Is Your Internet Device Spying on You?

By Judge Herbert B. Dixon Jr.

It is not my intention by the title of this technology column to suggest that your smartphone or other Internet device has the virtue of artificial intelligence such that, on its own initiative, it may decide to spy on you. I am merely suggesting that others might have the ability to use your device to invade your privacy. Although I have written previously on similar subjects, two recent news reports inspired me to issue another warning about our vulnerability to digital hacking.

The first news report that caught my attention concerned a group of U.S. Congress members asking the House Oversight Committee to launch an investigation into President Donald Trump's use of an insecure smartphone to post his many Tweets.[1]

The second report concerned a publication by WikiLeaks of thousands of documents describing activities of the CIA (Yes! The Central Intelligence Agency) that involved hacking many types of digital products including iPhones, Android devices, Wi-Fi routers, smart televisions, and autonomous cars that provide driverless transportation.[2]

In the request to the House Oversight Committee, the Congress members expressed concern that the president was disregarding commonsense cybersecurity best practices and jeopardizing national security by regularly using an insecure, consumer-grade Android smartphone to post Tweets. They also requested an investigation as to whether the president was using the device to engage in other communications with the public. Reading between the lines, it is obvious to techies that several security issues might arise if the president is using an insecure device. There is the possibility that a hacker could eavesdrop on the president's official and personal discussions. Another possibility would be a hacker infecting the president's device with malware that may spread to other devices in the administration. Another concern would be the possibility of a hacker tracking the president's movements and whereabouts. In addition, there is the possibility of a hacker cloning or taking control of the president's device to post inappropriate Tweets. If a hacker took over the president's Twitter account or device, imagine the enormous mischief or repercussions that could result from a negative Tweet about a world leader (friendly or adversarial), major U.S. employer, or financial market if the public believed the Tweet originated from the U.S.A.'s commander-in-chief.

The WikiLeaks disclosure confirmed that the CIA could hack into, clone, or even take over someone's smartphone and transmit communications that appeared to originate from that smartphone or account. The WikiLeaks disclosure also revealed the CIA's ability to read messages supposedly protected by a VPN (Virtual Private Network) or encrypted by smartphone applications such as WhatsApp, Signal, Telegram, and Weibo. In addition, the disclosure revealed the CIA's ability to hack computer routers that provide a Wi-Fi signal for smartphones and other devices to access the Internet. The disclosed documents revealed research about hacking autonomous cars (also known as driverless cars), which led to speculation about the ability of a hacker to take control of an autonomous vehicle and possibly cause an untraceable accident that was either debilitating or fatal. Wow!

Initial news articles about the WikiLeaks

release of CIA documents gave the impression that the CIA had developed the capability to break the encryption that protected messages sent using those encryption apps; however, a close inspection of the documents did not reveal that capability. The documents suggested that, after hacking a device, the CIA could see the message in its original form before the encryption or after the message was unencrypted by the receiving device. Interestingly, there was no indication the CIA had developed the capability to break the encryption by these apps.

Previous technology columns by this author already have discussed the casual nature by which some folks use their personal digital devices to store information;[3] the concern about the president's use of an insecure smartphone combined with the WikiLeaks disclosure of CIA hacking secrets was enough to remind the most cautious among us of the need to be ever vigilant.

The WikiLeaks disclosure of the CIA materials revealed capabilities that would allow a serious hacker to activate the camera and microphone of a victim's smartphone or Smart TV; watch like a peeping Tom; and listen to the victim's conversations in his home, at his business, and with others around him, wherever that might be. These capabilities are beyond those of a mere amateur. However, the idea that someone out there in cyberspace has that capability is more than a scary notion. In addition, there are amateurs out there who would love to have these capabilities and will ask, "Is there an app for that?"

Do not think that only inattentive novices are the victims. Just look back to a previous technology column in this magazine, "Cybersecurity . . . How Important Is It?,"[4] that described the miserable experience of a prominent and highly respected technology blogger whose iPhone, iPad, and MacBook devices, as well as iCloud, Gmail, Google Voice, and Twitter accounts, were invaded and taken over by a malicious hacker.

So, you ask, what does one do to minimize the possibility of a privacy invasion by the numerous forms of hackers in the world? Great question! Here are a few suggestions.

Use Strong Passwords

Several of our previous technology columns have railed about the use of weak or convenient passwords such as "123456," "password," and others that are based on known information about the user, e.g., children and pet names, street address, etc.[5] A strong password is still a very good safety practice for protecting your digitally stored information. Generally, a long password is safer, but you also should use upper- and lowercase letters, numbers, and symbols. Perhaps you should consider a password keeper that has the capability to generate strong passwords and store them for you. However, be careful! The password to access your password keeper should be very strong, and if you forget it, you will not have access to passwords for your various accounts. I know because it happened to me once. Also, if possible, the passcode you set to access your device should be at least eight to ten digits. Using the "no passcode" or "simple passcode" option merely increases your vulnerability to hackers or a person who finds your lost device or simply steals it. For these and other obvious reasons, always enable the configuration option to delete all data on your device after someone makes multiple incorrect passcode attempts to access your data.

