**Sandip Rai**

**Sa6662px@metrostate.edu**

**Protecting Our Online Privacy (Finished Edit)**

Many of you may have heard about the recent passage of a bill by Congress allowing Internet Service Providers (ISPs) to sell their customers’ browsing histories to advertisers. This one bill has essentially killed our online privacy. Our browsing histories are, after all, a treasure trove of data which can reveal almost everything about us: which sites we visit, where we bank, our shopping habits, our health concerns, our sexual orientation, and even when we are home.

Technology has made our life easier, certainly, but it has also left us far more vulnerable. A criminal from the other side of the world can easily hack our computers, mobiles and even our smart TVs. Everything we do online, whether on Facebook, Google, or indeed almost any website is recorded, packaged, and then sold to advertisers to target specific ads at us. One day, we start shopping for maternity wear, and the next every advertisement we see is directed towards new mothers. Even innocuous-seeming things, like Facebook’s new personal assistant ‘M,’ have the propensity to expose our personal information, with its ability to read all of our Facebook Messenger conversations. It’s high time for us to protect our online privacy, lest we expose our every moment, our every desire, our every purchase to outsiders. After all, our privacy needs to be private to ourselves and ourselves alone, and so this must become our most critical priority.

This article focuses on specific tools and applications that can help us prevent the leakage of our online privacy to outsiders. Messaging, browsing and emails will be the main focus.

**Messaging**

Texting has become the cornerstone of this generation. Yet most of the ways we send messages – from SMS to Facebook Messenger. – don’t encrypt our messages and often store full copies on company servers, making them vulnerable to being hacked and exposed. But there are secure options.

WhatsApp is the best popular messaging platform for online anonymity, as it encrypts every message we send and receive. Apple’s iMessage also provides encryption for texts, while the Signal Private Messenger offers even better encryption on both Android and iOS (it’s available in the Google Play store and the Apple App Store). The popularity of Signal is huge right now, as many politicians, journalists and activists use it to communicate, while WhatsApp uses the same underlying technology for its encryption. Notably, all of these options use end-to-end (E2E) encryption, which makes the encrypted data available only to the communicating users; WhatsApp never sees it, Signal never sees it, and even criminal hackers won’t be able to break through the encryption.

**Browsing**

For complete online privacy when browsing, the new Brave browser is a fantastic option which blocks advertising and the tracking cookies used to track the pages we visit. Better, Brave integrates HTTPS Everywhere, which forces supporting websites to use the secure, encrypted HTTPS pipeline for transferring data.

Popular web browsers, like Chrome and Firefox, don’t provide these features to users by default, but they are available as extensions; uBlock Origin is a great ad and tracking cookie blocker available for most browsers, and HTTPS Everywhere is also available as a browser extension.

The Tor Browser goes a step further, deleting almost all identifying information and routing connections through other browser users, making it impossible for anyone to identify the origin of your browsing traffic.

However, the Tor Browser is limited and often slow. A virtual private network (VPN) is an alternative – by using one, only the VPN provider will be able to see your internet traffic, not your ISP. Notably, the excellent Opera browser provides free VPN service for PCs and a free VPN app for iPhones and Android.

**Email**

Gmail is the most popular email client, but what it lacks is privacy. Gmail reads every email we share and then filters and categorizes them. If we want to send a sensitive email, Gmail will still index it. So, looking for a more privacy-conscious alternative, some scientists at CERN (a European organization for nuclear research) created an encrypted email offering called ProtonMail. This email client is essentially the ultimate private email option right now, featureing E2E-encrypted emails, anonymous emails, and auto-deleting and password-protected emails.

**Online Searches**

Googling is the thing we do if we have any query to be answered. But what most of us miss is that Google records every search we make. Our searches can then give them a complete picture of us: our interests, sexual orientations, our likes and dislikes, and even our professions. We lose our online privacy by searching on Google. This is where the DuckDuckGo search engine comes in: DuckDuckGo provides almost all the features of Google without storing our searches. Because it doesn’t store any search we make, it safeguards our online privacy. Other options include the Disconnect Search browser extension, which encrypts all of our searches even if we use Google, Bing or other search engines.

(Editor’s text) For more on what websites know about you, check our this article from our April edition: http://themetropolitan.metrostate.edu/issue/2017/04/007/

