Internet Privacy in the Crosshairs: What Do You Have to Lose?

Washington lawmakers have voted to overturn an Obama-era rule designed to strengthen Internet privacy by limiting what companies can do with personal user data that is collected online. The bill raises questions and concerns about how consumers will be affected and what individuals might do to protect their privacy.

For ISPs such as AT&T, Verizon, and Comcast, the repeal of the FCC rule represents a chance to garner a piece of the $83 billion online advertising market that has thus far been dominated by Internet giants such as Google and Facebook.

In a vote that was divided largely along party lines, Congress has agreed to nullify rules set forth by the Federal Communications Commission (FCC) in October 2016 that would require Internet Service Providers (ISPs) to obtain permission from their users before collecting personal information and selling it to advertisers and other third-party entities. The rule, which was set to go into effect later this year, had also required ISPs to step-up security measures to help prevent large-scale data breaches similar to those suffered in recent years by Yahoo, Target, and many others.

Specifically, the types of personal information the FCC's rule intended to protect included, "financial information, health information, Social Security numbers, precise geo-location information, information pertaining to children, content of communications, web browsing history, [and] application usage history."[1]

What's at Stake?

For ISPs such as AT&T, Verizon, and Comcast, the repeal of the FCC rule represents a chance to garner a piece of the $83 billion online advertising market that has thus far been dominated by Internet giants such as Google and Facebook. The fact that the FCC's rule would not have applied to these two companies or other search engines and websites that already collect and use personal consumer data has been a sticking point for ISPs who long to level the competitive playing field.

On that score, consumer advocates assert that while individuals can easily stop using a website or search engine whose privacy policies they oppose, abandoning an ISP is a different matter. Users need an ISP to gain Internet access and, according to government data, in many parts of the country there are only one or two broadband companies to choose from.

Further, consumer watchdogs point out that ISPs are in a position to know and gather much more information about a user's online activities than an individual search engine or website simply because they have a record of all the sites a customer visits.

Proponents of the repeal say that the FCC's rules defined privacy too broadly and

put broadband and wireless companies at a competitive disadvantage with online advertisers such as Google and Facebook, which are monitored by a different agency, the Federal Trade Commission (FTC). The FTC's privacy guidelines are more lenient in that the agency does not consider browsing history or app usage data to be sensitive and subject to protection.

Ideally, critics of the FCC rules want the agency to adopt rules that are in line with the FTC's less stringent guidelines.

How Will Your Online Experience Change?

If the new FCC regulations had gone into effect later this year, users logging on to the web may have begun seeing a request from their ISP for permission to access and share their information. But since the rules were never implemented, chances are you won't notice much difference in your online experience. That said, keep in mind that the leading business model among online companies is ad-supported, which means the average user likely sees -- and will continue to see -- ads based on his or her online activity. For instance, if you are planning a trip to the Caribbean, you may see more ads for all-inclusive resorts. Purchasing a home? You may see ads for realtors in your area and/or related service providers, including banks.

Protecting Your Privacy

According to Jules Polonetsky, privacy expert and CEO of the Future of Privacy Forum, effective control over personal data online "has become incredibly complex. Cookie controls are increasingly meaningless, because companies that fingerprint consumer devices track without cookies."[2] That said, here are a few suggestions that could potentially help strengthen your privacy practices.

- Consider using a virtual private network (VPN) service. A VPN creates a secure, encrypted connection for data leaving your device that makes it difficult for your ISP to collect.
- Standard ad industry opt-outs can be effective for declining ads targeted based on web surfing. If you see a triangle "I" on a banner ad, the company is offering you an opt-out.
- "Do Not Track" feature -- Web browsers may include some type of Do Not Track setting that lets you tell websites you visit, their advertisers, and content providers that you don't want your browsing behavior tracked. Selecting this setting does not guarantee that the websites you visit will honor your request. It just lets them know of your wishes.
- Use the "Limit Ad Tracking" feature on your smartphone. Generally these types of settings help users to opt out of targeted ads, but again, there is no guarantee that your data will remain private.
- Contact your ISP -- Ask them about the types of data they collect and what their procedures are for opting out of ad-targeting programs.

[1]Federal Communications Commission, "Protecting the Privacy of Customers of Broadband and Other Telecommunications Services," December 2, 2016.

[2]Future of Privacy Forum, "Broadband Privacy and the FCC: Protect Consumers from Being Deceived and from Unfair Practices," March 11, 2016.