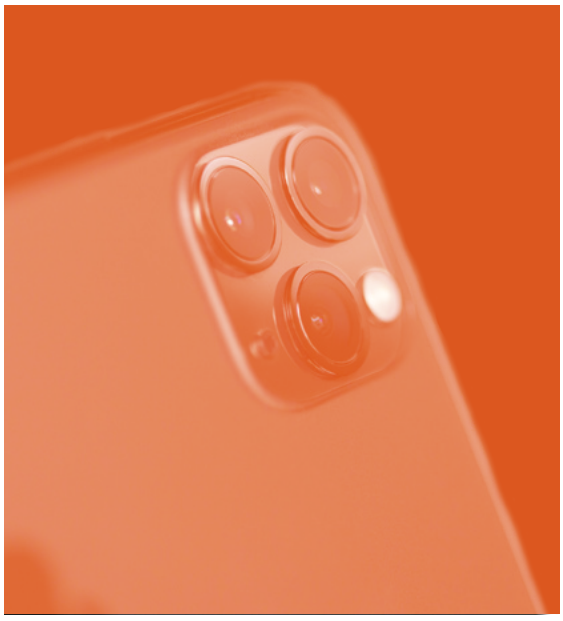
TECHNOLOGY AND COUNTER-TERRORISM

Mapping the impact of biometric surveillance and social media platforms on civic space



A report prepared by:
ECNL - European Center for Not-for-Profit Law

European Center for
Not-for-Profit Law

Programme

This report was prepared as part of the programme on Security and Technology of the European Center for Not-for-Profit Law Stitching (ECNL). It represents the preliminary findings and recommendations of ECNL's working group researching how emerging technologies for AML/CFT are impacting the nonprofit sector.

Acknowledgements

ECNL is grateful to the National Endowment for Democracy for making this report possible and to the institutions, experts, and practitioners who kindly shared their insights with ECNL. In particular, we thank the following organizations and experts for their contributions:

Forum Asia
Al-Hayat -RASED
Defenders Protection Initiative
Third Sector Foundation of Turkey, TUSEV
Centre for Democracy and Rule of Law, CEDEM
UnidOSC
Amber Sinha

Disclaimers

The information contained in this report is true and accurate to the best of the authors' and ECNL's knowledge and ability. The authors made every effort to ensure the accuracy of this publication but cannot be held liable for any loss or damage (direct or indirect), however caused, arising in any way from any information or recommendations contained in this report.

November 2022

European Center for
Not-for-Profit Law

European Center for Not-for-Profit Law Stichting
5 Riviervismarkt
2513 AM, The Hague
Netherlands

Table of Contents

Introduction

Since 9/11, the operating space for civil society has been under pressure in part due to counter-terrorism/financing, anti-money laundering, national security laws, and narratives. Poor design of, or an intentional misuse of counter-terrorism related laws and measures, has resulted in restrictions on human rights, including the rights to association, assembly, expression, privacy, and participation and in criminalisation of activists. Most recently, this trend was amplified by emergency-related regulations enacted to respond to the Covid-19 pandemic. [1]

Increasingly, counter-terrorism programs and initiatives use technology broadly for surveillance, tracking, and prediction. As a result, a person's movements, behaviours, and social networks may be monitored in the hopes of detecting future terrorist activity. Law-abiding individuals and civic actors are often caught in the surveillance dragnet.

This may well be inadvertent and unintentional. However, even when governments do not intend to abuse or maliciously use counter-terrorism technology against individuals in society, the mere existence of surveillance technologies can have a chilling effect on legitimate political expression and civic engagement. Indeed, intrusive technologies such as surveillance can "create an environment of suspicion and threat, which can cause people who are not engaged in any wrongdoing to change their behaviour, including the way they act, speak and communicate."[2]
"idespread data collection and biometrics can enable the targeting of protesters, activists, and human rights defenders, especially those from vulnerable and marginalised groups.[3]

Governments now also use emerging technology and artificial intelligence (AI) systems to detect potential cases of terrorist financing and money laundering. However, in practice, predictive analytics tools can be misused or abused to monitor civil society's activities and financial transactions.

1 See for example various reports on the topic by the UN Special Rapporteur on human rights in counter-terrorism https://www.ohchr.org/en/documents-listing?field_content_category_target_id%5B186%5D=186&field_entity_target_id%5B1283%5D=1283 or Statement by UN Secretary General António Guterres https://www.un.org/sg/en/content/sg/statement/2022-05-10/secretary-generals-video-message-the-high-level-conference-human-rights-civil-society-and-counter-terrorism

2 Privacy International, Protest Surveillance: https://privacyinternational.org/learn/protest-surveillance See also: ECNL. "Peaceful Assemblies and Facial Recognition Technology: International Standards," 2021.

3 ECNL Surveillance Learning Package https://learningcenter.ecnl.org/learning-package/surveillance-technology

Global bodies, such as the Financial Action Task Force[4] or the UN[5], are now focusing on how technology can be used to facilitate terrorism, and how it could potentially prevent it. However, some of their measures may instead amplify the negative impacts we already see on civic space. What's more, there are no guarantees or strong safeguards to be integrated in the design and deployment of such technologies that could limit negative impacts on human rights and civic space. For these reasons, more scrutiny and safeguards are urgently needed if technology and AI is to be used in the counter-terrorism and national security contexts. Relatedly, more research is needed to identify how such use impacts civic space, through meaningful engagement with external stakeholders.

ECNL launched this initial mapping in partnership with the researchers and organisations from the Centre for Internet and Society (India), Hayat-RASED (Jordan), UnidOSC (Mexico), FORUM-ASIA (Thailand), TUSEV (Türkiye), Defenders Protection Initiative (Uganda), and CEDEM (Ukraine). Our aim was to investigate how technologies introduced in the name of counter-terrorism impact or could impact civic space and civil liberties, to identify cross-country trends and identify gaps that can guide further research and action.

About the research

The scope of this study and the overarching research questions were initially developed by ECNL[6] in collaboration with the research partners from the national organisations in the seven countries.[7] Countries were chosen based on reported issues with both counter-terrorism measures and the use of technology, and with consideration of countries where the impacts of technology in the context of counter-terrorism puts civil society at elevated risk of harm, including severe human rights abuses. All partners agreed on a list of questions to guide their research efforts (see Annex 2).

4 https://www.fatf-gafi.org/about/

5 https://www.un.org/counterterrorism/about

6 ECNL team included: Katerina Hadzi-Miceva Evans (Executive Director), Vanja Skoric (Program Director), Emily Lawton (Project and Communications Assistant). ECNL's consultant Ms. Marlena Wisniak contributed subject matter expertise on content governance and social media platforms, and supported the problem framing, research direction of the project and guidance to partners, as well as editing the final draft. ECNL's consultant Ms. Nina Dewi Toft Djanegara provided subject matter expertise on biometrics, analysed the country reports, and drafted the initial text of this document.

7 Centre for Internet and Society (India), Hayat-RASED (Jordan), UnidOSC (Mexico), FORUM-ASIA (Thailand), TUSEV (Türkiye), Defenders Protection Initiative (Uganda), and CEDEM (Ukraine).

