European Center for
Not-for-Profit Law

Taking Action Against Biometric Surveillance

Civil society tactics and strategies

Acknowledgements

This report was written by the European Center for Not-for-Profit Law (ECNL).

Authors:
Ashwin Prabu (ECNL fellow)
Marlena Wisniak
with support from Berna Keskindemir, Vanja Skoric and Karolina Iwanska

Design:
Sushruta Kokkula
Andrea Judit Toth

Authors would like to thank the members of the Global Expert Hub on AML/CFT for their critical input and review of the report. We are also grateful to all the civil society organisations and individual experts who provided invaluable input and feedback when developing the report. In particular, we thank Ahmed Albibas (Moomken), Danilo Krivokapic (SHARE Foundation), Heartland Initiative, Hiperderecho, Kade Crockford (American Civil Liberties Union of Massachusetts, ACLUM) and Weaving Libertation for their time and expertise.

September 2024

Contents

Introduction

Biometric surveillance has become ubiquitous since governments have started collecting physiological data such as fingerprints. In recent years, we've seen a surge in the development and deployment of algorithmic-driven biometric surveillance, specifically facial and emotion recognition. Yet these systems are fundamentally incompatible with democracy and human rights, threatening the civic freedoms of all, especially marginalised groups and civil society. Against the backdrop of shrinking civic space around the world, it's paramount to collectively stand up against this threat. By focusing not on the technology itself, but on the harms it causes to civil society and affected communities, we can stop the use of biometric surveillance in the public space – and avoid amplifying and exacerbating structural discrimination, monitoring, targeting, and oppression of marginalised groups.

Based on feedback from our partners at the Global Expert Hub on AML/CFT, we learned that there is still a great need to map the ecosystem of what tactics and strategies civil society organisations (CSOs) use to push back against biometric surveillance, so that more CSOs, especially those that represent marginalised groups and don't typically engage in digital rights, can take action in their respective contexts.

We define biometric mass surveillance as the deployment of AI-driven "smart cameras" that can collect and analyse biometric data (e.g. faceprints) on indefinite or large numbers of people in public places.[1] These cameras can conduct remote biometric identification (RBI) to identify individuals at a distance by comparing their unique biometric features with a database. Law enforcement typically uses RBI either in real-time (live recognition) or post-time (retrospective recognition based on prior video footage).

We conducted virtual consultations with 11 digital rights experts who, through their CSOs, have conducted successful campaigns against biometric surveillance across Europe, the United States, Latin America, and Occupied Palestinian Territory. We learned about the advocacy strategies they used in their campaigns and received advice and recommendations for CSOs looking to launch campaigns of their own. These consultations, along with our own experience and desk research about the policy positions, campaigns, and litigation regarding biometric surveillance, informed our report.

In our report, we detail a multifaceted approach to pushing back against biometric surveillance. Specifically, we highlight key tactics to achieve this through policy advocacy, evidence collection, strategic litigation, coalition and capacity building, company and investor engagement, and awareness campaigns including through creative media outlets and art. We also spotlight two case studies of successful campaigns against biometric surveillance, led by SHARE Foundation in Serbia and Amnesty International in Occupied Palestinian Territory.

This report serves as an initial blueprint for CSOs worldwide to act against biometric surveillance in their communities. We intend for this to be a live document, to be updated with new case studies, tactics, and campaigns based on community and civil society feedback.

6 Strategies against biometric surveillance

Policy advocacy

Evidence collection/reporting/monitoring

Strategic litigation

Coalition and capacity building

Engage with tech companies and investors

Awareness raising/campaign/media

A. Policy advocacy

Policy advocacy is a powerful tool to push back against and regulate the use of biometric surveillance in the public space. Recent years have seen an uptake of legislations regulating the use of AI-driven surveillance technologies, such as the EU AI Act and the Council of Europe Convention on AI, and civil society has been at the forefront of these efforts.

As governments around the world race to regulate AI, including facial recognition technology (FRT), CSOs should have a seat at the table. When CSOs develop policy positions, it's important to first gather evidence about how biometric surveillance is impacting communities, by listening and engaging with them directly and learning from first-hand accounts and experiences. Then, it's helpful to build a coalition with other organisations,[2] engaging with many different groups and perspectives, especially from marginalised groups, and co-creating policy positions and advocacy strategies.[3]

EXAMPLE

CSOs actively participated in developing the EU AI Act, aiming for a full prohibition on the development and deployment of biometric surveillance. After years of advocacy and drafting, the EU AI Act was approved and includes prohibitions of "some uses of real-time remote biometric identification (RBI) by police in publicly accessible spaces; emotion recognition in workplaces and education settings; certain types of biometric categorization; and all scraping of the internet to get facial images for biometric databases."[20] Unfortunately, major loopholes still limit how much the AI Act truly protects people against the use of mass surveillance.[21] However, CSOs are now organizing to engage in the implementation of the EU AI Act.[22] European CSOs are also organizing beyond the scope of the AI Act, using existing laws like the EU General Data Protection Regulation (GDPR) to increase the standard of protection for digital rights and promoting anti-surveillance narratives.

Outlined below are some suggestions for policy positions that CSOs can advocate for in their respective countries or regions as needed.

