Vol. 41 No. 1 Fall 2014

Litigation

American Bar Association

The Journal of the Section of Litigation

Practice Makes Perfect

American Prosecutorial Imperialism?

The State of Clinical Education

Interview with Gary P. Naftalis

iWitness

HOW TO PROTECT DATA FROM UNCLE SAM

SHARON D. NELSON AND JOHN W. SIMEK

The authors are the president and vice president of Sensei Enterprises, Inc., Fairfax, Virginia.

At least once a week we are reminded that law firms' cybersecurity is at risk, and a newly discovered threat is the National Security Agency (NSA). Courtesy of Edward Snowden—love him or hate him, we believe he exposed substantial illegal and unconstitutional activity—we have learned that the United States is closer to the Big Brother state of George Orwell's *1984* than we ever thought possible.

Implications for Lawyers

Snowden has revealed that the NSA has broken privacy rules or overstepped its legal authority thousands of times each year since it was granted broad new powers in 2008. Most of the violations involved unauthorized surveillance of Americans or foreign intelligence agents in the United States. This surveillance, restricted under statute and executive order, resulted in the interception of emails and telephone calls.

How do they do that? Recent reports indicate that the NSA is intercepting shipments of computers purchased online in order to infect them with spyware or replace certain components with its own malware-infested hardware.

But suppose you didn't order a new computer. How could the NSA intercept your data? One possibility is called the NIGHTSTAND. It is designed to hack WiFi devices from eight miles away. It is a stand-alone tool that can exploit targets including Win2K, WinXP, WinXP SP1, and Win XP SP2 systems running Internet Explorer versions 5.0–6.0. There is no report that the NSA has hardware for the more modern operating systems or browsers. Yet another reason to make sure you are up to date with patches and versions.

The *Guardian* has also revealed, by way of another Snowden leak, new details on a very powerful, secret program run by the U.S. government called XKeyscore. With the program, NSA employees can obtain everything from phone numbers to email addresses, and can see email content, Internet activity, browser history, and an Internet provider address. According to the files and to Snowden, no warrant is needed.

And the NSA has some help in its efforts. According to yet another article from the *Guardian*, Microsoft has

- helped the NSA circumvent its encryption so that the agency can intercept web chats on the Outlook.com portal;
- given pre-encryption stage access to email on Outlook.com, including Hotmail;
- allowed the NSA easier access to SkyDrive; and
- helped to triple the amount of Skype video calls being collected through Prism.

As if the global surveillance capabilities of the NSA aren't enough, our friends from the Five Eyes Alliance (Australia, Canada, New Zealand, the United Kingdom, and the United States) are lending a hand, too. The *New York Times* reported that the NSA's Australian counterpart conducted surveillance of trade talks between Indonesian officials and an American law firm. So capturing privileged communications doesn't appear to be limited to the NSA.

Another report revealed that the NSA has the ability to capture 100 percent of a foreign country's telephone calls and then rewind and review them up to 30 days after they occur. So much for protecting the attorney-client privilege, especially if your client is in a targeted country.

The NSA revelations have serious implications for lawyers. For example, we used to tell lawyers that Skype was secure, but then Microsoft bought it and began changing the network architecture and now, apparently, unlocking data for the NSA. And what about the lawyers who are storing their data in SkyDrive? Or the solos who are using Hotmail? How does a lawyer keep data confidential?

Roughly half of all law firms are now holding at least some data in the cloud.

The recent news has shaken them, as well it should, but we are not preaching a mass exodus from cloud servers. Two major points here:

- If you are storing all your data in a data center, your biggest concern should be whether the data center personnel can gain access to your data. For this reason, we do not recommend putting law firm data on servers owned by the data center. It doesn't matter whether there is a master decryption key or whether a "backdoor" is built in. The safest way to store data in a data center is to use a hybrid solution—where you own the equipment and the access to your equipment and data are restricted to you and your own information technology folks in locked racks. Any emergency access to the data, by contract, should require immediate reporting to you, and, again by contract, you should receive notice of any law enforcement request for the data right away so you can file a motion to quash. Major players in the market may not give you these terms, but the smaller ones will. One caveat: If a request is made under the Patriot Act, you're toast—your data will be handed over on a silver platter. But the vast majority of law enforcement requests are not made pursuant to the Patriot Act.

- If you are using specific clouds to store data, encrypt your data before sending them. A great example is Dropbox, now utilized by many litigators. If you encrypt your Word or PDF documents before putting them in Dropbox, it doesn't matter that Dropbox holds a master decryption key (and it does). Even if it attempts to decrypt data for the federal agents at the door, Dropbox can only provide them with garbage. Stop being afraid of the word "encryption." If you password-protect a Word or PDF document (which you can do natively within the program—just search Help), it is encrypted. Just be sure you don't send it as an attachment with the decrypt key in the text of the email.

Encryption

You should also take a hard look at encryption on your smartphones. iPhones are encrypted when configured with a password. BlackBerrys are natively encrypted when "Content Protection" is enabled. Android encryption must be turned on in Settings, but it is there.

No lawyer should be performing work on a personal machine. In today's world, every lawyer should be issued a firm laptop and smartphone, so security can be controlled and monitored. All laptops, like smartphones, should have whole disk encryption.

It is now a lawyer's ethical duty to address confidentiality in any engagement letter.

One disclaimer concerning the capabilities of the NSA is worth noting. As security commentator Bruce Schneier has stated, "The NSA is breaking most encryption on the Internet." Because of this, some have suggested using encryption and security products from vendors that are not based in the United States to minimize any potential NSA backdoors. The good news is that a large number of products do not use the flawed Dual EC DRBG, and remember, we are only talking here about compromising SSL certificates, not all encryption. But the NSA is also alleged (unproven at the time of this writing) to have used the Heartbleed bug to collect critical information. Schneier happily notes that, "strong encryption makes the NSA batty." So encrypt away.

Now that we know the NSA (and others) have the ability to capture huge quantities of communications (voice, text, email, etc.), you should also consider whether some method of secure communication should be used. As mentioned above, encryption is your friend, and encrypted voice and text communication is also possible. Mobile apps such as RedPhone or TextSecure allow for encrypted voice and text communications. Another alternative is to purchase the Blackphone, which provides encrypted voice and text communication built into the handset.

Also consider regular security audits. We used to tell firms to perform security audits every 6–12 months to keep the Chinese and the cybercriminals out of their networks. Now we add that you need to protect your networks against our own government—sad but true. So get a referral from trusted friends, check out credentials, do whatever you must, but don't fail to do these audits.

With all the examples of the NSA data-capture projects, we have changed our advice to lawyers concerning protection of client data. We believe it is now a lawyer's ethical duty to address confidentiality in any engagement letter and obtain informed consent from the client as to what measures need to be taken to protect the potential collection of client communications.

Now, lest we seem overly paranoid, we'll give the parting words to George Washington—who better than the father of our country?—who reportedly said: "Government is not reason, it is not eloquent, it is force; like fire, a troublesome servant and a fearful master." *See* http://en.wikiquote.org/wiki/George_Washington. ■