as the alliance between corporations and the state strengthens.