1. Push for legislation that bans the use of RBI in public spaces

RBI enables government agencies to conduct mass surveillance and discriminatory targeted surveillance in a way that is incompatible with human rights. CSOs should therefore push states to legally prohibit government agencies from using facial recognition and remote biometric recognition technologies in public and publicly accessible spaces. These bans must avoid exemptions for law enforcement, criminal investigation, border control, counter-terrorism, and security agencies. States should prohibit government agencies, especially law enforcement agencies, from using and accessing data and information derived from the use of these technologies by private companies and other private actors. They should furthermore prohibit the use of these technologies by private entities in public spaces, publicly accessible spaces, and places of public accommodation.[4]

2. Ensure restrictions are narrowly defined, enforced, and effective at fully preventing the use of RBI in public spaces

a. Monitor and push back against exemptions for national security, counter-terrorism, or emergency measures that unduly restrict human rights.[5]
b. Ensure that both real-time (live) and post (retrospective) use of RBI are banned. For example, in the EU AI Act, some real-time uses of RBI are banned, but post-use of RBI is merely classified as high-risk.[6]
c. Advocate for legislation to detail accountability structures and independent oversight measures and ensure access to remedy for individuals whose rights are violated by biometric surveillance.[7]
d. Issue complaints to executive enforcement bodies about the illegal use of biometric surveillance.

Where a ban is not feasible, consider the following policy positions:

3. Oppose laws that authorise surveillance and limit their scope

If laws banning surveillance seem difficult to pass, then advocating against laws that authorise surveillance can be an effective tool to voice public opposition.

EXAMPLE

We can see an effective example of this with Serbia. Led by the SHARE Foundation, community organizers in Serbia twice stopped a law legalizing facial recognition from passing. This failure sent a clear message to the Serbian government that their constituents oppose FRT.[23] If laws authorizing biometric surveillance seem to be more popular, then CSOs can protect human rights by limiting the scope of authorization.

4. Push for mandatory transparency of government use of biometric surveillance

If AI surveillance technologies are already being deployed, then advocating for authorities to publicly release details about their use would be very powerful. Organisers should push authorities to disclose which government entities use AI surveillance systems,[8] what procedures are followed to authorise surveillance and usage, sharing, storage, and destruction of data acquired through the AI systems, and key information about the use of AI systems, such as the number of investigations they were used in and the outcomes of those investigations. Organisers could also push for legislation that requires entities to inform all people who are subjected to surveillance, share the information that was gathered, explain to them the reasons why they are subjected to biometric surveillance, and share opportunities for redress if surveillance exceeds its purpose.[9] Pushing for mandatory transparency can make it easier to collect evidence, engage in litigation, and organise citizens.

Corporate transparency: Legally require that private surveillance companies disclose products and services offered and sold, which clients are involved, and specify when products are used for national security and/or counter-terrorism purposes.

5. Restrict "mission creep" of surveillance

Regardless of the rationale for its collection, once biometric data has been obtained, it may later be drawn upon for other objectives. This phenomenon is known as function creep or mission creep, in which systems "originally intended to perform narrowly specified functions are expanded [...] thereby sidestepping or pushing the limits of legal frameworks meant to protect issues of privacy and data protection."[10] The same can happen with the use of the AI surveillance system itself, where the government uses it for purposes beyond the original one it was established to address.

EXAMPLE

For example, in 2009, EU member states began to share biometric data stored on European Asylum Dactyloscopy Database (EURODAC) with law enforcement to "fight terrorism." EURODAC was established with the sole purpose of helping states process asylum application; the data processed was never intended to be shared with law enforcement.[24] Such expansive use of biometric surveillance, without due protections for human rights and legal safeguards, should be prohibited.

a. Ensure that any collection of biometric data is in line with relevant international and national legislation (if it exists) and that it fulfills the conditions of necessity and proportionality, especially the need to consider if the collection of non-biometric data would achieve similar results (subsidiarity).
b. Restrict biometric data sharing between government agencies, especially law enforcement such as the police or border control.
c. Restrict government authorities from expanding surveillance beyond its initial scope, capabilities, and purposes.

6. Right to remedy

When advocating for legislation that restricts biometric surveillance, it's important to ensure the law includes effective right to remedy. For example, this could look like a right to bring grievances to an independent authority and have access to redress. Relatedly, including a right to refusal such as not being subjected to these AI systems, and a right to information about the use and functioning of AI systems, can provide individuals with legal standing to contest AI systems that have violated their rights.[11]

B. Evidence collection / reporting / monitoring

Government surveillance is often opaque to civil society and the public. Evidence collection and investigative reporting are crucial to uncovering how governments are using biometric surveillance against their citizens. Outlined below are some strategies that we recommend CSOs undertake to learn more about government surveillance in their local contexts.

1. Gather publicly available information

CSOs can start by looking for relevant public information shared by the government or other actors such as companies, journalists or civil society. For example, CSOs can study and map out the development or implementation of relevant laws such as data protection laws and laws that authorise surveillance.[12] Gathering this type of information can support CSOs to effectively organise communities and influence how policies are developed or implemented.

EXAMPLE

In Serbia, the government publicly announced a partnership with Huawei to procure thousands of cameras with FRT capabilities. This served as a starting point for SHARE Foundation to begin its advocacy efforts.[27] In Mexico, R3D, a Mexican digital rights organization continuously monitors bills and initiatives related to biometrics as well as to political discourse around "digitalizing" the government to inform its advocacy strategy.[28]

2. Freedom of Information requests / investigating

A Freedom of Information (FOI) request is a formal process for stakeholders such as CSOs to request access to information held by government authorities. It can help reveal crucial information about the deployment of biometric surveillance (e.g., how many cameras are deployed, what data is collected, etc.). Information received from FOIs can be a starting point for further investigation, policy advocacy, or strategic litigation.

