Beware the Internet of Things!

Connective devices could serve as backdoor threats from potential hackers

In earlier columns, we discussed the challenges attorneys face to become competent in electronic discovery and to keep pace with rapidly evolving electronic developments. We talked about the security of our devices and confidential lawyer and client information. We became somewhat comfortable with retrieving and reviewing electronically stored information (ESI) from computer memories. But next we had to face the challenges the universe of ESI on mobile devices such as phones and tablets present. Even a mobile phone with limited memory might contain data of 800,000 document pages.

If that weren't enough to get our arms around, we next faced text messages whose proliferation exceeded all knowledgeable projections. Simple text communications morphed into Twitter, WhatsApp, Facebook Messenger and Instagram. When we thought we understood those challenges, we ran into the issues raised by social media and cloud-stored applications and data. We learned to look for relevant evidence in Facebook accounts and on newer messaging apps such as Snapchat.

Now, we see frequent warnings about the Internet of Things (IoT), the "things" that are somehow connected to the internet, exchanging and communicating information. In a recent survey, only a small percentage of attorneys acknowledged having heard of the IoT, and few had confronted the challenges of IoT data as relevant evidence. Most of that early experience and gained knowledge seems related to wearable fitness devices, baby cameras, and smart thermostats and doorbells.

Basically, the IoT describes a universe of devices connected in one way or another over the internet while collecting and transferring information from one place to another. Technically, the things on the internet are physical devices with sensors that give an information system the ability to collect, communicate and process data. Residential applications include those baby cameras, smart thermostats, electrical controls, smart doorbells and other similar devices.

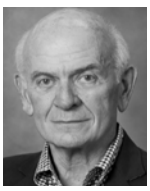
6.4 billion connective "things" will be in use worldwide this year, up 30 percent from 2015.

Automobiles are full of "things" that transfer information to security firms, manufacturers and mechanics investigating repair issues. Cars have multiple computers connected together through a maze of networks. Other IoT applications include GPS chips that inform the movements of runners, the location of containers, the defensive skills of baseball players and the location of almost anything allowing a GPS attachment. Medical devices constantly transfer information to physicians and drug companies that allows them to monitor medical conditions and the functioning of therapies.

Don't think there are only a few sources of IoT information. Gartner, Inc. has forecasted that 6.4 billion connective "things" will be in use worldwide this year, up 30 percent from 2015. And Gartner predicts there will probably be 21 billion by 2020.

This proliferation of IoT devices compounds an attorney's responsibility to preserve, collect, harvest and review ESI to determine what's relevant and should be produced upon request during litigation. An attorney's own devices and movements may present additional security issues if any "thing" lacks front-end security. That absence might allow hackers and curious visitors to enter through the back door and access an otherwise secure network to obtain client and attorney confidential information. The reports of Ukrainian hackers terrifying children through access to their baby cams — often unguarded by password protection — provide a simple analogue for the security weaknesses potentially inherent in the Internet of Things. A baby cam has an IP address but probably connects to the internet through the residential Wi-Fi network. If the hacker can access the camera, what other devices are on that network without additional firewall or password protection?

Few, maybe none, of us has enough experience with these devices or things to understand completely their impact on our duty of confidentiality, or the issues they present when we have to address preservation or production of thing-collected data, or their use as evidence. We can only pay attention to developments, try to stay alert and informed, and seek necessary assistance when we confront them.



Bill Kammer (wkammer@swsslaw.com) is a partner with Solomon Ward Seidenwurm & Smith, LLP.