Living Spaces

Is your smart home friend or foe when litigation starts?

BY **JESSICA HOFFMANN**

Technology is so prevalent that it has started being used in ways the developers did not envision. Google Earth, launched in the early 2000s, captures all angles of a mapped street. An article published in *People* in October 2018 described a situation in which a man, searching for tourist destinations via Google Earth, caught his wife with another man and filed for divorce.

Smart home electronics such as Amazon Echo, Google Home, Nest thermostats, Ring video doorbells, and Sonos sound systems can all be controlled remotely and may keep records of usage, including audio and video recordings. These devices are already having an impact in the legal world in crime prevention and investigation. We all remember the FBI requesting Apple to grant access to the iPhone of the San Bernardino shooter. In another instance, a murder investigation in Arkansas led police to request records of what the suspect's Amazon Echo may have recorded. Amazon refused to release the records but the suspect eventually agreed to allow access. The prosecution eventually dismissed the case indicating there was more than one reasonable explanation for the death.

Unfortunately, these devices are also being used to perpetrate crimes. In New York, a number of domestic abuse cases have been carried out using smart home devices. In these cases, the abuser uses access to the devices as a mechanism of control. They can control lights, temperature, music, and television access. This can also spill over into family law cases where one spouse remains in the home during the pendency of the case. A family lawyer in Houston is dealing with a case in which one party has been using access to the smart home to turn lights on and off in the middle of the night to intimidate and intrude on the other party who remains in the home. In a case in Denton County, a video doorbell system was used to prove that one party was entering the home in violation of a restraining order.

In certain instances, installing these devices secretly is illegal, for example, installing spyware on someone's phone or secretly recording a conversation to which you are not a party. However, in Texas, video recordings that do not have corresponding audio do not require consent of the parties depending on the location of the camera.

Whether you practice criminal law, family law, or want to understand how to best protect yourself and your clients when using these new technologies, here are some good tips to consider, because Alexa is listening.

1. Change the wireless password in your home periodically. Most of these devices are controlled and connected through the wireless network. Do not use something easily guessed; I recommend using a passphrase instead. For example, when my kids were into Harry Potter, my password variations would be something like "V0ldemort!" Include capitalized letters, numbers, and special characters.
2. Similarly, change account credentials for all in-home devices. Lights, music, pools, thermostat controls, video, smart locks, and doorbell systems can all alert others to your presence. Be sure only those who need access have it.
3. Include smart home devices as part of discovery requests and be sure to include injunctive relief related to them if applicable (i.e., require a party to stop accessing these devices if no longer living in the home).
4. Separate your Apple user ID from that of your (ex) spouse *and* your children. If your accounts are linked, apps you download or photos you take on your device may get downloaded through the cloud onto your children's devices and be in plain sight of anyone who has the device.
5. Be aware of and consider disabling device tracking like Find My iPhone, Life360, or Snap Map, a feature of Snapchat that shows friends where you are and what you are doing. These can be helpful in certain situations like knowing where your teenagers are, but they can also show any friend through Snapchat where and when to find your child.
6. Be aware that video games can be used to communicate in a way that is subtle and difficult to monitor.
7. Separate your Netflix, Amazon, DIRECTV, and other accounts from your (ex) spouse. No one needs to know what you are watching. **TBJ**

JESSICA HOFFMANN
is the founder and CEO of Family Docket, a software application that helps family law attorneys and their clients automatically track and aggregate text messages, maintain expense reimbursement requests, and securely store and access documents. She is also a lawyer, former law firm COO, and currently serves as chief strategy officer of a large national law firm.