Ethical Implications of NSA Surveillance for Lawyers

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

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. After 9/11, many Americans embraced the Patriot Act, numb from the tragedy and justifiably concerned about terrorist plots on American soil. After some time, most folks became complacent and more or less bought the government's reassurance that federal surveillance involved primarily foreigners and that the Feds were not snooping on the activities of ordinary Americans.

That proved wrong in a big way. Courtesy of Edward Snowden (like him or hate him, he exposed a lot of illegal and unconstitutional activities), we have learned that the U.S. is closer to the "Big Brother" state of George Orwell's *1984* than we ever thought possible. So, what do we know now and what are the implications for lawyers?

Thanks again to Edward Snowden, *The Washington Post* published a story based on an internal National Security Agency (NSA) audit and other top-secret documents. The story indicates 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 U.S., surveillance that is restricted under statute and Executive Order, which resulted in the interception of e-mails 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 to replace certain components with its own malware-installed hardware. Now, you have to be specifically targeted by the NSA before you'll get a little "something extra" arriving along with your shiny new computer, but that's still pretty gutsy.

But suppose you didn't order a new computer. How could the NSA intercept your data? Additional revelations were disclosed at the Chaos Communications Congress. Apparently, there is a whole catalog of equipment and software that the NSA is willing to sell to other agencies. One such device is called the NIGHTSTAND. It is designed to hack WiFi devices from eight miles away. It is a standalone tool and 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 they have 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 e-mail addresses, and can see e-mail content, Internet activity, browser history, and an IP 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,* citing top-secret documents from you-know-who, 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 e-mail 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 (United States, United Kingdom, Canada, Australia and New Zealand) are lending a hand too. The *New York Times* reported that the NSA's Australian counterpart, the Australian Signals Directorate, notified the NSA that they were conducting surveillance of trade talks between Indonesian officials and an American law firm. Of course they were willing to share the information. The law firm is yet to be identified (though thought to be Mayer Brown), but capturing privileged communications doesn't appear to be limited to the NSA.

Another report revealed that the NSA has the ability to capture 100% of a foreign country's telephone calls and then rewind and review them up to 30 days after they occur. The released documents state that there is money budgeted to target five countries, but the countries are not identified. So much for protecting the client/attorney 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 by running the calls through its servers and now, apparently, unlocking data for the NSA from time to time. 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 datacenter, your biggest concern should be whether the datacenter personnel can gain access to your data. For this reason, we do not recommend putting law firm data on servers owned by the datacenter. It doesn't matter whether there is a master decryption key or whether a "back door" is built in. The safest way to store data in a datacenter is to use a hybrid solution – where you own the equipment and the access to your equipment and data is restricted to you and your own IT 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 it. 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. And in case you're wondering, yes, encryption will work for SkyDrive, the iCloud (depending on the data type and device used), and other cloud servers. And no, this is not hard. 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 promise us you won't send it as an attachment with the decrypt key in the text of the e-mail.

You should also take a hard look at encryption on your smartphones – iPhones are encrypted when configured with a PIN, although poorly if just a 4-digit pin, so use a complex 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. This means no BYOD unless you are prepared to implement a MDM (Mobile Device Manager) solution to the tune of several thousands of dollars. All laptops, like smartphones, should have whole disk encryption.

Bottom line…you should be encrypting data on all devices. Now 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." This is accomplished by intercepting the data and compromising the secure certificate provider infrastructure or using intentional weaknesses inserted in encryption products. As an example, RSA Security released an advisory to stop using the Dual Elliptic Curve Deterministic Random Bit Generation (Dual EC DRBG) because of weaknesses in the algorithm. Apparently, the NSA had their fingers in the design of Dual EC DRBG. 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 back doors. 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. The NSA is also alleged (unproven at the time of writing this article) to have used the Heartbleed bug to collect critical information. Mr. 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, e-mail, 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.

Another preventative tool should be 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 your 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 get informed consent from the client as to what measures need to be taken to protect the potential collection of client communication.

Now lest we seem overly paranoid, we'll give the parting words to George Washington – who better than the father of our country? ***"Government is not reason; it is not eloquent; it is force. Like fire, it is a dangerous servant and a fearful master."***

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