EXPLORE

You are tracked through your browser in two main ways: third party trackers (cookies etc), which are embedded in most websites; and through your unique browser fingerprint.

- □ See which third party trackers are monitoring your online activity, using Lightbeam (Firefox).
- □ Test the uniqueness of your browser, using Panopticlick.

CHANGE

Use multiple browsers (Firefox, Chrome, Safari) for different purposes. This makes it a little harder to track you.

Consider using the Tor Browser Bundle for increased online anonymity. Please check the legality of using Tor in your country.

CONTROL

- □ Choose a search engine that does not track and profile you (DuckDuckGo, startpage, Ixquick or Searx).
- □ Block pop-up windows.
- □ Set your browser to auto-delete your history on closing.
- □ Don't save your passwords in your browser.

□ Restrict permissions for cookies.

□ Check the Do Not Track box, to send websites requests to disable their trackers.

□ Use Private Window (Firefox), or Incognito Mode (Chromium & Chrome).

ACCESSORISE

Install a few key privacy-enhancing add-ons/ extensions:

□ HTTPS Everywhere encrypts your communications with many major websites.

□ Privacy Badger stops advertisers and trackers from monitoring your online behaviour.

□ NoScript blocks banners and pop-up windows.

MAINTAIN

□ Regularly check for browser and add-on/ extension updates.

□ Keep your browser history lean and clean – clear it regularly.

□ Regularly delete cookies.

□ Regularly review your browser settings.

□ Log out from sites before you close your browser.