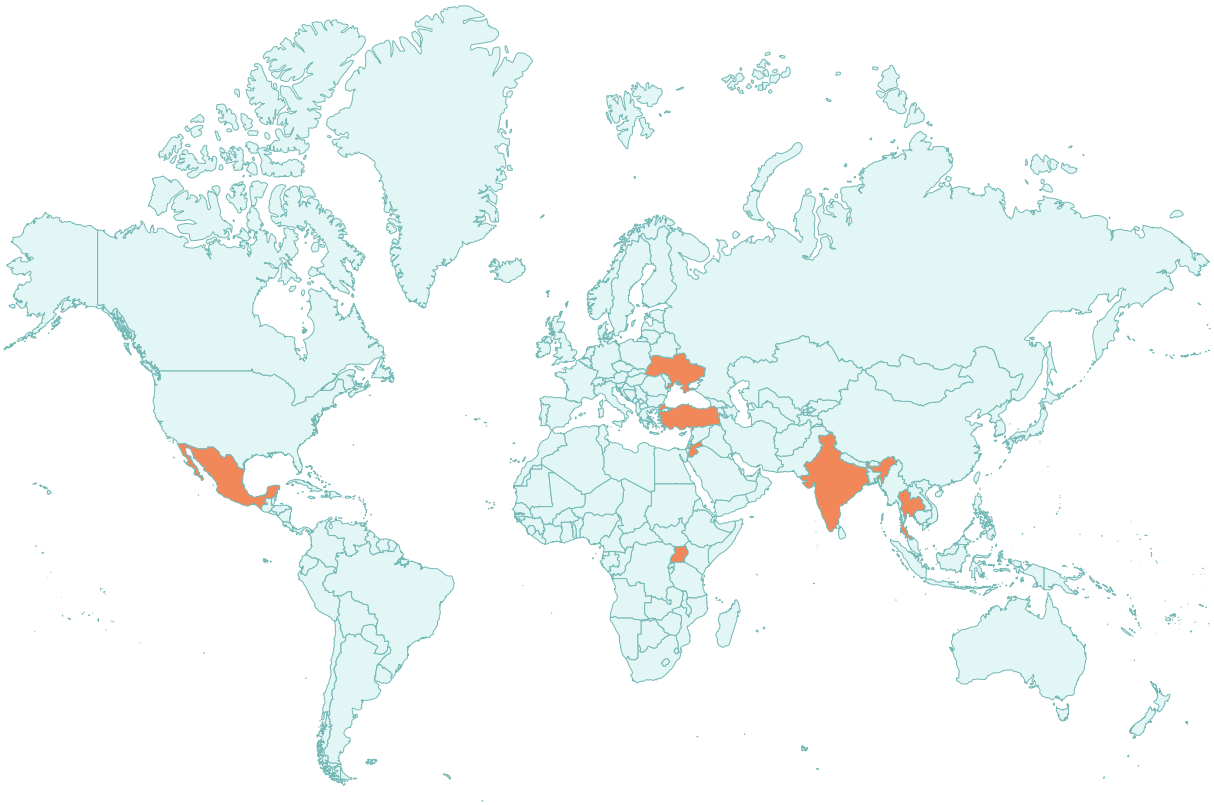


Figure 1. Countries featured in this report

Project scope

A wide range of technologies are deployed today in the pursuit of countering terrorism. These include, but are not limited to, surveillance cameras, predictive algorithms, mobile device trackers, augmented reality devices, millimetre wave body scanners, spyware, and drones. This report explores two major digital technologies that are commonly used in counter-terrorism efforts: biometric identification technologies and algorithmic-driven social media platforms.

Biometric identification technologies include facial recognition, fingerprint verification, and ocular scanning, among others. In the counter-terrorism context, the use of biometric technologies is justified by the claim that they can find and identify perpetrators of terrorist offences. While there is little to no evidence supporting these claims, this report shows how these technologies can, however, be used to the detriment of ordinary citizens, with disproportionate impact to civil society organisations (CSOs), activists, human rights defenders, and political dissidents.

Content moderation refers to the processes by which social media companies handle information that is posted on their platforms. In the counter-terrorism context, the partners of this research assert that there have been concerted efforts by companies and governments to identify and remove content that promotes and/or abets terrorism. The research partners also discovered that over-enforcement of policies pertaining to terrorist content or violent organisations has inadvertently resulted in the suppression of legitimate content, especially content shared by members of marginalised and vulnerable groups, such as Muslim and Arabic-speaking users[8]. Intentional or not, content exposing human rights abuses or criticizing powerful actors can be erroneously flagged as violative, and thus removed[9].

ECNL chose to focus on issues related to biometric surveillance technologies and content moderation of social media platforms because they are already widely operational in many national contexts and are highly likely to have salient human rights impacts on civil society representatives and activities. The format and scope of these technologies means that they are deployed broadly, therefore posing a particular threat to the public, including activists, journalists, human rights defenders, and CSOs. Furthermore, they were both specifically highlighted by Ms Fionnuala Ní Aoláin, the UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, in a statement about upholding human rights while countering terrorism[10]

After the specific technologies were selected, our research was guided by the following broad questions:

- What is the status of biometric technologies and social media platforms, especially online content moderation, in the participating countries?
- Are there any short-term plans to introduce or expand such technologies?
- What are the known impacts on civil society and human rights?

8 Case Study Jordan: Section Unique aspects of the local surveillance landscape ; Case Study Türkiye: Section Unique aspects of the local surveillance landscape

9 Allison-Hope, D., Andersen, L. and Morgan, S. (2021). Human Rights Assessment: Global Internet Forum to Counter Terrorism. BSR. https://gifct.org/wp-content/uploads/2021/07/BSR_GIFCT_HRIA.pdf

10 Ní Aoláin, Fionnuala. "Technology, Counterterrorism and Human Rights: An Overview from the Special Rapporteur." Presented at the Upholding human rights and promoting gender responsiveness while countering terrorism in the age of transformative technologies, New York, June 29, 2021. https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/210729_session_iii_professor_ni_aolain_statement.pdf

- What are the potential impacts on civil society and human rights based on local expertise about the political landscape in the participating countries?
- What kinds of mechanisms exist for CSOs to challenge surveillance technologies and/or suppression of speech online?

An extended list of research questions is included in Annex 2.

Methodology

The methodology for this study included:

- Desk research and analysis of policy documents, media reports, and white papers, among others;
- A questionnaire sent to research partners to guide the development of the research questions;
- A working meeting with research partners to increase their understanding of relevant issues, the project scope, and agree on research questions;
- National level research conducted by research partners;
- Summary and analysis of reports submitted by research partners[11];
- Discussions and review of key findings and trends across countries during meetings of the project team.

Trends subject to the analysis

The purpose of this scoping study was to map global trends in the use of emerging technologies for counter-terrorism purposes, with a particular focus on algorithmic-driven biometric surveillance and content moderation of social media platforms, and to identify the impact of this technology and counter-terrorism intersection on civic space.

