Prepared by AB for DC-DDHT Toolkit
EuroDig Session Discussions 2022

DC-DDHT Privacy Pack: Required steps to improve digital privacy:

- Encrypted messaging apps (to be used on phones and other digital devices): **Signal** (available for iOS and Android). Alternatively **ChatCrypt** is an "end-to-end encrypted group chat that doesn't store anything in the cloud".
- Encrypted email services: **Protonmail**; **Hushmail**. Emails can also be encrypted on services such as **Microsoft Outlook**.
- Data can be encrypted and authenticated using services such as **OpenPGP**, which uses public key cryptography.
- **Silent Circle**: "the world's solution to mobile privacy", providing "a variety of voice, text, video, and file transfer encryption packages for individuals and business users."
- Computer operating system (hard disk)-specific encryption: guides available to encrypting disks on **Windows**, **Mac OS X**, and **Linux**.
- Password managers (creating and securely storing unique, unbreakable passwords): **KeePassX** is free, open-source, cross-platform and does not store information in the cloud.
- Two-factor authentication: if a password is stolen, two-factor authentication provides an additional layer of protection: **DuoMobile**; **Jumbo.**
- Encrypted search engines: **Tor Project.**
- Google Docs alternative: **CryptPad**.
- Drop Box alternative: **SpiderOak**
- **HTTPS Everywhere** is a Firefox, Chrome, and Opera encrypted browser extension that provides secure communications with a large number of major sites.
- **Qubes** is an operating system that isolates programs in their own VM (virtual machine).
    - "In our digital lives… All of our activities typically happen on a single device. This causes us to worry about whether it's safe to click on a link or install an app, since being hacked imperils our entire digital existence… Qubes eliminates this concern by allowing us to divide a device into many compartments."
- **Privacy International** provides services designed to protect users from online tracking (covering **Firefox**, **Chrome**, **Edge**, **Safari**, **Android** and more). P.I. also offers advice to users, regarding collecting their data from apps (including Twitter, Facebook, WhatApp, Uber), and minimize targeted ads when using social media.
    - **Ghostery** is a popular 'browser plug in', which adds an extra layer of protection for browsers such as Chrome, Opera, Firefox, Safari, and mobile systems such as Android, iOS and Firefox Android.
- When phones, laptops and other digital devices are not in use, disable Wifi, Bluetooth, GPS and NFC (near-field communication). Only connect devices to trusted internet connections.
- **HaveIBeenPWNED?** Useful service to check if email accounts or phone numbers have been subjected to data breaches
- VPNs (virtual private networks), such as **Surfshark VPN** or **ExpressVPN**, create protected network connections when using public networks.
- More manual steps involve placing covers over cameras on digital devices.