EXAMPLE

The digital rights experts we consulted shared mixed experiences with FOI requests. For example, when SHARE foundation was advocating against biometric surveillance in Serbia, all their FOI requests were denied.[25] Other CSOs in the United States found difficulty with FOIA requests, describing the process as a "very slow and bureaucratic hurdle."[26] On the other hand, some CSOs in the European Union gained helpful information about surveillance thanks to this process. In the EU, CSOs also successfully collaborated with independent journalists who found alarming information about government procurement of surveillance technology through FOI requests.

3. Study biometric surveillance capabilities

If the government doesn't disclose information, CSOs can investigate the FRT companies themselves to learn more about surveillance capabilities. Surveillance Watch, a community-driven initiative that created an interactive map to expose the hidden connections between surveillance companies, financial backers, and governments, is an open repository of companies involved in surveillance technology. It is an incredible resource for any CSO looking to learn more about the surveillance industry.

EXAMPLE

The Serbian government was rejecting FOI requests from civil society regarding their use of biometric surveillance, so SHARE Foundation and allies researched the technology company supplying the FRT, Huawei, and their advertisements regarding their technological capabilities and patents.[32] Through this investigative process, SHARE was able to understand what biometric mass surveillance in Serbia could look like and expose capabilities and risks.

4. Grassroots evidence collection

Grassroots evidence collection can be helpful where there is limited access to government authorities or corporations. Open source intelligence (OSINT), the collection and analysis of data gathered from open sources, is a powerful method too. Whatever the specific tactic may be, anyone can collect evidence about how their own communities are subjected to surveillance, and CSOs can gain a lot of insight by engaging directly with communities targeted or in any way impacted by biometric surveillance.

EXAMPLE

In Serbia, SHARE Foundation mobilized citizens to take pictures of surveillance cameras in public spaces. With this information, they were able to geographically map out where FRT is being used.[29] Hiperderecho, a Peruvian digital rights organization, launched a campaign in 2021 called "Who watches over the watchers?" to support protestors in Peru. They collaborated with the Fotografx Autoconvocadxs collective, an organization that goes to protests and documents the events through pictures.[30] Photography is a powerful form of evidence gathering that can expose surveillance and police brutality. Other ideas we learned from our consultations include collaborating with local journalists and using public tools like Google Streetview to investigate surveillance infrastructure. [31]

5. Publish and disseminate evidence-based reports

Reports can inform the public on government abuse of surveillance technology as well as their relationships with companies. They can strengthen and empower the global movement against surveillance, and ultimately lead to government and corporate accountability.

EXAMPLE

Amnesty International exposed government surveillance through their Ban the Scan Project. They conducted research in Occupied Palestine, New York City, and Hyderabad City, India, publishing reports and videos on how governments in these respective locations are deploying biometric surveillance to strengthen control over civilians, thereby restricting human rights. As mentioned above, Surveillance Watch maps out the relationships between surveillance technology companies, financial backers, and governments.

C. Strategic litigation

Strategic litigation is an effective practice to ensure that rights and legal protections are upheld and to push for change in legal norms and set precedent. This can strengthen civil society movements and lead to large-scale impact. When pursuing litigation, it is important to organise communities strategically to support the legal cause and the overall movement. While litigation has the power to provide intermediary remedies to harm, coalitions around litigation can push for more transformative change.[13]

EXAMPLE

For example, Weaving Liberation advocates for community-centered strategic litigation (CCSL) where impacted communities are at the forefront and the goals and means of the litigation are decided collectively. CCSL decenters legal tools as the primary means for achieving justice and focuses on community organizing and capacity building. [33]

Outlined below are some strategic litigation cases that successfully pushed back against biometric surveillance.

Ed Bridges v. South Wales Police: Liberty, a UK human rights advocacy and legal organisation, challenged police use of FRT for the first time, by successfully supporting plaintiff Ed Bridges in their challenge of South Wales Police's use of FRT in public settings. Particularly, Liberty argued that South Wales Police's use of FRT violated the right to respect for private life under Article 8 of the European Convention on Human Rights and violated the Public Sector Equality Duty Convention outlined in section 149 of the Equality Act 2010. In August 2020, the Court of Appeals found that the South Wales Police violated privacy rights, data protection laws, and equality laws in their use of FRT.

Sao Paulo Metro System: A group of CSOs sued Sao Paulo Metro Company for collecting biometric data of users of the metro system. The Sao Paulo State Court ruled that the Metro company violated the General Law on Data Protection and ordered them to stop using the technology. The group of CSOs seized this momentum to spark a national discourse on how to shape jurisprudence on FRT and the collection, processing, and sharing of personal data.

Meta "Tag Suggestions Feature": Meta illegally captured biometric data "billions of times" from photos and videos that users uploaded to create "Tag Suggestions," which could recognise a user's friend in a photo and suggest that the user tags them. The company settled with U.S. States of Texas and Illinois for violating their respective biometric privacy laws. The company has since discontinued the "Tag Suggestions" feature.

