

Don't Spy On Us EU - Summer 2023 - Action plan

(Last updated August 29, 2023)

Contents

Don't Spy EU – the campaign.....	1
Website.....	2
Activism: involvement & future events.....	3
The whistleblowing initiative: "Sinkhole".....	4
Optional & additional activities.....	5
Timeline.....	6

Don't Spy EU – the campaign

March-May. Italian NGOs [Hermes Center](#), [The Good Lobby Italia](#) and [info.nodes](#) started the Don't Spy EU campaign in March 2023, with the launch of its website [dontspyonus.eu](#).

As representatives for these organizations, our main objective was and still remains that of providing educational tools, so that people understand the threats posed by biometric surveillance systems and the implications of other non-biometric surveillance AI devices.

The early phase of the campaign was about encouraging the general public to challenge pro-surveillance politicians involved in the AI Act trilogues. On the Don't Spy EU website ([old version](#)), users could "scan" the faces of MEPs through a facial recognition algorithm, as well as generate *deepfakes* and participate in *metadata enrichment* contests.

The main goal was to demonstrate how, by using technology available on the market (such as [this one](#)), public institutions and private companies can access sensitive information about citizens (age, gender, even "emotional state") and use it as they please - should RBI ever become legal.

In addition to that, we kept creating and posting content on our online platforms and social media channels. Don't Spy EU was also featured in [Wired Italia](#) (May 2023).

June-August. This initial phase, however, came to an end with the vote of the European Parliament on June 14, 2023. In the past couple of months, members of our three organizations have been meeting on a regular basis to ensure that the main goals of our campaign are met through efficient communication and planning.

The present document details the campaign-related activities planned for August - December.

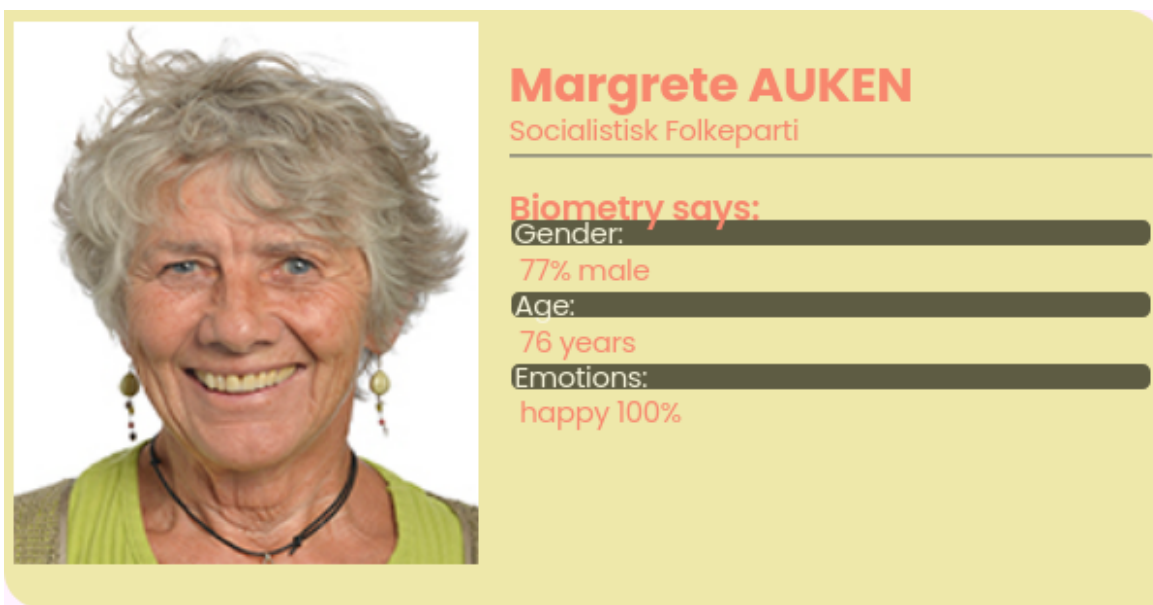
Website

As the third phase of the trilogues approaches, **we have quit the old domain dontspyonus.eu and launched <https://dontspy.eu>. The website will now focus on the last phase of the trilogue, addressing the entire Council of Europe.** The old version only featured MEPs that were involved in the first and second phase, whereas our goal is to include the Ministers who are going to take part in this third phase starting next September.

The website will feature technology designed to make users - from all backgrounds - understand how flawed and inaccurate facial recognition algorithms can be. For this, we need pictures of all Ministers' faces from all member States.

Three technical features (enrichment) will then be added to the website:

- We'll use publicly-available RBI software to assign emotions, gender and age attributes to each politician's photo and we'll display those on top of the photos;
- Users will be able to upload the photo of politicians to simulate the pervasiveness of surveillance;
- We'll make all data accessible to third parties, in order to anticipate a hypothetical market for biometric data. Here's an example of misattribution from: <https://dontspyonus.eu/list/>



These actions require cooperation from European citizens residing in the member states. To engage with member states, we could eventually promote the initiative in the national language.

