Terms of Reference
Consultant for producing 25 short technical guides to protect yourself from online tracking on a variety of devices and environments.

Background

Privacy International (PI) as produced research and advocacy on ad tech and data brokers over the past few years. Ranging from submitting complaints to data protection agencies to investigating tracking on mental health websites, this work explores data exploitation practices on the web and in apps, exposing techniques and key players while pushing for enforcement of the GDPR. PI's work on ad tech is part of the Corporate Exploitation programme, challenging companies that innovates on surveillance capitalism, exploiting people's data for profit and power.

Purpose of the Consultancy

PI is currently undertaking work to provide web users with practical advices on how to protect themselves from different existing tracking techniques. While no silver bullet exists, empowering users with a set of tools to limit to which extend they are being tracked both achieve a disruption of the online tracking economy while offering a better online experience. This work also builds on the lack of standards for consent and privacy choices, users being required to constantly opt-out and dig into lengthy privacy settings to refuse tracking and targeting.

The production of guides aims at giving users a large choice of actions they can take to minimise data collection, limit unwanted tracking, prevent identification and generally improve their online experience. They will serve as a way for our supporters, as well as any visitor, to express their dissatisfaction with the current ecosystem and practically oppose tracking and targeting. Guides will cover multiple environments and devices and have varying degrees of difficulty to satisfy all audiences. The defined format and the license under which they are distributed will make welcome contributions and make reproducibility easy.

The consultant will have a global understanding of the online tracking ecosystem including fingerprinting strategies, targeting techniques and more generally how the internet works. They will have a good knowledge of existing solution to limit online tracking and a broad technical understanding of their functioning. Ability to simplify and make easily understandable the different steps is required as well as knowledge of git and markdown for formatting and sharing.

Specific Tasks to be Performed by the Consultant

1) Writing and developing the 25 guides listed in Annex A in markdown format and with concise and clear language following the example in Annex B. Guides should include screenshots in English on the key pages and settings screens. The list is subject to change based on comments and feedbacks from the consultant;
2) Upload guides and attachment to Github following the nomenclature in Annex B;
3) Suggest and develop additional guides based on your experience and knowledge.

Outputs, Timelines, and Renumeration

25 guides based on the list defined in Annex A plus additional guides identified by the consultant and agreed on are to be delivered by 20 November 2020 (at the latest) as per a schedule of deliverables to be agreed between PI and the selected consultant. Guides should be uploaded to a Github repository provided by PI. All the screenshots and content mentioned should be free to publicly use without constraints.

The work expected is total and these are deliverables, the total fee to be awarded shall not exceed £2,000.

Please send your proposal at eliotb@privacyinternational.org with the subject "Proposal for guide consultancy" before October 30th.

Annex A – List of guides to write

Adblockers (7 guides)
On desktop
1. Install uBlock Origin on Firefox
2. Install uBlock Origin on Chrome (and derivates)
3. Install Privacy Badger on Firefox
4. Install Privacy Badger on Chrome (and derivates)

On mobile
5. Install 1Blocker X for iOS
6. Install Netguard and Blockada for VPN based solutions on Android
7. Install AdGuard on Android
8. Install AdAway on Android

Cookies clean-up (2 guides)
9. Install Cookie AutoDelete (including whitelisting) on Firefox
10. Install Cookie AutoDelete (including whitelisting) on Chrome (and derivates)

User Agent Spoofing/ Random user agents (2 guides)
11. Install Random User Agent or Chameleon (to the consultant discretion) extension on Firefox
12. Install Random User Agent or Chameleon (to the consultant discretion) extension on Chrome (and derivates)

CDN (2 guides)
13. Install Decentraleyes on Firefox
14. Install Decentraleyes on Chrome (and derivates)

DNS level Adblocker (5 guides)
15. Install and setup a DNS level adblocker on Windows (AdGuard or any alternative)
16. Install and setup a DNS level adblocker on Mac (AdGuard or any alternative)
17. Install and setup a DNS level adblocker on Linux (AdGuard or any alternative)
18. Install and setup a DNS level adblocker on iOS (AdGuard or any alternative)
19. Setup and run PI-hole on a Raspberry Pi