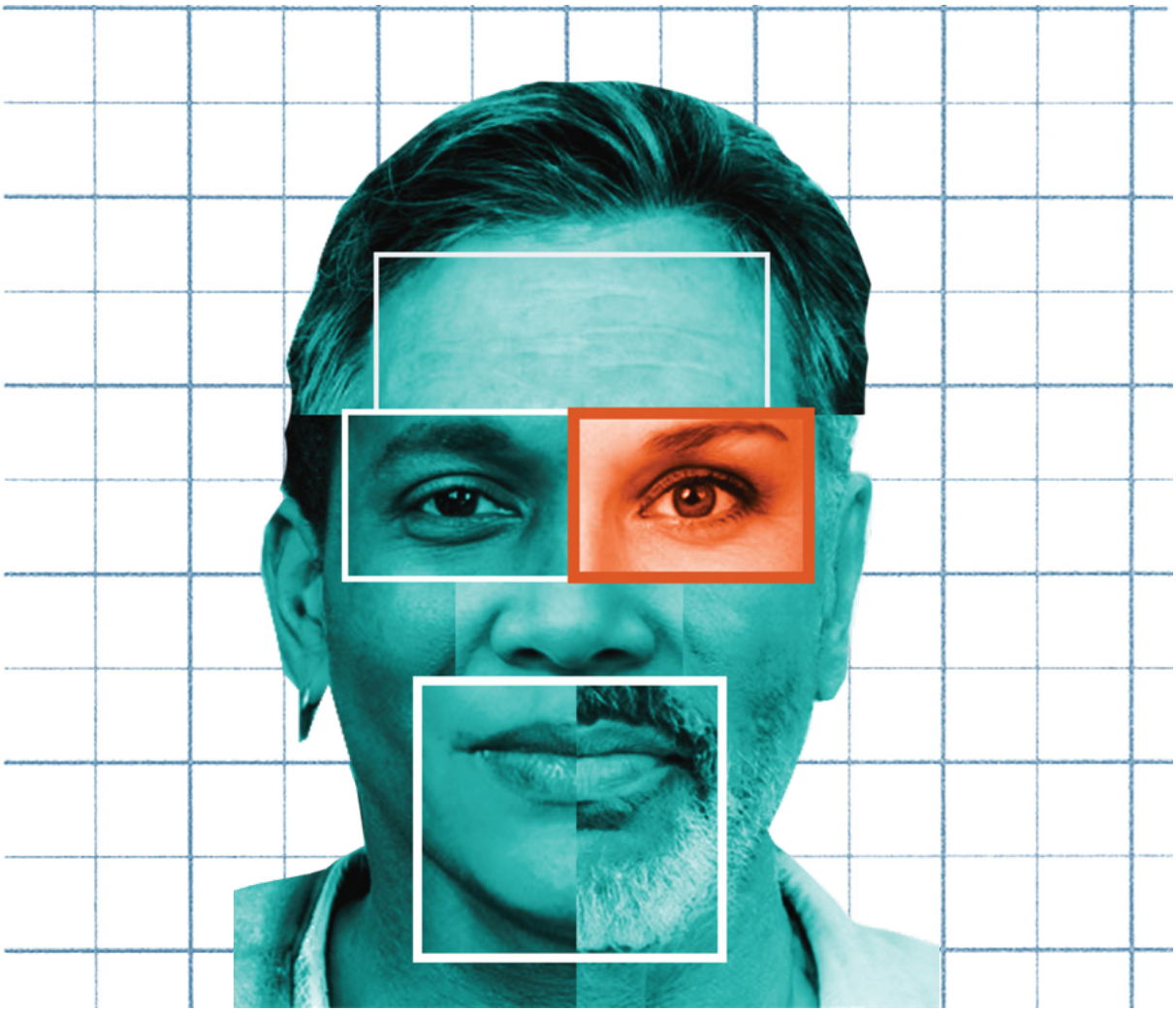
An analysis of the reports submitted by the partner organisations revealed 9 areas related to the use of technology for counter-terrorism that cut across national boundaries and impact civic space:

1. National identity databases
2. Biometric border control

11 ECNL did not independently validate the findings of the partners but relied on their reports.

3. International funding for biometrics development
4. Biometric surveillance of protests
5. Biometrics and mobile phone registration
6. Biometrics and financial services
7. Data disclosure to law enforcement by private companies
8. Suppression of activist content via pressure on private companies
9. Struggles between governments and social media platforms.

This report summarises and contextualises these major trends across the participating countries. More specific information about the current local surveillance and information landscape is provided in each country case study, based on the research conducted by partners. We conclude by discussing that technologies, even when not yet operational and/or existent in many of the surveyed countries, remain areas of concern due to their foreseeable deployment.



Conceptual Overview

What are biometric identification technologies and how are they used for counter-terrorism?

Biometric identification technologies refer to the measurement and recording of physical properties of the body and/or behavioural traits such as voice or gait for the purposes of identification. Algorithmic-driven biometric identification systems use sensors to scan bodies and apply pattern recognition algorithms to convert unique bodily features into binary code. This code can then be stored within a database and/or transmitted across computer networks. Put simply, within a biometric identification system, "bodies function as passwords."[12] Because biometric sensors enable linkages between a person's physical body and data profiles (which may contain information on past behaviour or projections based on predictive algorithms), this technology blurs the boundaries between the physical and the digital.

Biometric technologies such as fingerprint imaging, iris scanning, and facial recognition are used to identify, catalogue, and verify individuals, particularly in the context of national security. The use of biometrics-based technologies for counter-terrorism includes terrorist watchlists linked to biometric data, the collection of biometrics at border entry and exit points, the issuance of e-passports, and digital forensics.

While these technologies have been operational since the 1990s, they have been increasingly used for counter-terrorism purposes after the string of terrorist attacks that occurred in the United States on September 11, 2001. Following the events of September 11, the fight against terrorism was framed as a question of identity management.[13] U.S. politician Dianne Feinstein explained the security rationale used to justify the deployment of biometrics-based technology as follows:

> *"How could a large group of coordinated terrorists operate for more than a year in the United States without being detected and then get on four different*

12 Aas, K. F. "'The Body Does Not Lie': Identity, Risk and Trust in Technoculture." Crime, Media, Culture 2, no. 2 (August 1, 2006): 143–58. https://doi.org/10.1177/1741659006065401

13 Muller, Benjamin J. "(Dis)Qualified Bodies: Securitization, Citizenship and 'Identity Management.'" Citizenship Studies 8, no. 3 (September 2004): 279–94. https://doi.org/10.1080/1362102042000257005; see also Toft Djanegara, Nina. "How 9/11 Birthed America's Biometrics Security Empire." Fast Company, September 10, 2021. https://www.fastcompany.com/90674661/how-9-11-sparked-the-rise-of-americas-biometrics-security-empire

airliners in a single morning without being stopped? The answer to this question is that we could not identify them [...] And the biometrics technology, the state-of-the-art technology of today, really offers us a very new way to identify potential terrorists."[14]

Today, the usage of biometrics technologies for counter-terrorism has been adopted by national governments around the world. A 2021 report by the United Nations Security Council's Counter-Terrorism Committee Executive Directorate (CTED) found that 118 of the UN's 193 member states have introduced biometrics-based systems for counter-terrorism purposes.[15] The report also noted the increasing use of biometric data in new physical and digital domains, such as social media and public space, while marginally recognising the challenges that biometric systems present to human rights.[16]

The rapid uptake of biometric systems for counter-terrorism is due in large part to UN Security Council Resolution 2396, adopted in 2017, which obliged member states to "develop and implement systems to collect biometric data [...] in order to responsibly and properly identify terrorists, including foreign terrorist fighters."[17] Building on Resolution 2322, the 2016 agreement called on member states to share "information about foreign terrorist fighters and other individual terrorists and terrorist organizations, including biometric and biographic information."[18]

In addition to national security and counter-terrorism purposes, national governments are increasingly deploying biometric technologies for administering civil affairs, such as national ID cards, voter registration, distribution of welfare benefits, personnel management, and payroll, among others. Meanwhile, biometric identification systems have also found applications in banking, commerce, mobile phones, and other electronic devices, often under the logic of enhancing personal security and increasing user convenience. In other words, **the same technology has been mobilised for both counter-terrorism purposes and more mundane affairs.**

However, 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

14 Biometric Identifiers and the Modern Face of Terror: New Technologies in the Global War on Terrorism, § Subcommittee on Technology, Terrorism, and Government Information of the Committee on the Judiciary, United States Senate (2001). https://www.govinfo.gov/content/pkg/CHRG-107shrg81678/pdf/CHRG-107shrg81678.pdf.

