

User tracking



Inevitably using internet is linked to leaving behind some traces – information about ourselves. Some of it we leave consciously, for example when publishing information on social media profile, but some of it we leave without being aware of it. When visiting a website we are sharing our IP number and information about browser used (its version, operation system, language, fonts). This is information that can be used to track users. To check how few other people have the same settings as you, you can use [Panopticon.eff.org](https://panopticon.eff.org). The more unusual the settings are, the easier it is to identify and track you. Your activity can be tracked by using different tools, for example cookies – small text files which are saved on user's drive when using websites. On one hand, they allow websites to work properly, but on the other, they save browser settings (language, login details) or send some information back to the website servers (security settings, items in a basket).

Do you want to check how you are tracked? Install plug-in Lightbeam or Disconnect to see how other services, apart from the one you are currently using, collect data about you.

Activities

Watch a short film "[Monologue of the Algorithm – how Facebook turns users data into its profit](#)". Then try to find answers to 3 questions.

1. What information about users is collected?

Hints:

- information on our profiles
- information about what we like
- IP address
- wifi network
- connected devices
- clicks on websites (also reactions to our activity)
- social network
- geolocation
- correlations and behaviour patterns
- information about important life events (wedding, child birth, graduation)
- browser history
- time of logging in
- comments, chats

2. Why is this data collected?

Hints:

- tracking
- predicting unpredictable
- suggestions what is important and attention worth
- internet mapping
- how much we are willing to spend on a given product
- identifying political, social and marketing preferences
- matching messages to user's profile

3. What can we do? Is it possible to avoid tracking completely?

It doesn't seem to be possible to completely avoid tracking – it would mean stopping using the internet. Which is not the way we want to go. However, we can limit the power of algorithms by:

- logging out from social media sites, when we don't use them
- deleting cookies regularly, because even when logged out from a service, its cookies can still collect data and link it when we log in again
- installing useful plug-ins, e.g. Adblock Plus (blocks advertising), Ghostery (blocks certain), HTTPS Everywhere (automatically turns on safe HTTPS protocols, where possible) and Facebook Container (protects you from tracking through Facebook when using the internet)

Based on: Urszula Dobrzańska, Weronika Paszewska, Wojciech Budzisz, Michał "rysiek" Woźniak, Kamil Śliwowski „Kto nas śledzi w sieci?” <http://edukacjamedialna.edu.pl/lekcje/kto-nas-sledzi-w-sieci/>, CC BY-SA

Fot. CC0, [pxhere](#)

The publication was created as part of the project [EMELS](#)

Co-funded by the
Erasmus+ Programme
of the European Union



This publication reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Information about the resource

Publisher: Modern Poland Foundation as part of EMELS project co-funded by the Erasmus+ Programme of the European Union.

Rights: Creative Commons Attribution – Share Alike

This resource is attached to the European Media Literacy Standard for Youth Workers. To find out more about the Standard go to <http://emels.eu>

Resource prepared using [MIL/PEER](#) editing platform.

Source available at <http://milpeer.eu/documents/358/>