FIVE WAYS TO PROTECT AGAINST CELL PHONE SPYING

Our cell phones can store our most private information -- from our emails, texts and photos to our bank account, job and health records. They can track where we go and who we meet. Unfortunately, this makes our cell phones a target for unwanted spying, whether by the government or private parties seeking to abuse and misuse the information. Here are some tips to better protect all the information stored on your phone:

1 INSTALL SOFTWARE UPDATES

One of the easiest ways to put your phone at risk is by neglecting to install software updates. When phone app designers discover security flaws, they often send out updates that fix the problem. That's why it is important to keep all of the software on your devices as up-to-date as possible.

2 PROTECT YOUR PASSWORD

Short passwords, simple passwords or the same passwords for multiple accounts put your information at great risk. Use a password manager to generate better passwords for your accounts.

LastPass (https://www.lastpass.com/) is a free password manager that is accessible on all platforms.

3 ENCRYPT YOUR MESSAGES

Encryption is a method of turning data into code so people you don't want to see it cannot read it. A text message that is not encrypted can be read by anyone who intercepts it. But there are message apps that will encrypt your text messages so they can ONLY be read by the person you send them to.

Signal (https://whispersystems.org/) is a free and easy-to-use app you can download for secure text messaging and phone calls. You can use your existing number and address book, so there are no separate logins, usernames, passwords or PINs to manage or lose.

4 AVOID SEARCH ENGINES THAT TRACK YOU

Many of the major search engines store all of the search terms you use as well as other information from your device. Use search engines that do not track your activities and information.

Disconnect (https://disconnect.me/) is an internet browser and search engine that keeps your data and identity private.

DuckDuckGo (https://duckduckgo.com/) does not store personal information, track you or target you with ads.

5 PUBLIC WI-FI IS NOT SAFE – SO BE CAUTIOUS

Your information can be unsafe on public wi-fi. Make sure your phone is not set to automatically connect to public networks. If you do have to use public wi-fi, remember that social media, online shopping or banking and other websites require you to input private information, and consider accessing those through your cell phone network instead of the public wi-fi.

NYCLU
NEW YORK CIVIL LIBERTIES UNION

Date: 02/07/2017
Disclaimer: The NYCLU does not endorse any particular services or products, including the ones listed above -- remember that cell phone apps and technology can change rapidly!