15 United Nations Security Council Counter-Terrorism Committee Executive Directorate (CTED). "CTED Analytical Brief: Biometrics and Counter-Terrorism," December 10, 2021. https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Dec/cted_analytical_brief_biometrics_0.pdf.

16 Ibid.

17 United Nations Security Council. Resolution 2396, Pub. L. No. S/RES/2396 (2017). https://undocs.org/S/RES/2396(2017).

18 United Nations Security Council. Resolution 2322, Pub. L. No. S/RES/2322 (2016). https://undocs.org/S/RES/2322(2016).

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."[19] We have seen various examples of function creep in our investigation of biometrics and civic space in global policy and in the case studies included in this report.

For example, in its *Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism*, the United Nations Office of Counter-Terrorism (UN OCT) endorsed a strategy for "preventing terrorist attacks before they occur by using biometrics from the widest range of sources pro-actively together."[20] This predictive approach relies on interoperable databases, i.e. the collection and integration of multiple sources of biometric data, many of them drawn from civil registries (see Figure 2). In other words, the UN OCT has advised member states to consolidate biometric data from across branches of government with the aim of anticipating and preventing future terrorist activity. This is a quintessential example of function creep, as data gathered for one objective is later repurposed for another, in this case counter-terrorism.

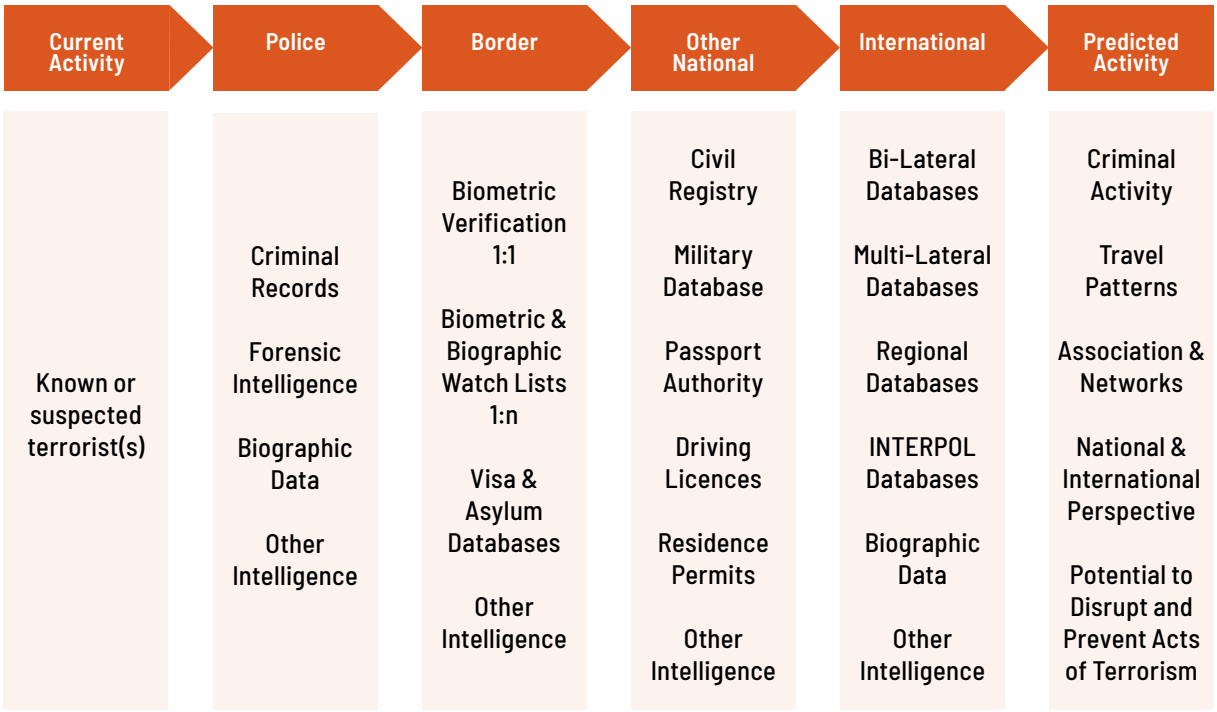


Figure 2. "Predictive Biometrics: The Proactive Use of Biometric Database Networks to Prevent Terrorist Attacks."

19 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.

20 United Nations Office of Counter-Terrorism. "Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism," June 2018. https://www.un.org/securitycouncil/ctc/content/un-compendium-recommended-practices-responsible-use-and-sharing-biometrics-counter-0

The chart in Figure 2 from the *UN Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism* illustrates how the UN-recommended approach links different databases together with the aim of predicting terrorist activity.[21]

The overall trend points to the unscrupulous collection of more and more biometric data with the assumption that it could hypothetically help identify terrorists at some unspecified future date. As stated by U.S. intelligence agents: "Even if biometric data does not have immediate value, it is stored for future use. That way, it can be accessed and compared or analysed whenever necessary to support intelligence activities."[22] This kind of widespread collection and integration of biometric databases is often executed without due consideration of human rights law or data protection standards.[23]

> Due to the growing development of interoperable databases, our investigation highlights a range of biometric data collection efforts. In some countries, biometric data gathering is explicitly linked to counter-terrorism.[24] In others, biometric databases are not necessarily built with counter-terrorism in mind,[25] but there is a possibility that they could be repurposed in the future.[26]

In a 2021 statement, Ní Aoláin cautioned that biometrics-based systems are a particularly concerning technology deployed for counter-terrorism purposes. She observed that the use of biometrics is accelerating in the counter-terrorism context and that its widespread expansion may present enormous impacts to human rights:

> *"[C]onsequences are felt across a range of fundamental rights, including, but not limited to, the rights to life, to liberty and security of person, the right to be free from torture, cruel, inhuman or degrading treatment, the rights to a*

21 United Nations Office of Counter-Terrorism. "Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism," June 2018. https://www.unodc.org/pdf/terrorism/Compendium-Biometrics/Compendium-biometrics-final-version-LATEST_18_JUNE_2018_optimized.pdf.

22 "Biometrics-Enabled Intelligence". Department of Army report. November 2015. https://fas.org/irp/doddir/army/atp2-22-82.pdf Department of Army of what country/ región/ institution? Pdf Link doesn't work.

23 Huszti-Orbán, K.& Ní Aoláin, F. (2020, July). Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?. Human Rights Center, University of Minnesota. https://law.umn.edu/human-rights-center/research/use-biometric-data-identify-terrorists

24 Toft Djanegara, N. (2021, May 28). Biometrics and counter-terrorism: Case study of Iraq and Afghanistan. Privacy International. https://privacyinternational.org/report/4529/biometrics-and-counter-terrorism-case-study-iraq-and-afghanistan ; Weitzberg, K. (2021, May 28). Biometrics and counter-terrorism: Case study of Israel/Palestine. Privacy International. https://privacyinternational.org/report/4527/biometrics-and-counter-terrorism-case-study-israelpalestine

25 E.g. Unique Identification Authority of India, Aadhaar. https://uidai.gov.in/en/

26 Weitzberg, K. (2021, May). BIOMETRICS AND COUNTER-TERRORISM Case study of Somalia. Privacy International. https://privacyinternational.org/sites/default/files/2021-05/PI%20Counterterrorism%20and%20Biometrics%20Report%20Somalia%20v6.1_0.pdf

fair trial, privacy and family life, freedom of expression or movement, etc. It is the scale of impingement, together with the universal, interdependent, and interconnected nature of these rights leading to manifold, interrelated effects across a series of individual and collective freedoms that makes the need for human rights compliant regulation of the use of biometric tools and data an imperative and urgent need."[27]

What is online content governance and how does it relate to counter-terrorism?

