CSO

FEATURE

6 tips for smartphone privacy and security

Computer forensic expert Ronald Kaplan thinks you should stop using your smartphone if you want any semblance of privacy in today's digital world. But, if you insist on keeping yourself electronically tethered, here are some ways to minimize the privacy and security risks

By Ronald Kaplan

CSO | Feb 11, 2014 7:00 AM PT

In the digital world, things are getting worse rather than improving with regard to the populist quest for personal privacy and security. Our smartphones track wherever we go, what we say, who we say it to, our likes and dislikes, and when we are playing games instead of working. Our computers track and record the same types of information day in and day out.

[iOS vs. Android: Which is more secure?]

These are the types of information marketers, insurance companies and employers would love to know before engaging with us, which means the information has great value. This should be troubling to all who read it. You may not be capable locating this often buried information on your own device, but rest assured trained specialists certainly can.

This is the type of information lawyers used to only dream about. They use it to devour the credibility of their foe under testimony. The racist or sexist jokes, the email between you and someone you testified you don't know, the evidence that you could not be in two places at one time, transfer of assets you testified you did not have, bank transactions you denied having, and the list goes on and on.

[What's wrong with this picture? The NEW clean desk test]

Just get sued or arrested and you will find out how easy it is to get to this information. We are not talking about NSA snooping which we all recently learned is more prevalent, pervasive and comprehensive than anyone imagined. What we are talking about here falls under decades old standards for discovery in civil and criminal litigation which are very difficult, or impossible, to stifle. These electronic discovery standards are already well established in civil procedure and what is referred to as case law.

If this concerns you then all you can do to protect yourself from this invasion is to stop using that smartphone and that computer you currently use almost round the clock. Sure you will have to live without all the conveniences in banking, travel, photography, and entertainment but you will know your private information and personal habits and activities will much more likely remain private. It is a very personal choice of whether the benefits outweigh the drawbacks, however most people never contemplate the tradeoffs, they just slide into embracing their electronic devices and pursue every app or application that meets their fancy or needs.

[7 security mistakes people make with their mobile device]

Many technology users have already been bitten by the likes of malware, computer virus, snooping software, and keyboard captures. Some have had to absorb the loss of a hard drive as a result of these invasions. Recovery is frequently achieved only by replacing the afflicted media or the entire device and restoring from any backup they may have maintained.

Afflicted users usually move on to find themselves vulnerable to the same attacks, making only small insignificant behavioral changes to protect themselves against the losses and aggravations that they swore they would never let happen again just a few months earlier.

[Experts warn of Russian spying, hackers at Sochi Olympics]

If you have the discipline to avoid all the behaviors that put you and your devices at risk and you install all the software/hardware designed to protect your devices, you are still vulnerable to loss of security and personal privacy. Don't fool yourself into thinking that you will continue to clean up after yourself when you use your devices and securely delete the trail others leave. This is not only very difficult to achieve, but requires knowledge of the trail you leave behind. Such a trail can be created by the operating system and applications not only running on your devices, but also on servers and other devices outside your control.

Just ask yourself "how do I acquire and maintain the knowledge about these operating system and applications behaviors?" Recognize that technical knowledge and specialized tools are required just to begin to understand what is happening under the surface of your actions on your devices. Very few people are capable of completely containing the trail of their activities, but those that are usually do so by dedicating specific devices for specific activities and are diligent about not cross-contaminating their devices. That is to say, they don't actually maintain a procedure for eliminating all superfluous data, but instead they isolate the information from non-related information.

Clearly, this solves some of the privacy and security problems, but not all. It also requires purchase of hardware and software that would not likely be necessary for any other purpose other than to maintain the integrity of the data. Further, it still requires time and discipline to maintain.

[Location tracking turns your smartphone into your stalker]

We continually see new techniques designed to protect your information like fingerprint readers and other biometric devices, but they bring their own risks along with them. Are they really more secure than passwords? How do you feel about these protections now that Apple's fingerprint reader took less than a week to defeat? Now that it has been defeated, if you use it to protect your iPhone is it now more or less secure than a password? Even if were not defeated, would a security key that can't be changed be a good choice?

As computer forensic experts, we have had many cases where it was our charter to secure and examine e-data in search of "the smoking gun." While we rarely find "the smoking gun," we often find significant amounts of periphery information to support our client's case. This information has been invaluable to erode or destroy the credibility of those witnesses, or others who have produced facts, that are detrimental to our client.

Recommendations

- Make sure you continually ask yourself when using these devices, "Do I care if anyone knows this?" where "this" means where you are, what's in the photos, what I am searching for on Google, that I am watching a movie, that I am telling a joke, or a host of other information you are producing.
- Isolate your professional life from your personal life. While it is clearly more convenient for you to use a single device for dual purposes, realize that if you maintain the integrity of your devices you will be able to shield irrelevant and personal information from business interrogations. While this is not ideal, it is light years better that being questioned about the homophobic, sexist, or racist joke you sent to your brother last year.
- Keep some privileged or confidential information on your devices. While this will not likely keep your devices free from prying eyes, it will necessitate the need to implement more costly procedures in the examination of your devices which protect the integrity and character of your information.
- Control the number and location of backups. The existence and locations of backup media can often be discovered in an examination of a device. If these backups are discovered by a competent examiner, you will be forced to produce them.
- Don't try to fool the professionals by hiding or deleting information. Be aware that the courts have tools for punishing those who get caught. Since you likely have little idea of the operating characteristics of all the applications and the operating system running on your device, you are not capable of discreetly eliminating data from your device.
- Quit posting everything you do on social networking sites. Twitter, Facebook, Instagram, foursquare and the like are fun, but can prove dangerous to your privacy. If you do post information on social networking sites make certain you use the privacy settings so that you can limit who has access to your information on an ongoing basis and so you can demonstrate your desire for privacy to a court if it orders your information production. At least don't use your common identity (your first and last name) to catalogue your information.

Mr. Ronald Kaplan, MS, MBA is a partner at SICons, a management consulting and computer forensic expert witness firm in Los Angeles.

Insider: How a good CSO confronts inevitable bad news ❯