# ISP Tracking of Our Online Actions and How We Can Minimize It

# “ISP” refers to our Internet Service Providers

Charter / Spectrum

AT&T

Mobile provers such as Verizon, T-Mobile, Sprint, and AT&T

I have based much of this presentation on an April 3 article by Glenn Fleishman on macworld.com

http://www.macworld.com/article/3186967/os-x/protect-against-potential-isp-snooping-by-using-https-and-a-vpn.html

The article comprises two main points:

(1) The Federal Communications Commission (FCC) under the Obama Administration created a new set of restrictions on Internet service providers (ISPs) intended to define more clearly and explicitly bar greater use of our information that ISPs could conceivably gather, store, and sell. A Congressional joint resolution … prevents those new rules from going into effect.
**The status quo remains.**

(2) There are at least 2 means available of hiding your online activity, preventing your ISP from seeing it and selling it.

A. Use of https connections

B. Use of a Virtual Private Network

A. Encryption of your web traffic via an htpps connection

"Web encryption via an https connection from your browser protects your browsing end to end… Though the Web server's operator can obviously see what you're up to, nobody in between can.

A. https connection, continued:

With https, an ISP can intercept the name of the Web site to which you connect…  but nothing more detailed.

"You can't rely on https to protect you from snooping, but it turns the dials down on a lot of specifics. The Web is rapidly moving to https being available everywhere, and beyond that to https-only Web sites."

A. https connection, continued:

For more on https see this site

https://www.instantssl.com/ssl-certificate-products/https.html

B. Use a Virtual Private Network (VPN)

A VPN “encrypts all the connections of any kind leaving your computer and decrypts it at some point on the Internet where the VPN operator has a termination point, usually in a data center, **which can be located in a country that’s not your own.**”

(Think China, Russia, etc)

B. VPN, continued:

A VPN “cloaks everything. Neither an ISP nor any party between you and the VPN termination point can inspect what you’re doing, except the amount of traffic flowing.”

## B. VPN, continued:

The downsides to using a VPN:

1. The good ones cost money
App Store VPNs range from free to $16.99 per month via In-App Purchases.

2. They can slow your browsing performance
Because a VPN terminates at another point, it can slowdown
(a) throughput (the net amount of bytes flowing) and
(b) latency (the time between an action happening on one side of the connection and a response being received on the other).

Glenn advises, re choosing a VPN:

"It's important to find a VPN run by a company with some history you can find online, so they aren't freshly minted or anonymous, and in a country that upholds legal norms."

He uses Cloak:
https://www.getcloak.com

For selecting a VPN he recommends this site:

https://thatoneprivacysite.net/choosing-the-best-vpn-for-you/

For more on ISP tracking and your web browsing privacy:

— A search of the Mac App Store for VPN returned over 40 apps.

— Listen to this story on last week's Science Friday

https://www.sciencefriday.com/segments/how-trump-is-letting-internet-providers-sell-your-data/

Recent statements from ISPs regarding selling customers' browsing history

https://arstechnica.com/tech-policy/2017/03/comcast-we-wont-sell-browser-history-and-you-can-opt-out-of-targeted-ads/-can-opt-out-of-targeted-ads/

https://prodnet.www.neca.org/publicationsdocs/wwpdf/12717ctia.pdf