Data Security and the Expert Witness: 14 Security Questions to Ask Your Witness

It is not safe to assume that every expert will keep data secure simply because they say they will.

Margaret A. Daley, Berkeley Research Group, Law Technology News

May 18, 2017

This article is Part 2 of a two-part series exploring sensitive data and expert witnesses. Part 1 published on Legaltechnews.com in March.

Everyone involved in the judicial process—judges, parties and experts—has an obligation to help protect sensitive third-party data produced in litigation. Simply executing a protective order and hoping for the best is insufficient when it is clear that an expert witness is operating out of her or his house or is otherwise without adequate technical support. This is true even if the expert witness appears to be technically savvy. Counsel for both the producing and receiving parties must have a basic understanding of the adequacy of their experts' network security before providing them with highly sensitive consumer data. Surely, counsel would not want their own personal data or health information loaded onto some stranger's home network with little or no security controls in place.

In order to assist in this necessary inquiry, below is a list of key questions to ask an expert witness before producing sensitive personally identifiable information (SPII) data to him or her.

Key Questions to Ask Your Expert Witness About Data Security

- Do you have a written data security/data privacy plan, and can I have a copy?
- Do you perform annual security audits of your network security, and can I have a copy of the most recent review? If not, why?
- Under what circumstances do you encrypt data? Are all the devices on which you store case data encrypted, including your traveling laptop?
- Under what circumstances do you scramble SPII data resident in databases?
- How do you transmit and store personally identifiable information and confidential data of third parties that is produced to you?

- Will you be storing any of the data produced to you on a home network? If so, who else has access to this network? Do you have any file-level encryption or access controls on this home network?
- Where will you be physically storing hard drives or storage devices that are produced to you that contain confidential or SPII data? If you will be storing this data at your home, is there physical security (e.g., locked doors, locked drawers, key cards) in the room where you will be storing the data? Who else may have access to the room where you will be storing the data (e.g., children, other family members, household help)?
- Do you maintain chain of custody information for the data that is provided to you for your review as an expert witness? If yes, under what circumstances?
- Will you be storing any of the data produced to you on any cloud accounts? If so, where will it be stored? Who else may have access to that account? What data security/data privacy controls are in place at this third-party site?
- Will you be accessing any of the case data produced to you in this case on any home or public Wi-Fi networks? If so, which Wi-Fi networks do you anticipate using? What data security/data privacy controls are in place at the Wi-Fi source that ensure the data accessed through the site remains protected?
- Will anyone that is not an employee of your company be provided with access to the data produced in this case to assist you with your work? If so, have these third parties executed the protective order? What data security/data privacy controls are in place at the third-party site to protect the data?
- Do you have data security/cybersecurity insurance?
- What data destruction processes do you follow for confidential data and IT equipment/media?
- Under what circumstances will you notify me if there has been a disclosure of the data produced to you in this case to an unauthorized person?

Basic Rules for Expert Witness Data Security

The answers to the above questions will provide either comfort or alarm to the questioner. A few basic guidelines should be considered by counsel who retain expert witnesses in order to adequately protect confidential and SPII consumer data. These rules will also protect counsel who retained an expert in the event the expert is responsible for unauthorized disclosure of the data.

Given the availability of secure cloud services and the low cost of encryption software, significantly reducing the risk that an expert will inadvertently disclose SPII third-party data can be accomplished without much fuss and expense. Many experts are simply unaware of the risk they are running by failing to adequately secure the data produced to them. Once advised of basic security expectations, most will put the controls in place if their livelihood is dependent upon it.

Consumer PII and SPII should not be stored on insecure home networks or transmitted over public or effectively public home Wi-Fi networks. This kind of data should not be stored on the same computer an expert's children use to do their homework or to play Minecraft. Hard drives containing PII or SPII should be kept in a locked cabinet, not on top of a desk in an expert's unlocked home office. And no PII or SPII should ever be transported on unencrypted hard drives or other electronic storage devices.

This risky behavior will continue to take place if counsel assumes that an expert's signature on a protective order is sufficient to keep any kind of data secure. It is not safe to assume that every expert will keep the data secure simply because they say they will. It is time to move into a trust-and-verify world, particularly when the SPII data of innocent third parties is at stake.

- No SPII should be hosted on an expert's home computer network without the express consent of counsel and a reasonable assurance of data security.
- Only individuals who are employed by the expert or have signed the protective order should have access to a device containing SPII data.
- Any laptop or other portable storage device containing SPII must be encrypted.
- Data containing SPII should be scrambled or redacted, making consumer names and other PII unreadable before production to an expert witness, unless that data is necessary to the expert's analysis.
- A written data security plan should exist and be made available by any expert witness receiving consumer data.
- All expert witnesses receiving SPII data should carry cybersecurity insurance.
- No SPII should be produced by the expert to a third party without the written consent of the counsel who retained the expert, and must be governed by the same protective order provisions.

Margaret A. Daley is a managing director at Berkeley Research Group. She has over 25 years of experience in investigations, data analytics, dispute resolution, and regulatory compliance.