No al padrón campaign: In 2021, Mexico tried to establish a registry of mobile phone users' biometric data, which the Mexican government claimed was needed to reduce crime. A coalition of organisations including R3D litigated against this bill. They created a legal brief that could be easily downloaded so that any citizen with a phone could start their own litigation process against the bill. In April 2022, Mexico's Supreme Court ruled that creating a national cellphone user registry with biometric data was unconstitutional.

D. Coalition and capacity building

Given the uneven playing field between governments, companies, and civil society, working in coalition is critical. This is especially important in the context of biometric surveillance, where there is increased opacity and severe human rights risks. That said, well-funded Western CSOs should be careful not to impose policy positions on other CSOs, especially when looking to grow a coalition to support a particular campaign. The traditional approach of one CSO spearheading a campaign and reaching out to others to sign on can be re-imagined to be more collaborative.

A specific tension that we noticed in our consultations is how to navigate the power dynamic between well-funded Western CSOs with digital rights teams and underfunded CSOs representing marginalised groups and the Global Majority when engaging in coalition building. CSOs representing marginalised communities and the Global Majority are most connected to the dangers of biometric surveillance and they should be empowered to set their own agenda around biometrics and how to push back against it. When launching campaigns, well-funded Western CSOs should scrutinise who is in the room when key decisions are being made and whose voice and views are being left out.

Outlined below are strategies that we and our allies believe can address power imbalances in coalition building:

1. Co-create policy positions and advocacy strategies and engage in shared knowledge production with coalition partners

EXAMPLE

For example, the prohibitions in the EU AI Act would likely not have been possible without coordinated civil society in the EU. As part of the 'Reclaim Your Face Campaign,' 198 civil society actors and 250,000 European citizens got together to demand a ban on all biometric mass surveillance practices. They were able to achieve some biometric surveillance bans in the EU AI Act. Even if there are loopholes in the act, this would likely not have been possible without effective, strategic coalition building. Their campaign also made the term, "Biometric Mass Surveillance," commonplace, which has supported latter campaigns.[34] However, reflecting on their 'Reclaim Your Face Campaign,' EDRi also shared that their efforts could have been more powerful if they were more intentional about co-creating policy positions and sharing knowledge with their coalition partners prior to launching the campaign.

2. Take concrete steps to redistribute power, access and resources

EXAMPLE

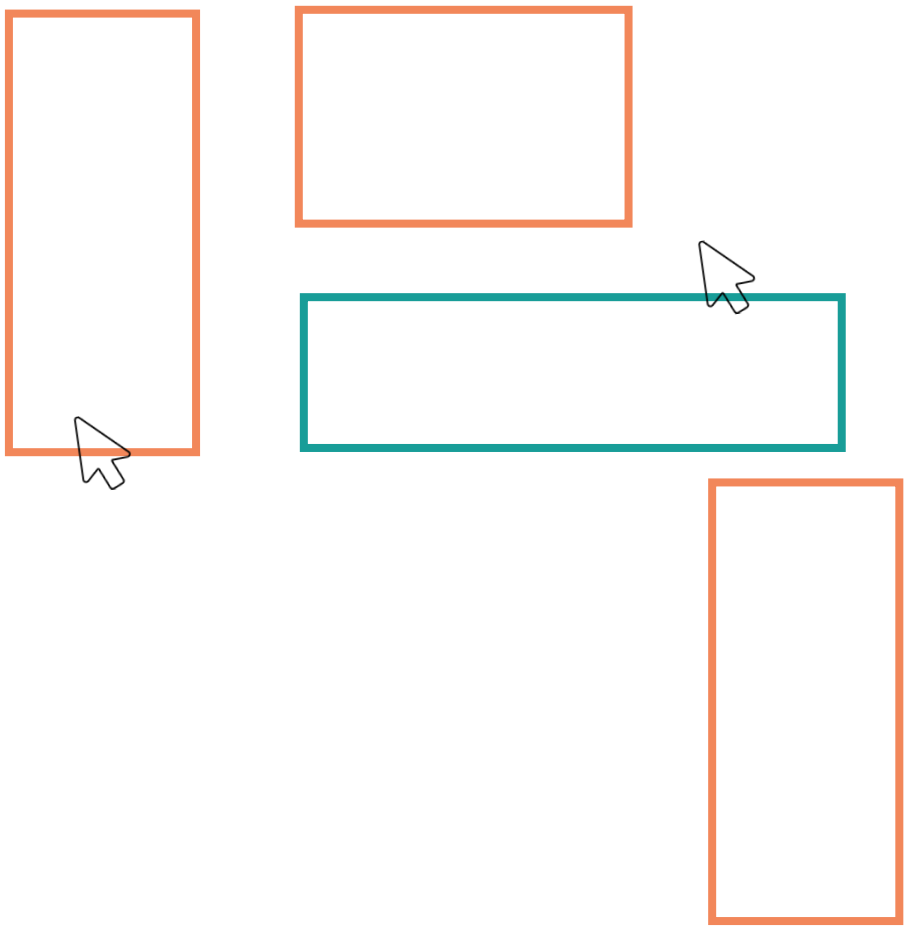
EDRi recognised that they were much more funded than the non-digital rights community organizations they were working with. In their Reclaim Your Face campaign, they addressed this disparity through group fundraising, re-directing funds, and providing stipends for experts participating in their papers and talks. EDRi also acknowledged that they had more access to Members of Parliament (MEPs) than their partners. They addressed this disparity by running a "Boot Camp," where they supported and empowered local community organizations to recognize parts of their existing work that already included digital elements, sharing knowledge on advocating to MEPs, and connecting these groups to MEPs through joint meetings.

