Tor Anonymizer for Lawyers

By Christopher B. Hopkins

As a young student, did you ever dream of skipping school by pulling the fire alarm? Maybe you thought of a devilish plan to call in a fake bomb threat to avoid a test. In our wireless era, such felonious hijinx would be a pitifully low-tech way to violate Florida Statutes 790.164 or 806.101. Just ask Eldo Kim, a (now former) sophomore at Harvard who anonymously *emailed* a bomb threat to avoid an exam. A perspicacious idea… until the FBI followed the electronic trail back to his laptop.

Lawyers and their clients can travel the internet undetected as long as they use "Tor," an internet anonymizing service, and take certain steps before sending emails or files. Tor is a legitimate service which you and your clients should to consider in light of the Snowden disclosures about mass surveillance. Originally developed by the U.S. Naval Research Laboratory, and now operated by a non-profit association, Tor encrypts your identity on the internet -- which is completely legal -- using standards which even the NSA has admitted is "the king of high-secure, low latency anonymity." If you can avoid human errors, Tor is the safest way to be anonymous online.

What is Tor and Is It Legal?

"Tor" stands for "The Onion Router" which creates anonymity on the web by bouncing your internet traffic through a myriad of nodes before reaching your intended destination. The end result is that your internet protocol address is obscured. It is legal to use Tor. Head over to TorProject.org and, within five clicks, you can install a Tor browser.

Why Do I Need to Be Anonymous?

As a website operator, I can see details about visitors: what Google search lead them to my site; whether they are using a Mac or PC; and even what browser they are running. Commercial sites are tracking visitors in greater detail (*e.g.*, if you close Facebook but never log off). A lot of sites can see your IP address -- the equivalent to the license plate on your getaway car -- which could lead someone back to your computer.

You may not want every internet search you perform to be tracked. At least occasionally, you will want to be anonymous on the internet. Likewise, there are times when you may want to send a document or image without it being traced back to you. Using Tor, you could create an email account and send files without the recipient knowing your identity.

Why Don't We Use Tor as a Default and Always Be Anonymous?

Speed and convenience keep us from using Tor for all internet traffic. First, using Tor takes twice as long to load a webpage. Second, there is a convenience to being "tracked." The exchange of "cookies" allows frequently-visited sites to appear more welcoming based upon your prior visits. Finally, for true anonymity, you would not log into accounts, accept cookies, or run "plug-ins" since those steps would betray your identity.

To this end, do not confuse Chrome's "incognito" mode or Explorer's "InPrivate Browsing" for Tor. The two former settings leave no trace of your web cruising *on your computer* by not saving cookies or browser history. Anyone in contact with you on the internet can still see you.

Can't the NSA Already Crack Tor?

It is hard to tell if the government can crack Tor. In September 2013, the New York Times reported, "NSA Able to Foil Basic Safeguards on the Web." That said, the NSA was identifying people by intercepting their transmissions *before* they reached Tor. On the other hand, four months ago, the Guardian published an internal NSA presentation entitled "Tor Stinks" which bemoaned the fact that "we will never be able to de-anonymize all Tor users all the time." Rather than be concerned about weaknesses in Tor's encryption, the first rule of anonymity is not making careless mistakes.

Lessons from Mr. Kim and Mr. Post

So how did our Harvard student get caught sending bomb-threat emails if he was smart enough to use Tor? Mr. Kim reportedly used his student ID to log into Harvard's wifi to send the anonymous email. The IP address on the email header was clearly anonymized so the school could not track him. But Harvard's IT people guessed that the threat was internal and they looked to see whether anyone on Harvard's system was using Tor around the time that the threatening email was sent. Once confronted, the FBI reports that Mr. Kim confessed. Lesson: to be truly anonymous, how you connect to the internet needs to be hidden from those who may be looking for you.

Similarly, to be anonymous, anything you transmit must not betray your identity. In *United States v. Post*, the defendant was apprehended uploading child pornography despite the fact he used Tor. Federal agents simply downloaded the images and found metadata revealing GPS coordinates, date, and that the images were taken with an iPhone 4. Using Yahoo Maps, the authorities visited Mr. Post and discovered a couch shown in the photos and his iPhone 4. Lesson: even though Tor transmissions are anonymous, any files sent over the internet need to be scrubbed of any identifying information.

Anonymity online is not just for alleged criminals. But you can learn from their mistakes.

Christopher B. Hopkins is a shareholder at Akerman LLP. Send your unscrambled questions or comments to christopher.hopkins@akerman.com.

Technology Seminar

April 11, 11:45-1:00 p.m.

"ESI Discovery for the Technically Challenged"