Browser Settings (if relevant given the current list – 4 guides) to limit tracking (includes DNT, policy on cookie retention, Search engine…)
20. Privacy friendly settings on Chrome
21. Privacy friendly settings on Firefox
22. Privacy friendly settings on Safari
23. Privacy friendly settings on Edge

OS settings (2 guides)
24. Reset Ad ID on iOS
25. Reset Ad ID on Android

Annex B – Example of a guide as hosted on github (Telegram apps settings)

Currently visible at: https://privacyinternational.org/node/3953/

Title
Telegram - App settings/permissions

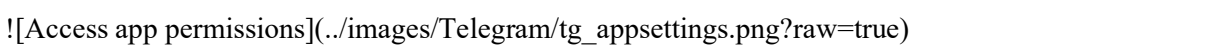
Summary
Telegram is an app running on your phone and as such may ask for permissions to access certain info such as location or contact. This guide shows you how to review these settings.

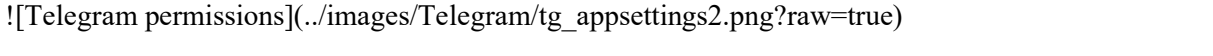
Body
Phone

The first time you use Telegram it will ask for permissions to use your phone. This is used for the verification process but shouldn't be used later on. However, if you don't change this permission, Telegram is theoretically able to make phone calls on your behalf. We recommend you check the app's permissions to disable anything you don't use within the app, such as permission to access phone calls or location. You will likely find this in your phone settings rather than the app.

To access permissions:
- Hold press on the Telegram icon
- Tap the "info" icon
- Tap permission

Alternatively:
- Go to your phone settings
- Look for permissions
- Find Telegram





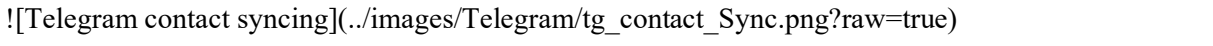
Contacts

Another thing Telegram will ask for is access to your contacts to find people using Telegram in your contact list. You may initially want to do this, but if you do that Telegram will keep a record of all the phone numbers in your contacts. If any of these people were to install Telegram in the future you would receive a notification and the person would know that you use Telegram. We recommend doing this only if you know and trust the contacts in your phone. If you refuse you will still be able to contact people using their handle or phone number. You also have the option to delete synced contacts from the app. This permission can be changed at any time in the settings of your phone!

Sync contacts

Following your decision above, you may not want to have your contacts and frequents contacts synced. This won't massively impact your user experience.

To access these settings:
- Open Telegram and tap the three bars on the top left corner
- Tap **Settings > Privacy and Security > Sync contacts**



App password

You may set a password per device to unlock the app. This password is only valid on a given device. If there are chances that your device be accessed while unlocked you might want to add this second security layer. Make sure you use a unique password different from your two steps verification password!

To access this setting:
- Open Telegram and tap the three bars on the top left corner
- Tap **Settings > Privacy and Security > App password**

What we do with your data

If you apply for a position at PI, your application is shared with relevant staff internally until you become a candidate for employment (or volunteering).

In the recruitment process, further data may be collected from you for the purposes of progressing your application, this will either be with your consent, because there is a legal requirement to obtain the information or because it is necessary for the purposes of entering into a contract. Where you are applying to be a volunteer, we will rely on our legitimate interest in processing your application and also your consent. This data may include biographical information, contact details, immigration-related information, references, and payment details for reimbursement purposes. This will only be shared on a need to know basis with relevant PI staff and our trustees.

For successful candidates, we will keep this data as long as necessary for the purpose of your employment or volunteer period with PI, otherwise we will securely delete your data 6-12 months after the end of the recruitment process.
We keep all accounting and administration information for auditing purposes, in accordance with standard practice and UK law.

For more information about how PI's personal data practices please see PI's Privacy Policy. The Privacy Policy includes information about your rights in relation to your personal data, including the right of access and your right to make a complaint to the data protection regulator, the ICO.