3. Decenter technology, center harm

Instead of focusing on technological tools, it{s important to analyse the harm that these technologies can have on communities. In our consultations, CSOs suggested moving away from tech jargon, a set of vocabulary that they feel can be “opaque and difficult to organise around,” and instead make space for community organisations to reclaim epistemology around technology.

EXAMPLE

Weaving Liberation creates these spaces through their workshops, where they focus on building a community where marginalized groups are in the majority, feel that they have control over the space and discourse, and build capacity to share knowledge within communities.[35]



E. Engage with tech companies and investors

Technology companies can contribute to or be linked to human rights abuses, for example by selling FRT to governments who can use these technologies in a way that causes harm. Under the UN Guiding Principles on Business and Human Rights (UNGPs), companies have a responsibility to prevent, mitigate, address, and remedy any adverse impacts that may be caused by, or connected to, their products or activities. To effectively push back against biometric surveillance, CSOs can engage with technology companies and investors to effectively conduct human rights due diligence and hold them accountable.[14]

CSOs can push technology companies (or engage with investors who can influence companies) to take the following key actions:[15]

1. Technology companies should develop and enforce a publicly available human rights policy.
2. Technology companies should conduct human rights due diligence, including by assessing the human right impacts that their products may have at all stages of the AI lifecycle (design, development, promotion, deployment, sale, licensing, and use). They should publish their human rights impact assessments and meaningfully engage with civil society and affected communities when conducting the assessments.
3. Technology companies should implement export controls and restrict sales to authoritarian regimes or countries with poor human rights records.
4. Technology companies should ensure effective access to remedy for those whose rights have been violated by their products through internal governance mechanisms.
5. If establishing permanent human rights policies does not seem feasible, CSOs can push companies to implement moratoriums on their partnerships with law enforcement or countries with poor human rights records.[16]

EXAMPLE

Heartland Initiative furthermore advises CSOs to make the "business case for human rights" to investors and technology companies. This consists of connecting human rights violations to regulatory risks (e.g. sanction violations, trade controls), legal risks (e.g. strategic litigation against companies that have been sued for violating international humanitarian law), operational risks, and reputation risks.

F. Awareness raising / media campaigns

Many of the organisations we consulted mentioned how CSOs need to counter dominant narratives around surveillance. Governments and technology companies argue that biometric surveillance promotes safety by helping law enforcement address crime and protect their citizens ("safety and security narrative"). Governments also promote narratives that biometric identification prevents fraud, is efficient, and makes citizens' lives easier. Against this backdrop, CSOs should develop counter narratives to raise awareness of the human rights risks of biometric surveillance and the lack of evidence of its effectiveness for security.

In a 2022 poll of citizens in 12 EU countries, ECNL found that 38% of respondents were not concerned about government use of AI for national security and 49% of respondents were not concerned about the use of AI for crime prevention.

In their campaign, "Press Pause on Surveillance," the ACLU of Massachusetts emphasised the invasiveness of biometric surveillance. They explained how citizens can be tracked from the moment they leave their house to the moment they come back. They also tried to creatively work around the "safety and security narrative" by focusing on narrow exceptions for rights-based used of FRT, based on legality and proportionality (e.g. law enforcement can only use FRT under strict rules and in limited circumstances during an investigation).[17] In Mexico, R3D also worked to shift the narrative promoted by the government, who argued that digitalizing the government would make it more efficient.[18] Amnesty International pushed back against the narrative that Israel's right to sovereignty justifies the use of mass biometric surveillance.[19]

Documentaries can help CSOs design and promote new narratives. Documentaries can raise awareness about the dangers of surveillance and serve as a platform for individuals impacted to share their stories. CSOs can collaborate with filmmakers to make documentaries to reach wider audiences.

Powerful documentaries created by CSOs on biometric surveillance include Coded bias and "How Surveillance Tech is Used to Oppress Palestinians Through Apartheid".

How Surveillance Tech is Used to Oppress Palestinians Through Apartheid?

Art is another beautiful way to counter narratives and reach large groups, especially those who aren't involved in activism or digital rights. CSOs can explore ways to showcase their work by partnering with artists or creatives.

Such as;

- Algorithmic Justice League has many art exhibitions that are critical of AI
- Poet of Code (Dr. Joy Buolamwini) Shares: AI, Ain't I A Woman

EXAMPLE

In their campaign against biometric surveillance in Serbia, SHARE foundation collaborated with local artists. Below is a political cartoon encouraging people to sign SHARE's petition against facial recognition.

https://kit.exposingtheinvisible.org/en/anti-biometric.html

Conclusion

Taking action against biometric surveillance is most effective when multiple or all the tactics outlined in this report are pursued in tandem, as they strengthen and enhance each other. Pursuing one strategy opens opportunities for other ones. Indeed, advocating for policies that include a right to remedy enables strategic litigation. Collecting evidence and disseminating it widely supports awareness raising campaigns. Strategic litigation shifts the legal ecosystem and can promote anti-surveillance narratives, led by coalitions. From organisers, affected communities and researchers to policymakers, private sector actors and funders, we need people everywhere – and we need to bring them together to protect our communities from biometric surveillance.