Online content governance (generally including content moderation and curation) refers to how content posted on the Internet is processed, particularly content which appears on social media platforms, from large platforms such as Facebook, Twitter, Youtube, or Instagram, to smaller lesser-known ones like Parler, Discord, Happn, Hoop or HOLLA, among many others.

Social media companies regulate the content that is shared on their platforms based on their own internal policies (often referred to as "community standards", rules or guidelines),[28] informed by laws and regulation. Policies range from hate speech, harassment, and misinformation, to terrorist or extremist content, among other categories. Social media companies and governments have been particularly concerned about platforms contributing to or facilitating terrorist and extremist organising and activity through the spread of terrorist-related material online, as such content may be used to radicalise and recruit individuals.[29] For example, Facebook removed 25.9 million pieces of content between January and September 2021, according to its own internal reports, for considering this content terrorist.[30]

27 Ní Aoláin, Fionnuala. "Technology, Counterterrorism and Human Rights: An Overview from the Special Rapporteur." Presented at the Upholding human rights and promoting gender responsiveness while countering terrorism in the age of transformative technologies, New York, June 29, 2021. https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/210729_session_iii_professor_ni_aolain_statement.pdf.

28 Facebook Community Standards https://transparency.fb.com/policies/community-standards/ ; Tiktok Community Guidelines https://www.tiktok.com/community-guidelines?lang=en; ; Instagram Community Guidelines https://help.instagram.com/477434105621119/?helpref=uf_share; Youtube Community Guidelines https://www.youtube.com/howyoutubeworks/policies/community-guidelines/; Twitter rules https://help.twitter.com/en/rules-and-policies/twitter-rules

29 Thompson, Robin. "Radicalization and the Use of Social Media." Journal of Strategic Security 4, no. 4 (December 2011): 167–90. https://doi.org/10.5038/1944-0472.4.4.8.; Huey, Laura. "This Is Not Your Mother's Terrorism: Social Media, Online Radicalization and the Practice of Political Jamming." Journal of Terrorism Research 6, no. 2 (May 25, 2015). https://doi.org/10.15664/jtr.1159.

30 Facebook. "Community Standards Enforcement | Transparency Center." Accessed January 19, 2022. https://transparency.fb.com/data/community-standards-enforcement/.

It is virtually impossible for social media companies to monitor everything posted on their platforms due to the immense scale of content. Therefore, most removed content is either pre-screened by an algorithm (and then either automatically deleted or passed off to a human moderator) and/or reported by users and then adjudicated by a moderator. In some cases, governments may submit a request to social media companies to remove content that they consider potentially terrorist.[31]

Companies use several mechanisms to curb the spread of illegal or policy-violating content:

Content removal

Deleting illegal content or content that violates the platform's terms and services, while leaving the user's account intact.

Deplatforming

Permanently suspending the user's account and preventing them from creating a new account.

Shadow-banning

Reducing the visibility of a user's content or account to a level where the content is de facto removed (often without notifying the user).

In the wake of government pressure to address content that promotes or facilitates terrorism,[32] YouTube, Facebook, Twitter and Microsoft came together in 2016 to establish a common database to share "hashes" – digital fingerprints that contain records about sensitive content.[33] The database allows social media companies to coordinate efforts to remove terrorist-related content; industry partners share "hashes" so that other platforms can automatically detect when content previously removed from one platform is uploaded to another platform. For instance, if Facebook

31 For example: EU Internet Referal Unit flagging terrorist and violent extremist online content and sharing it with relevant partners; Europol. (2022). EU Terrorism Situation and Trend Report (TE-SAT). Europol, https://www.europol.europa.eu/cms/sites/default/files/documents/Tesat_Report_2022_0.pdf & Detecting and requesting removal of internet content used by smuggling networks to attract migrants and refugees: https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/facilitation-of-illegal-immigration

32 "White House Briefing Document for Jan. 12 Counterterrorism Summit With Tech Leaders," January 12, 2016. https://theintercept.com/document/2016/01/20/white-house-briefing-document-for-jan-12-counterterrorism-summit-with-tech-leaders/.

33 Google. "Partnering to Help Curb the Spread of Terrorist Content Online," December 5, 2016. https://blog.google/around-the-globe/google-europe/partnering-help-curb-spread-terrorist-content-online/.

detected a terrorist recruitment video and then added the hash for that video to the shared database, industry partners at Twitter would be able to monitor whether a similar video was uploaded to their platform. The CSO Center for Democracy & Technology expressed its concerns about this database, which it fears will create conditions for censorship across platforms and inhibit freedom of speech because the database could become a "new point of centralized control that governments and others will seek to exploit."[34]

In 2017, the same four tech giants gathered once again to form the Global Internet Forum to Counter Terrorism (GIFCT), which later expanded to include Amazon, LinkedIn, WhatsApp, and others among its members. This consortium has received criticism from civil society groups for its lack of transparency and accountability, insufficient consideration of human rights, targeting of Muslim and Arab users, and for its creation of "an uneven playing field that disadvantages civil society."[35] The 2021 independent human rights assessment of GIFCT confirmed that the organisation "contains some features of a multi-stakeholder initiative (i.e. non-companies actively participate in the work of GIFCT) but lacks others (i.e. decision-making power rests solely with companies)" and emphasised the importance of transparency. [36]

As content policy is primarily self-regulated by platforms, governments have historically had limited ability to restrict or take down content they deem objectionable or illegal[37] – and rightfully so, as the alternative could severely harm users' freedom of expression. However, some government agencies take advantage of platforms' terms of service by flagging policy-violating content and relying on companies to enforce those terms. In other words, instead of requiring content removal by law, they identify content that violates the companies' internal policies related to terrorist and extremist content. They then report it so that companies will voluntarily remove it in compliance with their own terms of service. Such a model for content removal was spearheaded by the UK Counter Terrorism Internet Referral Unit (CTIRU) in 2010.[38] Since then, multiple European states have created their own Internal Referral Units (IRUs).[39] An analysis by the Global Network Initiative and Harvard's Cyber Law Clinic expressed concerns that

34 Llansó, Emma. "Takedown Collaboration by Private Companies Creates Troubling Precedent." Center for Democracy and Technology (blog), December 6, 2016. https://cdt.org/insights/takedown-collaboration-by-private-companies-creates-troubling-precedent/

35 Human Rights Watch. "Joint Letter to New Executive Director, Global Internet Forum to Counter Terrorism," July 30, 2020. https://www.hrw.org/news/2020/07/30/joint-letter-new-executive-director-global-internet-forum-counter-terrorism

36 Allison-Hope, D., Andersen, L. & Morgan, S. (2021). Human Rights Assessment Global Internet Forum to Counter Terrorism. BSR. https://gifct.org/wp-content/uploads/2021/07/BSR_GIFCT_HRIA.pdf

37 E.g. child sexual abuse material and human trafficking/ sex trafficking, as well as other illegal goods & services.

38 Clark, Liat. "UK Gov Wants 'unsavoury' Web Content Censored." Wired UK, March 13, 2014. https://www.wired.co.uk/article/government-web-censorship

39 Europol. (2022, February 23). EU Internet Referal Unit. https://www.europol.europa.eu/about-europol/european-counter-terrorism-centre-ectc/eu-internet-referal-unit-eu-iru

IRUs circumvent conventional legal procedures, operating without transparency and accountability, while failing to enable users to dispute removal decisions.[40]

In the EU, the Terrorist Content Regulation,[41] which entered into effect in June 2022, establishes some transparency requirements for authorities and social media platforms, as well as redress mechanisms for users. However, the extremely short deadline of one hour imposed on social media platforms to act upon removal orders issued by authorities[42] poses a clear risk of over-removal of legitimate content. A coalition of over 75 organisations rightfully condemned this regulation for "forcing platforms to use content filtering, and empowering state authorities to enable censorship."[43]

> Over-broad efforts to remove terrorist content can inadvertently result in the suppression of legitimate content, thereby limiting freedom of expression, and civic engagement and activism. This can disproportionately suppress the speech of users and groups that are already marginalised and vulnerable. Both algorithmic and human-led content moderation includes some subjective (and thus biased) decisions.[44] Given that detailed criteria for content moderation, including enforcement guidelines related to internal policies, are not disclosed, it's difficult to assess the scale and contours of such bias.

