Ashley Madison and the Deep (and Sometimes Dark) Web

by Sharon D. Nelson, Esq. and John W. Simek

There are lawyers – mostly family and criminal defense lawyers – who know at least a little about the Deep Web and the Dark Web. But the average lawyer? Not so much. In fact, after the Ashley Madison breach, a lot of family law colleagues began asking us questions about the Deep Web and the Dark Web – where the full steamy contents of the Ashley Madison breach were published in many places. Most had no clue that there was any distinction between the Deep Web and the Dark Web.

So what is the Deep Web? Think of the Web we search (via Google or other search engines) as an iceberg. Conventional browsers only index about 4% of the Web – that's the top of the iceberg. Everything beneath the waters is the Deep Web – 96% of the Internet content. That content is deliberately kept away from conventional search engines, via encryption and masked IP addresses - and accessible only by special web browsers.

Much of the Deep Web is perfectly legitimate. Many privacy advocates are there, wishing to operate without being tracked. Journalists are often there, generally concerned about government prying. You can also find whistleblowing sites. Some of it is also dynamically generated web pages or forums which require registration.

We're not sure how much of the Deep Web is also the Dark Web though experts say it is a small percentage. The Dark Web contains the seamy places where drugs and guns are sold, human trafficking occurs, criminals offer their services for hire, hackers and cybercriminals operate and child porn is viewed, distributed and sold. And those are only some of the activities on the Dark Web.

Most people, if they know the Dark Web at all, know it because of the black market website called Silk Road – which was shut down twice by the FBI in 2013-2014. Silk Road's founder, Ross Ulbricht, was convicted of a number of crimes, including several attempted murders-for-hire.

Sometimes, the Dark Web is known as the Darknet. By whatever name you use, it is accessed via Tor (The Onion Router), Freenet or I2P (Invisible Internet Project), all of which use masked IP addresses to allow users and website owners to operate anonymously. In common parlance, when you use Tor, you are in Onionland.

It amazes most lawyers when we tell them that Tor was originally funded by the U.S. Department of Defense. While it is now a nonprofit run by volunteers, it is funded in part by the U.S. government and the National Science Foundation.

Why would the U.S. government support it? Because it is part of the State Department's Internet freedom agenda, allowing people in repressive countries to have access to data censured by their governments. Even Facebook has a version of its site on the Dark Web in order to make it easier to use in countries that restrict Facebook, such as China and Iran.

We spend some time there because of our work as criminal defense expert witnesses as part of our digital forensics work. And recently, we've helped family law colleagues ferret out some of the Ashley Madison evidence.

Make no mistake about it – the family law grapevine is rife with stories about snaring clients since the AM breach. And as many conventional sites began to remove Ashley Madison information upon request, or to report the information only in part, the lawyers surged to Tor to find more evidence in their cases.

Since we find questions about the Deep Web and the Dark Web popping up frequently in our recent presentations, we though a small primer would be timely. Happy travels in Onionland – just be careful which streets you walk down!

The authors are the President and Vice President of Sensei Enterprises, Inc., a legal technology, information security and digital forensics firm based in Fairfax, VA. 703-359-0700 (phone) www.senseient.com