Case Studies

Serbia: In January 2019, the Serbian Ministry of Interior announced a collaboration with Huawei, a Chinese technology company, to deploy 8,000 cameras with facial recognition capabilities in Belgrade. The Serbian government pledged that the deployment would make Belgrade safer for all Serbians. Understanding the severe threat to human rights this project posed, SHARE Foundation quickly launched a campaign to push back. They first started with evidence-gathering. They submitted Freedom of Information requests to learn more about these technologies, but the Serbian government denied them all. SHARE then employed a reverse engineering strategy and researched Huawei's technological patents and capabilities, based on information that the company shared publicly on their website. With this information, SHARE crafted a counter-narrative that exposed the capabilities of FRT and the risks it posed to fundamental freedoms such as the right to privacy, freedom of expression, and freedom of assembly and association, among others.

They successfully mobilised Serbian citizens around this narrative, raised money through crowdfunding and micro-donations and shared their message via media outlets. They were even able to map camera locations by mobilizing citizens to take photos of cameras in their neighborhoods and post them on their 'Thousands of Cameras' Twitter account. They also engaged in coalition building with EDRi, joining the "Reclaim Your Face" campaign to ban biometric mass surveillance. SHARE's campaign applied pressure on the Serbian government and forced them to engage with external stakeholders, including civil society.

After a hard-fought campaign, the Serbian government withdrew the proposed legislation to legalise mass biometric surveillance and halted the deployment of facial recognition cameras. However, thousands of CCTV cameras without facial recognition capabilities are still deployed in Serbia. SHARE will continue to advocate against future attempts to legalise and deploy biometric surveillance in Serbia.

Occupied Palestinian Territory: Amnesty International investigated the use of FRT in Occupied West Bank, specifically Hebron and East Jerusalem. In the context of an apartheid state with Israeli settlements and institutionalised discrimination, Amnesty investigated how biometric surveillance is strengthening apartheid in these cities and impacting Palestinians' right to movement. To do this, Amnesty partnered with academics and local organisations in Palestine, visited the cities with 360-degree cameras, and interviewed Palestinian families, activists, and students. However, to ensure the security of the researchers and participants, Amnesty decided not to directly engage with Israeli officials.

Amnesty exposed Israel's new system called 'Red Wolf.' 'Red Wolf' is an AI system used in military checkpoints that makes automated decisions on entry based on facial recognition. If a biometric entry does not exist for an individual, then the system captures the individual's biometric data without their consent. Amnesty claims that it is highly likely that 'Red Wolf' is connected to an expansive database containing personal information about Palestinians in Hebron, helping Israeli military officials make quick decisions about allowing or denying entry without even having to check the individual's identification card. In their interviews, Amnesty found that Red Wolf heavily and systematically restricts freedom of movement, erodes social life, represses activism, and instills fear in Palestinians. With a poor record of discrimination and human rights violations, Israeli authorities are using FRT to strengthen discriminatory policing and segregation in the West Bank.

Building off this work, Amnesty is now advocating for export controls to prevent companies from selling this technology to Israel, as part of a wider effort to incorporate human rights due diligence into investor and corporate decision-making.

Endnotes

1 European Digital Rights (EDRi). (2020, May). Biometric mass surveillance: Explainer. https://edri.org/wp-content/uploads/2020/12/Biometric-mass-surveillance-explainer.pdf

2 Interview with Surveillance Technology Oversight Project, personal communication, August 8, 2024.

3 Interviews with European Digital Rights, personal communication, August 7, 2024, and Center for Democracy and Technology, personal communication, August 9, 2024.

4 Access Now. (2021, June 7). Ban biometric surveillance: Statement (English version). https://www.accessnow.org/wp-content/uploads/2022/08/BanBS-Statement-English.pdf

See endnote 3 for EDRi advocacy

ARTICLE 19. (2021, April). Biometric technologies, privacy, data and freedom of expression: Privacy and data concerns associated with biometric technologies. https://www.article19.org/biometric-technologies-privacy-data-free-expression/

5 European Center for Not-for-Profit Law (ECNL). (2022, October 18). Rights-free zone? The blanket national security exemption in AI legislation (pp. 14–15). https://ecnl.org/news/rights-free-zone-blanket-national-security-exemption-ai-legislation

Skoric, V. (2022, November 15). Why the EU needs to rethink the AI Act's public exemptions. EUobserver. https://euobserver.com/opinion/156421

6 See endnote 3.

7 See endnote 4..

8 For example, a public register register in the Netherlandsn list cases of AI systems used in policing, such as predictive policing. See: Crime Anticipation System https://algoritmes.overheid.nl/en/algoritme/81228922 , Amsterdam Top400/600 criminals https://algoritmes.overheid.nl/en/algoritme/top-400600-municipality-of-amsterdam/75856898#verantwoordGebruik

9 Amnesty International. (2024, July). Under-protected and over-restricted: The state of the right to protest in 21 countries in Europe (p. 206). https://www.amnesty.nl/content/uploads/2024/07/Under-protected-and-over-restricted.-The-state-of-the-right-to-protest-in-21-countries-in-Europe-FINAL.pdf?x25503

10 Broeders, D. "The New Digital Borders of Europe: EU Databases and the Surveillance of Irregular Migrants." International Sociology 22, no. 1 (January 1, 2007): 71–92. https://doi.org/10.1177/0268580907070126.

