FIVE WAYS TO PROTECT AGAINST CELL PHONE SPYING

KNOW YOUR RIGHTS

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 about you and the people you are in touch with:

1. MAINTAIN GOOD PHONE HYGIENE

One of the easiest ways to put your phone at risk is by neglecting to install software updates. Security vulnerabilities and bugs are frequently discovered, so keeping all of the software on your devices up-to-date fixes these problems.

Only install apps you trust and delete the ones you no longer use. Be conscientious with your phone's sensors, such as GPS, WiFi, and bluetooth: turn them on when needed and keep them off at all other times to avoid surreptitious data collection and tracking. Consider turning your phone off when you are attending a protest.

2. PROTECT YOUR PASSWORD

To unlock your phone, use a passcode, not a biometric method such as your fingerprint or your face. Short passwords, simple passwords or the same passwords for multiple accounts put your information at great risk. Instead, use long passphrases or a password manager to generate more complex passwords for your accounts.

- KeePassXC and LastPass are free password managers that are accessible on all platforms.

3. ENCRYPT YOUR COMMUNICATIONS & TRAFFIC

Encryption ensures that your data can only be accessed and read by the people you want to communicate with. Any communication or web traffic that is not encrypted can be read by anyone who intercepts it. Thankfully, there are message apps and browsers that will encrypt your data so they can only be read by the party you send them to.

- Signal is a free and easy-to-use app for secure messaging, phone, and video calls.
- Tor Browser is a free internet browser that will encrypt your web traffic anonymously through its network and protect you against surveillance, tracking, or censorship.

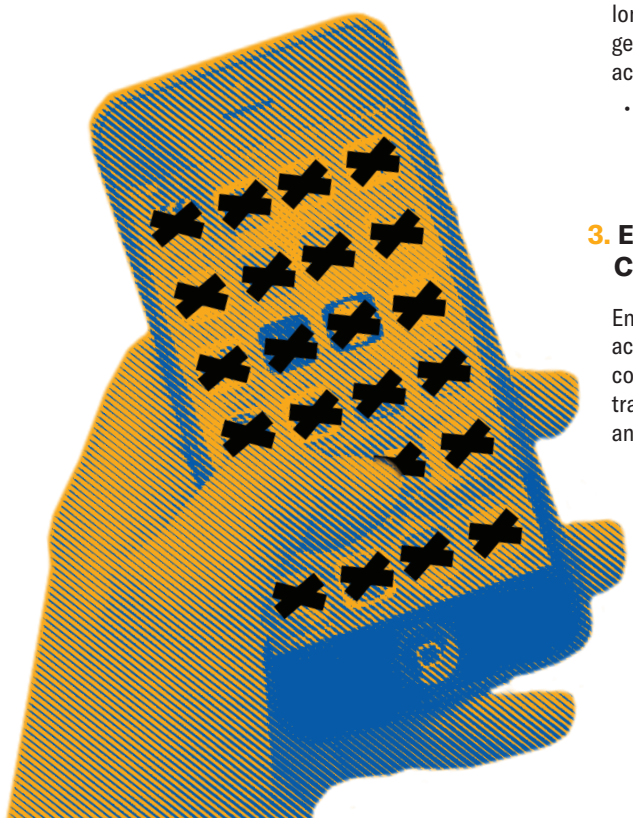
4. AVOID SEARCH ENGINES THAT TRACK YOU

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.

- DuckDuckGo 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 your traffic could be collected and only enter sensitive information if the website uses a secure connection, indicated by the lock in the address bar.



Date: 10/22/2020

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.

NYCLU
ACLU of New York
www.nyclu.org