Today, content moderation is increasingly automated through algorithmic systems. While such systems can be helpful in moderating content at scale, they have significant limitations.[45] These systems often exacerbate and accelerate existing challenges related to content moderation, not least related to the lack of transparency and understanding of local context. Indeed, algorithmic systems based on keyword

40 Pielemeier, Jason, and Chris Sheehy. "Understanding the Human Rights Risks Associated with Internet Referral Units." Global Network Initiative (blog), February 5, 2019. https://globalnetworkinitiative.org/human-rights-risks-irus-eu/.

41 Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (Text with EEA relevance). (2021, May 17). EUR-lex. https://eur-lex.europa.eu/eli/reg/2021/784/oj

42 Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (Text with EEA relevance). (2021, May 17). Article 3(3). EUR-lex. https://eur-lex.europa.eu/eli/reg/2021/784/o

43 EDRi. (2021, April 29). European Parliament confirms new online censorship powers. EDRi. https://edri.org/our-work/european-parliament-confirms-new-online-censorship-powers/

44 Thakur, D. & Llansó, E. (2021, May 20). Do You See What I See? Capabilities and Limits of Automated Multimedia Content Analysis. Center for Democracy and Technology. https://cdt.org/insights/do-you-see-what-i-see-capabilities-and-limits-of-automated-multimedia-content-analysis/

45 Thakur, D. & Llansó, E. (2021, May 20). Do You See What I See? Capabilities and Limits of Automated Multimedia Content Analysis. Center for Democracy and Technology. https://cdt.org/insights/do-you-see-what-i-see-capabilities-and-limits-of-automated-multimedia-content-analysis/

detection and language models are not able to fully capture the nuance of statements, particularly when it comes to irony or culturally-specific references.[46] This has led to the inadvertent deletion of legitimate speech such as journalism, satire, art, anti-terrorism critique, and documentation of human rights abuses.[47] Additionally, because algorithms can only be trained on known examples, they are biased towards removing certain kinds of content and can be blind to others. Enforcement of content in languages other than English further exacerbates these issues.[48]

The UN Office of Counter-Terrorism (UN OCT) is beginning to take notice of the limitations of automated content moderation. In a 2021 report, the UN OCT stated "a machine learning model trained to find content from one terrorist organization may not work for another because of language and stylistic differences in their propaganda."[49] Additionally, analysts from the CSO Brennan Center for Justice found that content uploaded by Muslim users is disproportionately policed on major social media platforms, in comparison to content in support of white-supremacist organisations.[50] The impact of this uneven enforcement is felt by civil society; for instance, when Facebook suspended the accounts of dozens of Syrian and Palestinian journalists and human rights activists in 2020.[51] An independent human rights assessment of Meta's activities in Israel/Palestine further showed that "a key over-enforcement issue in May 2021 occurred when users accumulated "false" strikes that impacted visibility and engagement after posts were erroneously removed for violating content policies. The human rights impacts of these errors were more severe given a context where rights such as freedom of expression, freedom of association, and safety were of heightened significance, especially for activists and journalists, and given the prominence of more severe [dangerous individuals and organisations] policy

46 Vincent, James. "AI Won't Relieve the Misery of Facebook's Human Moderators." The Verge, February 27, 2019. https://www.theverge.com/2019/2/27/18242724/facebook-moderation-ai-artificial-intelligence-platforms

47 Human Rights Watch. "Joint Letter to New Executive Director, Global Internet Forum to Counter Terrorism," July 30, 2020. https://www.hrw.org/news/2020/07/30/joint-letter-new-executive-director-global-internet-forum-counter-terrorism; see also Al Jaloud, Abdul Rahman, Hadi Al Khatib, Jeff Deutch, Dia Kayyali, and Jillian York. "Caught in the Net: The Impact of 'Extremist' Speech Regulations on Human Rights Content." EFF, May 2019. https://www.eff.org/files/2019/05/30/caught_in_the_net_whitepaper_2019.pdf

48 Nicholas, G. & Aliya Bhatia, A. (2022, August 18). Lost in Translation: Automated Content Analysis in Non-English Languages. Center for Democracy and Technology. https://cdt.org/insights/lost-in-translation-automated-content-analysis-in-non-english-languages/

49 United Nations Office of Counter-Terrorism. "Countering Terrorism Online with Artificial Intelligence," 2021. https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/countering-terrorism-online-with-ai-uncct-unicri-report-web.pdf

50 Diáz, Angel, and Laura Hecht-Felella. "Double Standards in Social Media Content Moderation." Brennan Center for Justice at New York University School of Law, August 4, 2021. https://www.brennancenter.org/sites/default/files/2021-08/Double_Standards_Content_Moderation.pdf

51 Solon, Olivia. "'Facebook Doesn't Care': Activists Say Accounts Removed despite Zuckerberg's Free-Speech Stance." NBC News, June 15, 2020. https://www.nbcnews.com/tech/tech-news/facebook-doesn-t-care-activists-say-accounts-removed-despite-zuckerberg-n1231110

violations. Further, these strikes remain in place for those users that did not appeal erroneous content removals."[52]

Decisions to moderate or curate content online tend to be made opaquely and independently by platforms, without external oversight. While social media platforms offer internal appeals processes to reinstate removed content or blocked accounts, there's limited means of redress for users who believe their content has been unfairly removed or de-amplified in practice. Other types of mechanisms could be helpful for overturning decisions to remove online content because it was unduly deemed as terrorist. For example, the Oversight Board overtured the removal of an Instagram post "encouraging people to discuss the solitary confinement of Abdullah Öcalan, a founding member of the Kurdistan Workers' Party,"[53] as well as the removal of a news report from Al Jazeera which relayed information about threats made by the Palestinian group Hamas.[54] However, this is a limited strategy of redress since the Oversight Board has a limited mandate and currently only exist for Meta. It rarely intervenes; as of November 2022, the Board has only made 41 decisions.[55]

The unfortunate reality is that across social media platforms, only a fraction of appealed content actually gets reviewed, let alone reinstated.[56] Furthermore, the appeals process only allows users to make a complaint based on enforcement of the platform's existing terms of service (and not the content policy itself), despite the fact that experts such as Ní Aoláin questioned social media companies' definitions of controversial terms like "terrorism" and "terrorist organizations."[57]

52 BSR. (2022, September). Human Rights Due Diligence of Meta's Impacts in Israel and Palestine in May 2021 Pg. 5. BSR. https://www.bsr.org/reports/BSR_Meta_Human_Rights_Israel_Palestine_English.pdf

53 Facebook Oversight Board. "Oversight Board Overturns Original Facebook Decision: Case 2021-006-IG-UA | Oversight Board," July 2021. https://oversightboard.com/news/187621913321284-oversight-board-overturns-original-facebook-decision-case-2021-006-ig-ua/.