11 European Digital Rights (EDRi). (2022, May). Rights and redress: Amendments to the Artificial Intelligence Act for online platforms. https://edri.org/wp-content/uploads/2022/05/Rights-and-Redress-AIA-Amendments-for-online.pdf

12 See endnote 3

13 Meyer, L. (2023, April 4). A season of digital rights for all: The case for community-centred strategic litigation. Digital Freedom Fund. https://digitalfreedomfund.org/a-season-of-digital-rights-for-all-the-case-for-community-centred-strategic-litigation/

14 For CSOs looking for a resource on how to have meaningful engagement and dialogue with companies, ECNL's framework for meaningful engagement is a great resource

https://ecnl.org/publications/framework-meaningful-engagement-human-rights-impact-assessments-ai

15 Heartland Initiative et al. (2022, March). Navigating the surveillance technology ecosystem: A human rights due diligence guide for investors. https://www.accessnow.org/wp-content/uploads/2022/03/2022_STAP_Guide.pdf

Heartland Initiative also has a saliency materiality index whitepaper coming out in September 9

16 Amazon has implemented an indefinite moratorium on US police use of its facial recognition software, following protests in the United States against police brutality.

Dastin, J. (2021, May 18). Exclusive: Amazon extends moratorium on police use of facial recognition software. Reuters. https://www.reuters.com/technology/exclusive-amazon-extends-moratorium-police-use-facial-recognition-software-2021-05-18/

17 Interview with ACLU Massachusetts, personal communication, August 6, 2024

18 See endnote 13.

19 See endnote 20.

20 European Digital Rights (EDRi). (2023, August 14). How to fight biometric mass surveillance after the AI Act: A legal and practical guide. https://edri.org/our-work/how-to-fight-biometric-mass-surveillance-after-the-ai-act-a-legal-and-practical-guide/

21 European Center for Not-for-Profit Law (ECNL). (2024, March 4). Packed with loopholes: Why the AI Act fails to protect civic space and the rule of law. https://ecnl.org/news/packed-loopholes-why-ai-act-fails-protect-civic-space-and-rule-law

22 ECNL recently wrote a report called “Towards An AI Act That Serves People And Society” (August, 2024) identifying opportunities for civil society to influence implementation of EU AI Act

23 SHARE Foundation. (2023). Beyond the face: Biometrics and society (pp. 233–235). https://www.sharefoundation.info/wp-content/uploads/Beyond-the-Face_Biometrics-and-Society.pdf

24 Privacy International. (2020, July). Responsible use and sharing of biometric data in counter-terrorism (pp. 14–15). https://privacyinternational.org/sites/default/files/2020-07/Responsible%20use%20and%20sharing%20of%20biometric%20data%20in%20counter-terrorism.pdf

25 See endnote 12.

26 Interview with Center for Democracy and Technology, personal communication, August 9, 2024.

27 Interview with Danilo Krivokapić, personal communication, August 5, 2024.

28 Interview with Grecia Llanas, personal communication, August 6, 2024.

29 See endnote 12.

30 Interview with Hiperderecho, personal communication, August 2, 2024

31 Interview with Amnesty International, personal communication, August 14, 2024

32 See endnote 12.

33 Interview with Amnesty International, personal communication, August 14, 2024

34 See endnote 16.

35 Interview with Weaving Liberation, personal communication, August 12, 2024

ANNEX A: Overview of international AI regulation of biometric surveillance

Legal frameworks regulating AI systems can provide opportunities to counter biometric surveillance. This annex outlines the key laws and policies that have emerged in recent years at the national, regional and international level.

International

1. Council of Europe convention on AI (adopted 17 May 2024)

The Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law is a legally binding international convention regulating AI. When developing and/or using AI systems (including AI-driven biometric surveillance technologies) **outside the context of national security interests (article 3(2)) or national defense (article 3(4))**, signatory States are obliged to:

- Adhere to relevant human rights, democracy and rule of law principles as listed in articles 4 trough 13, which include transparency and oversight (article 8), equality and non-discrimination (article 10), and privacy and personal data protection (article 11).
- Provide accessible and effective remedies for violations, including effectively lodging a complaint to competent authorities (article 14(c)). This could be interpreted as requiring relevant information and documentation of biometric surveillance systems used that will allow the affected persons to lodge a complaint.
- Provide procedural safeguards and notify persons interacting with the AI system (article 15);
- Assess the need for a moratorium or ban or other type of appropriate measure where the State considers certain uses of biometric surveillance systems incompatible with human rights, democracy and rule of law (article 16(4)).

For more information about the promises and limitations of the Convention on AI, especially as related to the national security exemptions, check out ECNL's reflections.

2. United Nations standards on technology and human rights

The Human Rights Council (HRC) and UN General Assembly (UNGA) resolutions are non-binding but can nonetheless have considerable political force.