In addition, on the website we will

- Document, prove, and write about counter-surveillance systems. We'd like to remind the user that there are ways to deal with these invasive technologies, and possibly teach them biometric self-defense techniques. This idea comes from a couple of considerations. Learning self-defense techniques could be very useful in the worst-case scenario of legalized biometric surveillance. After all, these systems do exist outside of Europe. Plus, not all citizens are currently protected by the official AI Act's draft approved in June. European and non-European citizens "on the move" or at the continent's borders still need to learn how to protect themselves from these invasive technologies, as at present there are no protective measures in place for them. A section of dontspyonus.eu will be dedicated to this goal - details will be further discussed.
- Emphasize the amount of "false positives" obtained by using biometric recognition algorithms. We will compare photos of politicians with photos of common citizens collected from public databases, such as lists of wanted persons or sex offenders. The amount of "wrong" (false) matches, based on similarities in physical appearance, is expected to be astonishingly high.

Activism: involvement & future events

We would also love to continue working on our "activism" side.

We ask to be included in daily/weekly updates on the technical and legal discussions around the AI Act's draft. We commit to having at least one member of our team monitor the news, someone who's in touch with the policy experts who work with us in lobbying. We need to be more informed on the AI Act in order to raise awareness on surveillance, AI accountability, and the importance of transparency, especially in the long term.

We commit to organizing a public advocacy event, later on in the year or in 2024, as soon as we have access to enough resources. We intend to apply for a **EU AI Fund grant** and organize an event focused on AI ethics and regulation, with guests such as independent software developers who are trying to build better AI systems. We are working on a more definite map of partners and a calendar of events.

In the meantime, we commit to producing a constant update in our communication channels (once the new website is ready), without engaging in *media terrorism*. We commit to supporting our communication strategy and actions with proper technical evaluation.

The whistleblowing initiative - temporary name "sinkhole".

Here's another project we are working on. **Sinkhole** will be a platform aimed at soliciting whistleblowers who work in places where facial recognition is adopted to collaborate with reporters who can validate the information received.


We have long-standing experience in setting up whistleblowing initiatives because Hermes Center was originally funded to develop <https://globaleaks.org>.

Warning

You are strongly advised to visit this site using the app called Tor Browser, that protects your identity.

[Download the Tor Browser](#)

Then, copy and paste the following address into the Tor Browser: `oua5tryyvrypbrlmjxkk4y5jnhbhp4x2r54j6uifse67ub262vdwl`
`ad.onion`



Sinkhole - investigate biometric identification trends

AIAct Policy lobbying

Which policy area is affected? *

- ☐ Artificial Intelligence (AI Act)
- ☐ Privacy (Gdpr)
- ☐ Digital Markets Act (DMA)
- ☐ EU rules on platform work
- ☐ Digital Services Act (DSA)

What type of activity do you want to report?

- ☐ Off the record lobby meeting
- ☐ Corruption and kickbacks
- ☐ Conflict of interest
- ☐ Revolving doors
- ☐ Other

What do you want to share in brief? ⓘ *

How are you involved in the reported facts? *

Please describe the evidence in detail. *

A thorough description of the submitted evidence enhances our ability to evaluate claims and investigate. Please take care to reference significant portions of any videos, images or documents submitted.

Have you reported the facts to other organizations and/or individuals? *

Can we validate this information from a different and/or external source?

Please attach any evidence to support your report

Upload

Select a file or drag it here.

Submit

Powered by [Globleaks](https://globaleaks.org)

As part of the new **Don't Spy EU** campaign, it would be possible to leak material to a group of recipients. A recipient is someone who would do the work of verification of the material being received. They could be EDRI members, for instance.

Sinkhole's hypothetical target audience would include:

- o People working on AI Act lobbying activities
- o Companies, developers, or people processing RBI data who can share information on how that market works.

We defined specific questions for the questionnaires in order to avoid uncontextualized submissions. To get updates check <https://sinkhole.dontspyonus.eu>.

Optional, additional activities

There are three other actions that we are still considering, that connect well with past experiences of our group. Here's a list, from the most feasible to the most arduous one. Please note that they have yet to be fully evaluated.

- o Use the right of access that every Italian citizen has to their public administrations. Should they have a legitimate interest, they can request by law to view and obtain public documentation. In this case, we would look for the presence of facial recognition-related documentation. We don't expect this transparency action to go through, and that would be great, because it would justify a demand for more transparency in the AI Act. Think of police/law enforcement: they are allowed to rely on biometric surveillance for "serious crimes". When asked to be transparent, they would be required to keep a publicly accessible record of all the times they used such systems.
- o If RBI is allowed on online material, RBI systems will be able to link whoever is portrayed in a picture to the context around them through massive face acquisition. Affected people cannot avoid the acquisition by giving their consent (they simply are not in control of all photographic material on the Internet) and cannot evade the judgment, because databases of this kind are used to pre-judge/profile individuals. What we can do to interfere with said systems is "polluting" the material that is being acquired. The next action would then be encouraging the creation of fake photos (=deepfakes), in which people's faces are doing things they've never done before. By doing so, the reliability of systems such as clearview.ai would plummet, because their technology would not be able to distinguish deepfakes from real photos anymore.