54 Facebook Oversight Board. "Oversight Board Overturns Original Facebook Decision: Case 2021-009-FB-UA | Oversight Board," September 2021. https://oversightboard.com/news/389395596088473-oversight-board-overturns-original-facebook-decision-case-2021-009-fb-ua/.

55 Oversight Board. (2022, June). Oversight Board publishes first Annual Report. https://www.oversightboard.com/news/322324590080612-oversight-board-publishes-first-annual-report/ ; Meta. Oversight Board Cases. (2022, September 15). https://transparency.fb.com/de-de/oversight/oversight-board-cases/

56 Alexander, J. (2020, April 28). YouTube rarely reinstates removed videos — even when creators appeal. The Verge. https://www.theverge.com/2020/2/28/21157476/youtube-video-removal-appeal-takedown-community-guidelines-report; Meta. (2022, October 4). Appealed Content. https://transparency.fb.com/policies/improving/appealed-content-metric/

57 Ní Aoláin, Fionnuala. "Mandate of the Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism," July 24, 2018. https://www.ohchr.org/Documents/Issues/Terrorism/OL_OTH_46_2018.pdf

What do we mean by terrorism?

There is a lack of globally agreed upon definition of terrorism. Hence what is defined as terrorism has been subject to significant debate, with different organisations and national governments operating under different understandings of terrorism.[58] The act of labelling certain groups as "terrorists" is a normative claim; the line between terrorism and legitimate political violence is not always clear.

The lack of definition and ambiguity over what constitutes terrorism is important to understand when considering the spread of technology for counter-terrorism purposes. As GIFCT notes, "the lack of a globally agreed upon definition of terrorism and the highly politicized context within which counterterrorism takes place have resulted in government overreach." This may lead to the persecution of legitimate political expression.[59] Indeed, as shown in this report, national context and local understanding of what terrorism means have affected the national surveillance and counter-terrorism approach in each of our case studies. For instance, in places such as Mexico, the local interpretation of terrorism is linked to gang activity and organised crime, whereas in Thailand, counter-terrorism efforts are generally focused on the region in the South, where there has been an ongoing conflict with ethno-religious separatists.

No unique definition of terrorism

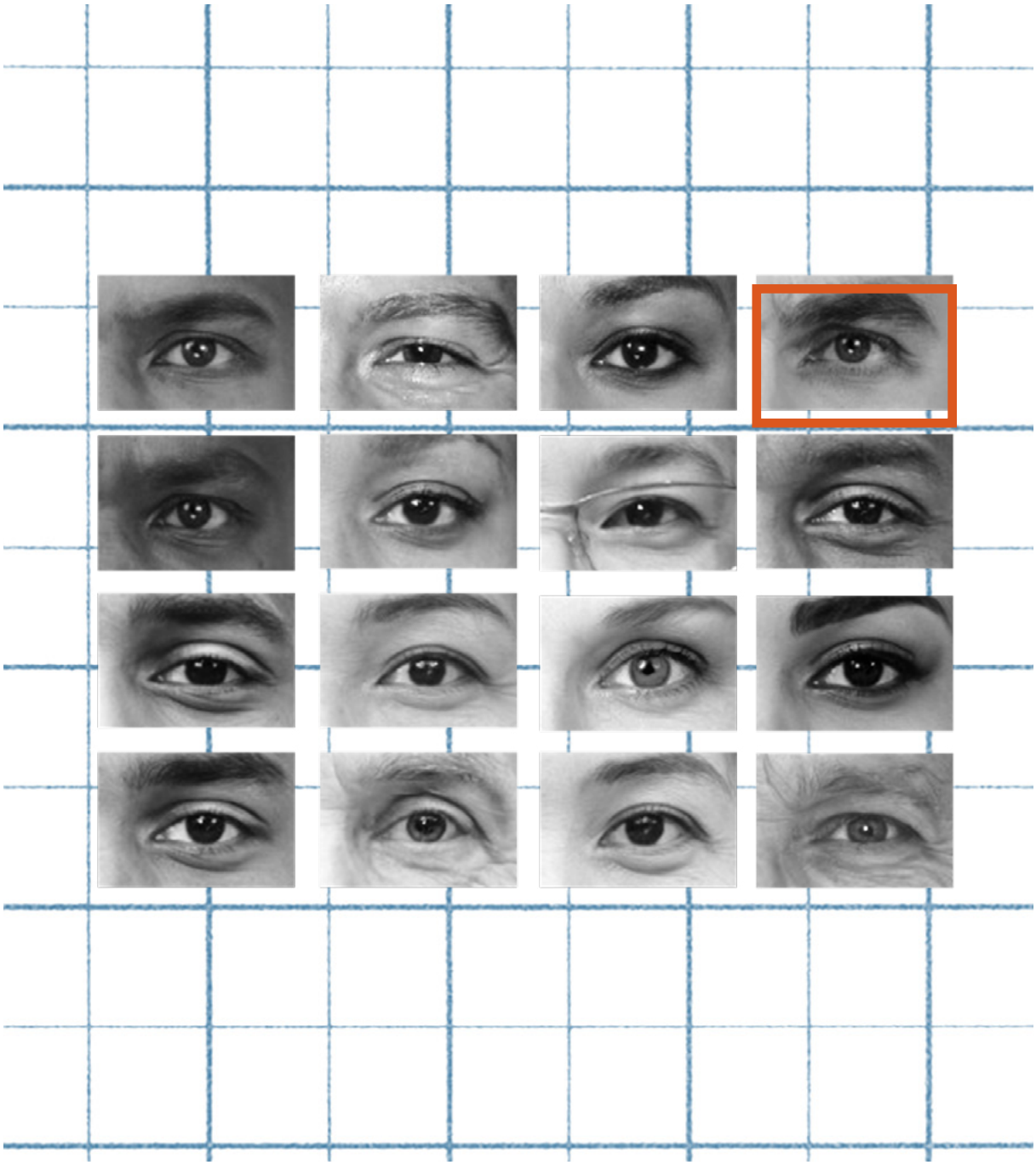
UN Security Council: "[C]riminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organisation to do or to abstain from doing any act."

European Union: Terrorists offenses are those committed with the aim of: "seriously damage a country or an international organisation [which are] committed with the aim of: (i) seriously intimidating a population, or (ii) unduly compelling a Government or international organisation to perform or abstain from

58 Hardy, Keiran, and George Williams. "What Is 'Terrorism'? Assessing Domestic Legal Definitions." UCLA J. Int'l L. Foreign Aff. 16 (2011): 77. https://heinonline.org/HOL/LandingPage?handle=hein.journals/jilfa16&div=7&id=&page=

59 BSR. "Human Rights Assessment: Global Internet Forum to Counter Terrorism," July 2021. https://gifct.org/wp-content/uploads/2021/07/BSR_GIFCT_HRIA.pdf

performing any act, or (iii) seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation."[60]



60 UN Security Council. (2004, October 8). UN Security Council Resolution 1566. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N04/542/82/PDF/N0454282.pdf?OpenElement ; EUR-Lex. (2017, March 15). Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32017L0541

Key Trends in the Use of Technology for Counter-Terrorism

The following key trends were identified through an analysis of national research reports produced by partner organisations in India, Jordan, Mexico, Thailand, Türkiye, Uganda, and Ukraine.

