Your communication: Is it secret? Is it safe?

Intelligence services often have an unlimited, secret budget with which to purchase interception and surveillance equipment. They hide behind the secrecy requirements of "national security", never revealing their operations, expenditures, or technical capabilities. Journalists and activists have much to fear when it comes to having their communications intercepted. With spyware, it becomes even more difficult for journalists and activists to protect themselves. There are, however, several simple steps one can take to protect yourself. Here, we discuss a few, although the list is by no means exhaustive.

Basic protections

- Use a virtual private network (VPN) on your smartphone and computer. This hides your IP address, making you less easy to trace, and it also encrypts your communications. You can opt for a free resource like Tor and Onion, but if you're not a techie, it's easier to just get a paid service.
- Get anti-virus software, even if it's a free version (anything is better than nothing)
- Make sure your computer's firewall is on
- Change all your passwords often, especially for email and social media accounts that you use to communicate

Sharing, storing and recording

- Choose a more private and secure messenger service (NOT WhatsApp). Signal is better. It's also free.
- Use a secure email service, like ProtonMail. Better yet, learn how to use OpenPGP to encrypt your emails (see https://www.openpgp.org).
- Don't share sensitive stuff with Google Drive, Dropbox, or WeTransfer. ProtonMail also offers a secure drive/file-sharing option.
- Store the really important, sensitive stuff OFFLINE, and keep it offline.
- Don't record conversations with your phone - use a separate recorder. Don't plug that recorder into your online computer. Always keep it offline, and don't listen to it out loud when you're close to your computer or smartphone.

Talking

- NEVER use a landline.
- If you must use a phone, remember that when you register a sim card in your name, security services will know it's your phone, and will be able to pull your call records and target your phone for monitoring.
- Always try to meet your source in person (not at/in their house or car, nor your house or car - intelligence services may have planted bugs). Meet at a random, neutral location, preferably somewhere noisy, like a restaurant or a park with lots of passing traffic. DO NOT TAKE YOUR PHONE WITH YOU. Either leave it at home, or in the car.
- DON'T USE GPS when travelling to meet your source. Put your phone in airplane mode. It doesn't mean that you can't be tracked, but it can make it a bit harder. If you can, best leave your phone at home.
- Meet your source at a prearranged meeting point, and go from there to a new meeting point that you decide on together.