2.1 UNGA resolution A/RES/78/213 (Promotion and protection of human rights in the context of digital technologies - adopted 19 December 2023)

Relevant to biometric surveillance, the UNGA:

- "Notes with deep concern the use of technological tools developed by the private surveillance industry and by private or public actors to undertake surveillance (...), and data collection, interfering with the professional and private lives of individuals, including those engaged in the promotion and defence of human rights and fundamental freedoms, journalists and other media workers, in violation or abuse of their human rights, and therefore:"
- "Urges Member States to refrain from employing unlawful or arbitrary surveillance techniques" (para. 15);
- "Calls upon Member States to ensure that targeted surveillance technologies are only used in accordance with the human rights principles of legality, necessity and proportionality, and that legal mechanisms of redress and effective remedies are available for victims of surveillance-related violations and abuses" (para 16).

2.2 HRC Resolution 53/27 rev.1 (New and emerging digital technologies and human rights - 12 July 2023)

Relevant to biometric surveillance, The Human Rights Council:

- Recognizes the "serious risks" that "artificial intelligence systems can pose to human rights "when used without appropriate safeguards and including when used for identification, tracking, profiling, facial recognition, the generation of synthetic photorealistic images, behavioural prediction or the scoring of individuals."
- Highlights "the importance of the need to respect, protect and promote human rights and fundamental freedoms, in recognition of the inherent dignity of the human person, throughout the lifecycle of artificial intelligence systems" (article 3), including biometric surveillance technology, and towards this end, "the need to pay attention to:
    - 3(c): Promoting the transparency and explainability of AI systems, which include biometric surveillance technology;
    - 3(d): Ensuring that data for artificial intelligence systems are collected, used, shared, archived and deleted in ways that are consistent with the States' respective obligations under international human rights law and the responsibilities of business enterprises in line with the Guiding Principles on Business and Human Rights;"
- Stresses that "certain applications of artificial intelligence present an unacceptable risk to human rights." While it falls short of explicitly calling for a ban or moratorium on such applications and outlining which applications reach this threshold, this statement can serve as a base for advocating that biometric surveillance must be prohibited as it poses an unacceptable risk to human rights.

2.3 HRC Resolution 53/13 (Civil Society Space - adopted 6 July 2023)

Relevant to biometric surveillance, The Human Rights Council:

- Reiterates its "grave concerns" that in many countries, human rights and fundamental freedoms defenders are facing attacks "both online and offline" including "unlawful or arbitrary surveillance" and "restrictions on freedom of association or expression or the right to peaceful assembly."
- Acknowledges that "digital surveillance and undue restrictions (...) are not conducive to a safe and enabling space for civil society."

Regional: Europe

The EU AI Act is the first binding legislation on AI that includes specific rules on real-time biometric identification (RBI) and limited prohibitions. While binding for EU Member States only, the AI Act and its prohibitions are expected to set a global precedent.

Article 5

5(1) "The following AI practices shall be prohibited:

- g) the placing on the market, the putting into service for this specific purpose, or the use of biometric categorisation systems that categorise individually natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, sex life or sexual orientation; this prohibition does not cover any labelling or filtering of lawfully acquired biometric datasets, such as images, based on biometric data or categorizing of biometric data in the area of law enforcement;
- (h) the use of 'real-time' remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement, unless and in so far as such use is strictly necessary for one of the following objectives:
    - the targeted search for specific victims of abduction, trafficking in human

beings or sexual exploitation of human beings, as well as the search for missing persons;
- the prevention of a specific, substantial and imminent threat to the life or physical safety of natural persons or a genuine and present or genuine and foreseeable threat of a terrorist attack;
- the localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution or executing a criminal penalty for offences referred to in Annex II and punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least four years. Point (h) of the first subparagraph is without prejudice to Article 9 of Regulation (EU) 2016/679 for the processing of biometric data for purposes other than law enforcement."

5(4): "Without prejudice to paragraph 3, each use of a 'real-time' remote biometric identification system in publicly accessible spaces for law enforcement purposes shall be notified to the relevant market surveillance authority and the national data protection authority (...)."

Article 6(2): "AI systems referred to in Annex III shall be considered to be high-risk."

Annex III - Article 1: "Biometrics, in so far as their use is permitted under relevant Union or national law:
- (a) remote biometric identification systems. This shall not include AI systems intended to be used for biometric verification the sole purpose of which is to confirm that a specific natural person is the person he or she claims to be;
- (b) AI systems intended to be used for biometric categorisation, according to sensitive or protected attributes or characteristics based on the inference of those attributes or characteristics;
- (c) AI systems intended to be used for emotion recognition."

Article 50(3): "Deployers of an emotion recognition system or a biometric categorisation system shall inform the natural persons exposed thereto of the operation of the system, and shall process the personal data in accordance with Regulations (EU) 2016/679 and (EU) 2018/1725 and Directive (EU) 2016/680, as applicable. This obligation shall not apply to AI systems used for biometric categorisation and emotion recognition, which are permitted by law to detect, prevent or investigate criminal offences, subject to appropriate safeguards for the rights and freedoms of third parties, and in accordance with Union law."

For an explainer about how the provisions relevant to biometric surveillance might be implemented, read EDRi's "How to fight Biometric Mass Surveillance after the AI Act: A legal and practical guide." To better understand the exceptions and exemptions of the AI Act, read ECNL's "Packed with loopholes: Why the AI Act fails to protect civic space and the rule of law."

European Center for
Not-for-Profit Law

European Center for Not-for-Profit Law Stichting

Riviervismarkt 5, 2513 AM,
The Hague, Netherlands

www.ecnl.org
LinkedIn
X