Protecting Your Internet Activity at Home and in the Office

by Hyatt Shirkey

On September 21, 2017, a "Congressional disapproval under chapter 8 of title 5, United States Code, of the rule submitted by the Federal Communications Commission relating to 'Protecting the Privacy of Customers of Broadband and Other Telecommunications Services'" became effective.[1] The result is that an Internet Service Provider (ISP) can collect and sell customers' internet activity. The ISP is the company that gives a consumer access to the internet (Cox, Comcast, Verizon, etc.). The detail of the activity varies based mostly on the security features of the website, but an ISP almost always knows where the user goes online and when.

Other companies and services, such as Google and Facebook, can do the same thing, but they are much easier to avoid. If a user doesn't want Google knowing their activity, they can change search engines, logout of Google, and use another browser. Users cannot change search engines or logout to avoid the ISP. Also, Google and Facebook only know what a user does online that involves Google and Facebook websites. Also, Google and Facebook have a motivation to keep the information as a competitive advantage; the only value to an ISP is to sell the information. An ISP can know a lot about what a customer does online. Based on the security of the connection, an ISP can know every detail of the customer's activity on each website they visit. This change in the law allows ISPs with that information almost limitless options.

There are some benefits that this expansion in the internet usage law could provide. Large research companies and universities could buy chunks of ISP data to learn about people's behaviors. Psychologists could purchase activity after a major event to learn about aspects of the nation's reaction, and investors may find relationships between a given news source and market activity. The primary concern on this new market for ISPs has been companies buying this data and using it for direct advertising. Business magazines can send offers to users who often visit business pages, political candidates can target voters who may be more likely to be undecided, and users who often or for an extended period use websites designed for trading stocks may see additional loan or investment advertising. There is a wide variety of uses in the private market for people's internet activity.

Critics often cite "big business" as the motive for this Congressional Disapproval (and that may be), but there may also be law enforcement implications as well. In *Kyllo v. U.S.*,[2] the United State Supreme Court drew a distinction between the government using something that is "in general public use" and something that is not when evaluating whether police using a thermal-imaging device was a violation of the Fourth Amendment. Making internet usage available for purchase may implicate what is or is not a search by law enforcement.

Several options exist to reverse this change in the law, but not without cost. The most simple and effective possibility is to call your ISP and find out if they allow you to opt out of them selling your data. If that isn't a possibility, one of the best ways to preserve anonymity is a Virtual Private Network (VPN). This will send your internet activity to one or more servers before your chosen destination. If you use this all the time, the ISP would only see that VPN in your usage. It would look as though you only visit one internet location. It is important to carefully select your VPN provider or you may just be changing who you give your information to. A reputable VPN provider will offer multiple connection points, make no record of your activity, and charge you. There are two negatives. First, it is an added, although nominal, expense. Second, it may slow your internet usage because it has more places to go. Additionally, if you go to a website and it starts with https ("s" is key), then your ISP should not be able to see content, but will still know the location, time, and duration of your visits. When protecting internet privacy, keep in mind that there are other risks beyond the new issue of ISP tracking. Malicious applications can log and transmit your keystrokes, and your employer's tracking or router hacking can track your activity. Also, as mentioned, Google, Facebook, Amazon, etc. track and store information about you. Like the call-recording warning before a phone call, don't forget you are being watched when you are online.

Endnotes:

1 82 FR 44118 was approved April 2, 2017. *See also,* 47 CFR 64.

2 533 U.S. 27

Hyatt Shirkey is a member of the Virginia State Bar's Special Committee on Technology and the Practice of Law. His Roanoke area practice includes criminal defense, elder law litigation, custody, and work as a guardian ad litem. He has taught courses on Microsoft Applications and undergraduate courses on law. He has also been published in the areas of law and psychology.