Encryption: Its Time Has Come

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

© 2014 Sensei Enterprises, Inc.

Lawyers tend to cringe when they hear the word "encryption." To most lawyers, encryption is a dark art, full of mathematical jargon and incomprehensible to the average human being.

When South Carolina suffered a major data breach of taxpayer data, what did Governor Nikki Halley say? "A lot of banks don't encrypt. It's very complicated. It's very cumbersome. There's a lot of numbers involved with it."

Leaving aside the laughable notion that a lot of banks don't encrypt data, the rest of her quote is in keeping with what we hear from lawyers. What we hear always translates into the same thing: Encryption is hard.

So let's make this more fun with some things you can relate to.

Encryption is designed to secure data from prying eyes. It keeps secrets secret. Think about your childhood. Did you play with invisible ink? Did you watch the mailbox for a magic decoder ring? Perhaps you spoke Pig Latin with a sibling so your parents remained clueless about what you were plotting.

You've seen secrets hidden in the movies – remember the World War II Navajo code talkers in "Windtalkers?" Cryptography has been featured in many movies, including the *National Treasure* movies, *Sneakers* and, perhaps most famously, in *The Da Vinci Code*.

See? Cryptography can be fun. Really!

In the simplest terms, cryptography is the science of secret communication. It involves transmitting and storing data in a form that only the intended recipient can read. Encryption is one form of cryptography.

Encryption is the conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form (plaintext), so it can be understood.

Read those two definitions a couple of times and presto – you have the essence of what encryption is about. Want it simpler still? Here it is in graphic form.

Plaintext → Encryption → Ciphertext → Decryption → Plaintext

It is a simple representation of a process that can be very complex, but this is the fundamental process that all encryption goes through from start to finish.

The goal of encryption is to make obtaining the information too resource-intensive (time, work and computing power) to be worthwhile. It is unlikely that there will ever be perfect encryption that can never be broken, particularly over extended periods of time. However, strong encryption, properly implemented, provides very strong protection.

Encryption can protect stored data (on servers, desktops, laptops, tablets, smartphones, portable devices, etc.) and transmitted data (over wired and wireless networks, including e-mail).

In the early days, people carved messages into wood or stone and the recipient had the "key" to know how to translate them. Today, cryptography is far more advanced and is found in streams of binary code that pass over wired networks, wireless networks and Internet communications pathways.

Fortunately, you don't have to understand the math and computer science behind encryption in order to use it. There are now many easy-to-use encryption tools available for end-users. Many of our clients are adopting ZixCorp for e-mail encryption, which integrates with Outlook. You don't need to use it all the time – just when you are transmitting sensitive data. Bottom line – it is EASY – and inexpensive. Clients love it.

While most attorneys will need help to set up encryption, it's generally not difficult after set up – often automatic or point-and-click.

Trust us, it has now reached the point where all attorneys should have encryption available for use, where appropriate, to protect client data.

No less an expert than Edward Snowden has said that strong encryption is currently the best defense we have to protect our data. Now is the time to think about adopting encryption – its time has come – even for law firms, almost always the laggards in adopting security technology.

The authors, in collaboration with Pittsburgh litigator Dave Ries, are the authors of the book Encryption Made Simple for Lawyers, scheduled for publication by the ABA next March. This post is partially excerpted from the introduction to that book. Authors Nelson and Simek 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.