Information Security, Leaking Data and the Duty of Confidentiality

By David J. Fetters

All attorneys owe clients a duty to their client information confidential.

A colleague and close friend called me in a panic a few months ago. A confidential memo from one of his previous cases had shown up in a Google search. Not just the name of the file, a link to the actual file. It was a letter between a group of attorneys discussing settlement, and understandably my friend was concerned that the contents of his computer might be showing up publicly on the internet. Social security numbers, bank account numbers, and confidential business information potentially shared with the world.

All attorneys owe clients a duty to their client information confidential. The Ohio Rules of Professional Conduct, at Rule 1.6, prohibits lawyers from "reveal[ing] information relating to the representation of a client, including information protected by the attorney-client privilege under applicable law," without informed consent from the client or the occurrence one of several other specified circumstances. The usual remedy to a known or potential inadvertent disclosure is notifying any clients or former clients who may have been affected. I gasped over the phone thinking of the sheer number of clients and former clients he would need to notify if it was true.

After one or two quick jokes at my friend's expense, I offered to help him figure out why we could both search for his confidential memo on Google. We determined fairly quickly that the file was being shared from a computer with a different internet protocol ("IP") address, a different service provider, and was located across town from his office. Moreover, none of his other clients' files turned up when he searched specifically for them. We had determined that it was not his computer that was sharing the file, but we still had no clue as to why it was showing up in Google.

I stumbled onto a website post with a list of thousands of IP addresses that were noted as having one of several ASUS brand routers with a massive security vulnerability. A quick search revealed that the other computer sharing the file was using one of the IP addresses listed as being vulnerable. CNET had picked up on the obscure post and published a more comprehensive explanation of the breach. The problem affected nearly a dozen models of ASUS brand routers sold for home or small office use.

The affected routers could accidentally be configured to share publicly the contents of any USB memory card or external storage plugged into it. Any owners who turned on one of ASUS's AiCloud services on their router would inadvertently enable global access to the files. Originally discovered in June 2013 by security researcher named Kyle Lovett, ASUS did not resolve the problem until sometime in 2014 when it released a firmware patch for the affected routers. Owners of vulnerable routers need to go to ASUS's website, and then download and install the patch to resolve the issue.

The incident served to remind my very relieved colleague and I that information security is at least as important as physical security. As the practice of law continues its inevitable march toward the paperless future, attorneys will need to remain vigilant of the ever changing nature of the threats to protected information. Major law firms have already been the targets of foreign hacker attacks. Small to medium sized firms, while arguably less likely to be the target of international espionage, can still improve their information security programs without investing much financially.

Developing a consistent password use policy is one of the easiest and most effective methods of improving security. Passwords do not need to be a mix of random letters and symbols to be secure. Long but ordinary sounding passwords, say your three favorite ADAs on Law and Order or a series of words that evoke a comically memorable visual, are ultimately more secure than a short sequence of random symbols. Using different passwords for email services and support services like PACER or Franklin County's eFiling program compartmentalizes the potential damage if one of those services suffers a data breach.

Another simple practice is remembering to use passwords on everything. Attorneys regularly deal with confidential client information whenever they pick up or interact with a digital device. Password protecting all manner of electronic devices, from personal cellphone and work computer to thumb drive or home computer, is an easy way to decrease the likelihood of revealing confidential information.

Consider the serious threat posed by the humble, omnipresent USB thumb drive. Commonly available USB storage devices can easily hold whole libraries of documents or years of confidential State Department cables. Get in the practice of using only one thumb drive for client materials, and regularly remove files that are not actively needed to limit the potential damage of loss or theft. The prices for thumb drives are so low that it is well worth it to invest in one with encryption capabilities. While losing one will still be a frustrating event, encryption can prevent it from being a costly and embarrassing event.

David J. Fetters
Barney DeBrosse, LLC
david.fetters@gmail.com