

# Can You Trust Your Expert Witnesses with Confidential Data?

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

© 2017 Sensei Enterprises, Inc.

Not always. There was a recent case in which confidential data was not, to put it mildly, well handled. The corporate defendant, a mortgage servicer, was accused of violating a consumer's privacy rights based on the manner in which it handled collection calls. The defendant protected its customer data with layers of network security consistent with best practices and ISO guidelines. During discovery, the plaintiff's experts received the calling data and copies of the customer service call recordings.

Both experts had unrelated full-time day jobs. Their expert witness work was a side business run out of their homes. Neither expert had a technical degree, and neither had taken a course in data security for over a decade. Both experts stored the sensitive case data in their homes. There were no locks on the doors to their home offices, so anyone in the houses had access to the drives. Neither expert was familiar with the basic ISO standards relating to data security. Neither had a written data security plan for their home network, and no outside company had ever performed vulnerability or penetration testing on their networks. One expert had no automatic intrusion detection software on his network. Both routinely produced data with sensitive PII (personally identifiable information) in unencrypted form.

The produced debt-collection calls included highly personal discussions in which debtors explained why a mortgage was in default, such as health or financial problems. One expert testified that he kept these recordings on an unencrypted portable laptop and accessed it on his home and public Wi-Fi networks. He also produced the call recordings to a third party to obtain technical assistance. The third party was not asked to execute the protective order, and that data presumably still resides on the third party's servers.

Well, you get the message. Expert witnesses, including us, routinely receive highly sensitive PII for review and analysis. Sensitive PII (SPII) is data that, if lost, compromised or disclosed without authorization, could result in substantial harm or embarrassment to the individual.

Attorneys cannot ignore how their experts manage the data produced to them. When highly sensitive data is produced in a lawsuit, it is removed from the protected network environment built by the data's owner and produced to the lawyers on the other side. The manner in which it is produced is up to the producing party. Sometimes the data is scrubbed of identifying information, such as names and dates of birth, but not always. Sometimes it is produced on encrypted drives, but again, not always. Instructions are rarely given to an expert regarding the manner in which to store the data or the type of security controls that need to be employed to keep it safe from unauthorized disclosure. That is certainly true. I can only recall a handful of cases where attorneys have given us explicit instructions.

Confidential data produced in a lawsuit is often subject to a protective order that contains generic language that the data will be kept confidential. Protective orders typically do not specify the security measures that the receiving party needs to have in place. The promise to keep the data protected is considered enough.

Under most protective orders, the receiving party has the right to produce the confidential information it receives to its experts in the case. Those experts are in turn required to sign the protective order and promise to protect the data. Again, the promise to keep the data protected is considered enough.

Experts at sophisticated firms generally have very competent IT and cybersecurity support. They could still be breached, but it is less likely than when engaging experts who are self-employed or who work in small firms with limited support.

Concrete suggestions?

Pay attention to physical security. Our forensics lab requires a prox card and a registered fingerprint to enter. Entries into or out of the lab are video recorded. There is a dual authenticated safe in the lab for high profile cases. Only three of us have access to that safe. We have a security system with motion sensors – and the police will be summoned unless someone with authority quickly acknowledges an equipment problem or a mistake (such as arming the system when someone is still in the lab – and yes, of course that has happened). We have a human receptionist monitoring the front door – in addition to more surveillance cameras. The building itself is locked nights and weekends.

Pay attention to logical security. Our evidence is on standalone offline hard drives or on a NAS unit which has no Internet access. The local network in the forensics lab is dedicated to forensic usage, unconnected to our corporate network. There are software and hardware protections for the lab network as well.

Pay attention to production security. It is the way of the world that most of our productions, by the instructions of our clients, are made via Dropbox. It makes sense since it is instantly available though one must trust that authorized access is not given by the receiving party to anyone who shouldn't have it. All production files are encrypted using 7-Zip before being placed in Dropbox with the password given via phone or a separate e-mail (not the e-mail containing the Dropbox link). If a file is not so large that it cannot be accommodated by Mimecast's Large File Send, we may use that – the data is encrypted as part of the process.

If we use the old school method of shipping drives, they are always encrypted.

There may be more security measures that are not coming to mind, but those are the basics. And, of course, if there is a court order with specific mandates, that order must be strictly adhered to. Most of them, as noted, do not require specifics measures.

*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*