UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

OHCHR digital security tips series for human rights defenders in South-East Asia

1 Identifying sensitive information

Human rights defenders (HRDs) should observe the principle of "do no harm" at all times while performing their duties online and offline. In practical terms, this principle of "do no harm" means that your actions or inactions should not jeopardize the safety of victims, witnesses, or other sources contacted. When engaging with sources, your use of technology should take into account context-specific risks, both your context and that of the source. These risks are linked to the surveillance technologies in use, surveillance legislation, capabilities of cyber threat actors, data localization laws, and the history of attacks against and other forms of repression of human rights defenders. You may need to seek specialist advice on these matters.

The term "sensitive information" includes (not an exhaustive list):

- Personal information belonging or relating to HRDs, civil society organizations, journalists, and lawyers, such as geographical location, photographs, emails, nicknames, family names, date of birth and other personal identifiers e.g., passport/ID numbers.
- Information related to the work done by HRDs or civil society organizations. The sensitivity level of such information must be evaluated on a case-by-case basis considering the political, economic, and social contexts i.e., political regime, religious customs, etc.
- Information gathered during monitoring, investigations, conversations, and interviews, witness statements and recordings. The sensitivity of such information must be evaluated on a case-by-case basis considering political, economic, and social contexts i.e., political regime, religious customs, etc.
- Information contained in organizational plans, budgets, projects, and activity implementation.
- Information can be contained in documents, photos, videos, emails, audio recordings and/or other digital media formats.
- All digital media formats contain two types of data: content data and meta-data. For example, the data contained in a photo is the image, and the meta-data is the date, time stamp and geographical location.
- In certain circumstances, information about travel plans within the country or to another country, places visited, or websites visited may also be considered sensitive and should be protected i.e., if you are travelling for a meeting with a source, make sure you do not leave a digital trace of this meeting if this can put the person at risk.

If meeting with particularly sensitive sources, and you worry about your phone being under surveillance, one recommendation would be to place your phone in a Radio Frequency Identification (RFID) blocker[1] or Faraday bag.[2] If you do not have such tools at hand, you may also put your phone inside the microwave (do not turn the microwave on!) or fridge.

Note: References to external entities and websites are only indicative and should not be considered an OHCHR's endorsement to such entities and websites and the services provided by them. These references are provided, without warranty of any kind, either express or implied, including, without limitation, warranties of merchantability, fitness for a particular purpose and non-infringement. Under no circumstances shall OHCHR be liable for any loss, damage, liability or expense incurred or suffered that is claimed to have resulted from the use of these websites. The use of these websites is at the user's sole risk. The external websites are not under the control of OHCHR, and OHCHR is not responsible for their content or any link contained in these sites.

[1] RFI blocking wallets block RFID signals using electromagnetic enclosure technology called a Faraday cage.

[2] A Faraday bag is designed to shield a mobile phone or small digital device from radio waves entering the bag and reaching the device, or to stop radio waves escaping through the bag from the device. (https://faradaybag.com)(we usually don't include reference to commercial websites, related to the purchase of devices)