Choose your phone with care:

- ☐ Inform yourself about different operating systems and their compatibility with key security apps.
- ☐ Removable batteries make it possible to really switch your phone off.
- ☐ Phones where the baseband (mobile phone provider) and CPU (your phone's computer) are separate offer more privacy.

Check your settings and change where needed:

- ☐ Location, Contacts, Photos, Camera, and Mic.
- ☐ Password: Create a strong password to protect your phone.
- ☐ Encryption: If the phone is not encrypted by default, encrypt it.
- ☐ Set up a SIM-card lock.
- ☐ Disable USB debugging so your data can't be copied without your permission.

- ☐ Use a VPN.
- ☐ Use Orbot to connect to the Tor anonymity network.

- ☐ Use a secure messaging app like Signal or Chatsecure.
- ☐ Install a privacy-enhancing browser like Orfox or DuckDuckGo.
- ☐ Regularly delete your Wi-Fi history.
- ☐ Turn off Bluetooth/NFC when not in use.
- ☐ Install a free anti-virus, Avira or Avast, which can catch known malware, detect phone location and remotely wipe data if your phone is stolen or lost.

MAINTAIN

- ☐ Regularly check app permissions.
- ☐ Delete unused apps.
- ☐ Make regular backups of your data and clean your phone.
- ☐ Sometimes leave your phone at home, to break behavioural (and therefore data) patterns.
- ☐ Be aware of spam and viruses - don't click on random links.
- ☐ Enable the 'opt out of interest-based ads' option in your Google account, and tap Reset Advertising ID (Google settings > Services > Ads)
- ☐ Disable location tracking. (Note that this will prevent you from using the GPS in Maps) (Google settings > Services > Location)
- ☐ Disable and delete your Google location history (Google Settings > Services > Location > Google Location History)