English

Police surveillance : protect yourself from your phone and Whatsapp!

At the French-British border, as elsewhere, there are numerous indications that the French police are remotely monitoring the content of the Whatsapp communications of many people, particularly those they suspect of wanting to cross the border clandestinely.

Numerous investigations are underway at the French-British border to arrest "smugglers". The authorities' definition of the word "smuggler" is highly controversial : it is illegal to help someone cross the border clandestinely, even for free, and the police arrest many people for this. Because of this, some people are sent to prison and sometimes deported from France afterwards.

During a police investigation in France, **it's easy for the police to monitor telephone conversations** just by knowing the telephone number they want to monitor. They do not need to physically access someone's phone. The phone can be monitored for several months by the police without the person being monitored knowing it. If the police are monitoring you, they can listen to your telephone conversations and read your text messages.

Even if you are not being monitored, certain information is still kept for at least 2 years by your operator and the police could consult it later : **the geolocation of your phone even if the GPS option was off**, with which numbers you exchanged text messages and calls, how long the calls lasted, as well as details of the exact days and times of each text message, call and geolocation. Your phone's geolocation can be used by the police to find you in real time so they can arrest you, or in court to prove that you were somewhere at a particular time. The history of your text messages and calls, even if the police do not have access to the content, can be used to find out who you are in contact with and when.

The police have plenty of ways of finding out your phone number :

- By asking the phone or credit shop.
- If they arrest you with your phone.
- If they find your phone number in someone else's phone after an arrest or surveillance.
- By searching all the phones that were in a specific place at a specific time. For example, to identify people trying to cross the sea illegally : all phones detected at 2 AM on a french beach near England.
- By installing an interception device. For example, a plain-clothes policeman could hide a small antenna in his backpack and walk past you; he would then be able to see your number if your phone was switched on. It can also work at a distance of several dozen metres with a larger device, which police officers can hide in a vehicle.

As practical as they are, **our phones are true spies for the police!**

To prevent your phone from being geolocated, the only solution is to put it in airplane mode, or ideally to switch it off and remove the battery. As soon as the phone is switched on, even if the GPS is off, it bounds on the network, which records its location. To make it harder to monitor your messages and calls, it's best to use internet messaging systems with end-to-end encryption, so that the communication is only visible to you and the people you're talking to.

Whatsapp is an online messaging app owned by the US company Meta, which also owns Facebook, Messenger and Instagram. The company claims to use end-to-end encryption for its messaging, so no one can intercept a call or message apart from the person sending it and the person receiving it. But Whatsapp's security protocol is kept secret because the company refuses to reveal it. So it's not possible to know whether there are any loopholes in Whatsapp's security that the police can use to monitor users. **There are many indications that in some investigations, the police are able to listen to Whatsapp messages and calls**. On its website, Whatsapp state that they working with the authorities to monitor its users.

An alternative way of protecting yourself is to use the Signal app. It's easy to use and very similar to Whatsapp. But Signal's security protocol is open-source : it is accessible to everyone and anyone can check that there are no loopholes that would allow the police or other malicious people to intercept communications. Thousands of computer scientists around the world monitor and improve Signal's security every day, in complete transparency. This is not to say that Signal is infallible, but there are more reasons to trust it than Whatsapp. What's more, Signal is a not-for-profit company, whereas Whatsapp makes money by collecting and reselling its users' data, which is one more reason to choose Signal over Whatsapp !

Installing Signal is simple: just download "Signal Private Messenger" onto your smartphone:

- On Android devices, in the GooglePlay application.
- On iPhone or iPad, in the AppStore application.

Once the application is installed, all you have to do is create an account with a validation code sent by text message. Security tip: when you create your profile, use a pseudonym rather than your real name. Once your account is created, you'll be able to communicate with all your contacts who also use Signal : text messages, voice messages, photos, videos, calls, group conversations, etc. It only works with people who also have Signal installed on their phone, so invite your friends and family to install it too so you can communicate together more securely.

Just be careful! If one day the police stop you with your phone, it is possible that they will open it and read your Signal messages, even if you have set a code. If they arrest someone you're in contact with, they can read the messages you've sent them in the same way. So remember to delete your messages regularly. In the Signal settings, you can set the "disappearing messages" option to automatically delete messages after a certain period of time.

Let's fight against surveillance! Privacy is a human right!