Enable Two-Factor Authentication

A chain is no stronger than its weakest link. For a mobile device, that conventional wisdom usually applies to the owner. Using two-factor authentication adds an extra layer of security for accessing your account information. Examples of two-factor authentication are instances where the account holder would first enter a known password, and then be required to enter a second passcode received via a text message or generated by a mobile device or app. Under these circumstances, the owner, hacker, or thief could not access the account without the authentication provided by the second factor. Many readers are familiar with the feature of two-factor authentication at online banking and financial websites and when remotely accessing office information technology systems from home. However, included among frequently visited websites that provide the option of two-factor authentication are Facebook, Yahoo, Instagram, Twitter, Dropbox, LinkedIn, Snapchat, Amazon, WhatsApp, Tumblr, and many others.[6]

Install Security, Operating System, and Firmware Updates

Most of us are familiar with automatic update notices for some smartphone and tablet operating systems and apps. However, manufacturers and vendors do not automatically send update notices for all smartphones, tablets, apps, and other hardware, especially Wi-Fi routers that are the gateway to the digital history and possessions of many families. One must actively search for some of these updates, but that does not diminish their importance. Manufacturers and vendors issue some updates to improve performance and fix ordinary bugs. In addition, they issue other updates to add new security features and fix recently discovered vulnerabilities. These updates are frequently described as software updates, security fixes, and firmware updates, as well as by other names. Although owners of older devices are sometimes reluctant to install updates because performance of the device may degenerate, the trade-off is not benefiting from the repair of a recently discovered security flaw through which knowledgeable hackers might gain access to your device.

Judge Herbert B. Dixon Jr. is the technology columnist for *The Judges' Journal*, a member of the ABA Board of Governors, and a former chair of the National Conference of State Trial Judges. He sits on the Superior Court of the District of Columbia. He can be reached at Herbert.Dixon@dcsc.gov. Follow Judge Dixon on Twitter@Jhbdixon.

Encrypt Your Stored Data

Encrypting stored data is a nuisance to most users of Internet devices. That is an understandable reaction. However, the suggestion is worthy of consideration if the data you are storing are highly confidential or very sensitive. It is not necessary to encrypt your entire library of stored data. You should consider encrypting those files that are sensitive or might embarrass you if they became public.

Exercise Caution Before You Click the Link

This takes more restraint than you might realize. No longer are you merely watching for links in an email from a European Lottery official or the estate of a Nigerian prince advising you of your recent winnings or inheritance, financial and medical institutions are using secure links on the theory they are protecting you. It is up to you to figure out which is the malicious link and which was set up for your protection. As an example, I wrote one of my financial institutions this year asking for the name of a contact with whom to discuss my investments. When I did not receive a response within a reasonable time, I wrote again—this time to the customer service unit, a vice president, and several other officials within the institution. I later learned that the institution had sent a secure email to me through another vendor, which I ignored because I did not recognize the sender. Finally, I complained about the ridiculousness of the financial institution's protocol to send financial balances and account information by regular email, but resorting to secure email through a third-party vendor to provide me with the name and telephone number of a financial advisor. Go figure!

Don't Post Your Cell Number on Social Media Sites

Some successful hacks occur because a perpetrator was able to obtain the victim's cell number from a social media site. Occasionally, a cell number provides one more bit of information to facilitate a successful hack by allowing the perpetrator to give a correct answer to a request for information about you. The perpetrator knowing your cell number may have just enough additional information about you to defeat the security of a password reset request.

Use a Camera Cover

I thought it was funny the first time I saw digital natives with a Band-Aid® or other similar products to cover the camera lens of their device. I later learned these folks knew of instances when a hacker took over a victim's Internet device to spy on the victim. Now, some techies are using camera cases, cardboard, aluminum foil, and other materials to cover the camera lens at strategic times.

Your Smart TV

If you are concerned about your Smart TV spying on you, there are two options, which are not mutually exclusive. Check your owner's manual for any instructions to access and install the most recent software, firmware, and security updates; or disconnect the Smart TV from the Internet, either permanently or at suspicious times.

Conclusion

This is not really a conclusion but a few final thoughts. If the suggestions throughout this technology column are overwhelming or too difficult to implement, consider confining your communications activities to writing letters and sending them in sealed envelopes or using a landline to make telephone calls and send faxes. At least you will have the psychological comfort of knowing that anyone breaching these methods of communication mostly likely had a warrant based on probable cause issued by a court of competent jurisdiction—unless, that is, you regularly communicate with a foreign government or someone else who is the subject of surveillance. ■

Endnotes

1. David Z. Morris, *Congressman Calls for Investigation of Trump's Insecure Phone*, Fortune (Feb. 18, 2017), http://fortune.com/2017/02/18/trump-android-phone-ted-lieu.

2. Brian X. Chen, *With Claims of C.I.A. Hacking, How to Protect Your Devices*, N.Y. Times (Mar. 8, 2017) https://www.nytimes.com/2017/03/08/technology/personaltech/defense-against-cia-hacking.html?_r=1.

3. Herbert B. Dixon, *#AI, #VR, and #IoT Are Coming to a Courthouse Near You!*, 55 Judges' J., no. 4, Fall 2016; Herbert B. Dixon, *Technology and the Courts: A Futurist View*, 52 Judges' J., no. 3, Summer 2013; Herbert B. Dixon, *Cybersecurity . . . How Important Is It?*, 51 Judges' J., no. 4, Fall 2012.

4. Dixon, *Cybersecurity*, *supra* note 3.

5. Herbert B. Dixon, *The End of Privacy as We Know It?*, 54 Judges' J., no. 2, Spring 2015; Herbert B. Dixon, *Technological Advancements Coexisting with Tech Stagnation*, 54 Judges' J., no. 1, Winter 2015; Herbert B. Dixon, *Worst Passwords of 2013*, 53 Judges' J., no. 2, Spring 2014.

6. For more information about two-factor authentication, see Eric Griffith, *Two-Factor Authentication: Who Has It and How to Set It Up*, PC Mag. (Mar. 10, 2017), http://www.pcmag.com/article2/0,2817,2456400,00.asp; and Jason Cipriani & Dennis O'Reilly, *How to Enable Two-Factor Authentication on Popular Sites*, cnet.com (Aug. 6, 2014), https://www.cnet.com/how-to/how-to-enable-two-factor-authentication-on-popular-sites.