Biometric Surveillance

National identity databases

One of the most common uses of biometrics by governments is the creation of national identity databases, where the biometric and biographic information of all citizens and residents is registered. In their studies, research partners found that national biometric identity databases are in use or development in India,[61] Jordan,[62] Mexico,[63] Thailand,[64] and Ukraine[65], while a similar national ID system was also proposed in Uganda.[66]

61 Case Study India: Section Notable uses of biometric technology

62 Case Study Jordan: Section Notable uses of biometric technology

63 Case Study Mexico: Section Notable uses of biometric technology

64 Case Study Thailand: Section Notable uses of biometric technology

65 Case Study Ukraine: Section Notable uses of biometric technology

66 Case Study Uganda: Section Notable uses of biometric technology

The largest example of this kind of national biometric identification scheme is India's Aadhaar database, which contains the fingerprints, iris scans and facial photos of over 1.3 billion people.[67] These biometric databases are often linked to the provision of social and financial services; for instance, under the Aadhaar program, a registered fingerprint allows Indian citizens to access pensions, basic foodstuffs, and subsidised fuels.[68] Academics have coined this trend "biometric citizenship," referring to how states increasingly require citizens to supply their biometric information in order to claim the basic rights and benefits of citizenship.[69]

National biometric identity systems are not typically motivated by counter-terrorism concerns. However, as seen in the introduction to this report, the UN Office of Counter-Terrorism has recommended that governments draw upon national biometric identity registries to assist in counter-terrorism efforts.[70] Therefore, it is important to monitor the growth of these databases, especially in countries with poor human rights records. Considering that these national identity initiatives aim to enrol all citizens, a national biometrics database could pose a potential risk to human rights defenders and members of civil society. Their digitised biometric data would be readily available for misuse, such as targeting and monitoring them.

Biometric border control

Biometric technologies are generally used by national governments to determine who is eligible to enter their borders and keep track of those who are exiting the country. These systems work by comparing the facial print of a person physically present at the border with biometric information stored in their passport. Biometric verification at the border can either be fully automated, through "e-gates,"[71] or take place in front of a human border agent. When used at national borders, biometric checkpoints are often linked with terrorist watchlists, advance passenger

67 https://uidai.gov.in/aadhaar_dashboard/

68 Sinha, A. et al (2017, February 19). The Centre for Internet & Society, Big Data in Governance in India: Case Studies. https://cis-india.org/internet-governance/files/big-data-compilation.pdf.

69 Breckenridge, Keith. Biometric State: The Global Politics of Identification and Surveillance in South Africa, 1850 to the Present. Cambridge: Cambridge University Press, 2014.

70 UN Security Council. (2017, December 21). UN Security Council 2396. S/RES/2396(2017). https://www.un.org/securitycouncil/content/sres23962017 ; UN Security Council. (2021, December 30). UN Security Council http://unscr.com/en/resolutions/doc/2617

71 Labati, Ruggero Donida, Angelo Genovese, Enrique Muñoz, Vincenzo Piuri, Fabio Scotti, and Gianluca Sforza. "Advanced Design of Automated Border Control Gates: Biometric System Techniques and Research Trends." In 2015 IEEE International Symposium on Systems Engineering (ISSE), 412–19, 2015. https://doi.org/10.1109/SysEng.2015.7302791.

information (API) systems, and passenger name record (PNR) data, all of which provide biographical information about travellers.[72]

The proliferation of biometric border control systems is due, in part, to funding and support by international donors. The United States government, for example, has financed the construction of biometric border control systems in Afghanistan, Burkina Faso, Cameroon, Chad, Djibouti, Ethiopia, Iraq, Jordan, Kenya, Maldives, Mali, Niger, North Macedonia, Tanzania, Uganda, and Yemen,[73] with the justification that such programs enable "foreign partners to better protect their own borders and prevent terrorist travel, including travel that poses threats to the safety and security of the United States."[74] The use of biometric border technology has been reported in airports

72 Huszti-Orbán, Krisztina, and Fionnuala Ní Aoláin. "Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?" University of Minnesota Human Rights Center, 2020. https://www.ohchr.org/Documents/Issues/Terrorism/biometricsreport.pdf.

73 Privacy International. "Briefing to the UN Counter-Terrorism Executive Directorate on the Responsible Use and Sharing of Biometric Data to Tackle Terrorism," June 2019. https://privacyinternational.org/sites/default/files/2019-07/PI%20briefing%20on%20biometrics%20final.pdf.

74 White House. "National Strategy to Combat Terrorist Travel," December 2018. https://www.hsdl.org/?view&did=821737.

in Jordan,[75] Mexico,[76] India,[77] Ukraine,[78] Thailand,[79] and Uganda,[80] while in Türkiye[81] biometrics are used to register immigrants and refugees.

The use of biometric systems to enforce national borders could pose a threat to civil society members, whose movements might be tracked or who might be prevented from traveling. For example, the Belarussian activist Roman Protasevich was intercepted on a commercial flight after his name was added to a list of "individuals involved in terrorist activity."[82] While our research partners could not identify definitive instances when CSO members were apprehended at the border in connection with biometrics and/or terrorist watchlists in their countries, such cases are often opaque and the lack of information does not necessarily mean that border detentions and apprehensions are not occurring in practice.

International funding for biometrics development

In Resolution 2396, the UN Security Council "calls upon other Member States, international, regional, and sub-regional entities to provide technical assistance, resources, and capacity building to Member States in order to implement such systems [to collect biometric information]."[83] International powers like the European Union have enthusiastically taken up this call, for instance by granting €60 million to

75 Diplomatic Note. (2021, June 16). United States Mission Organization for Security and Cooperation in Europe. Account of measures to prevent and combat terrorism. OSCE Secretariat https://www.osce.org/files/f/documents/a/2/490781.pdf

76 Burt, C. (2018, April 12). SITA biometric border control kiosks deployed in Mexico. Biometric Update. https://www.biometricupdate.com/201804/sita-biometric-border-control-kiosks-deployed-in-mexico

77 Choi, T. (2022, April 26). India moves to ease biometric registration for air and cruise travel in wake of COVID-19. Biometric Update. https://www.biometricupdate.com/202204/india-moves-to-ease-biometric-registration-for-air-and-cruise-travel-in-wake-of-covid-19; Pandit, R. (2022, August 7). India Times. Army Steps up deployment of AI powered surveillance systems on borders with China and Pakistan. https://timesofindia.indiatimes.com/india/army-steps-up-deployment-of-ai-powered-surveillance-systems-on-borders-with-china-pakistan/articleshow/93402906.cms;

78 Mayhew, S. (2018, January 3). Ukrainian border guards collecting biometric data from international travelers. Biometric Update. https://www.biometricupdate.com/201801/ukrainian-border-guards-collecting-biometric-data-from-international-travelers

79 Pascu, L. (2020, February 13). Thailand pilots Dermalog's biometric border control solution with fever detection. Biometric Update. https://www.biometricupdate.com/202002/thailand-pilots-dermalogs-biometric-border-control-solution-with-fever-detection

80 Mayhew, S. (2019, January 14). Gemalto wins contract for biometric border management system in Uganda. Biometric Update. https://www.biometricupdate.com/201901/gemalto-wins-contract-for-biometric-border-management-system-in-uganda

81 Hersey, F. (2021, October 29). Biometrics use in Türkiye expands from migration system to ATMs. Biometric Update. com. https://www.icisleri.gov.tr/55-milyon-parmak-izi-milli-sistemde, https://www.biometricupdate.com/202110/biometrics-use-in-Türkiye-expands-from-migration-system-to-atms

82 Smith, Alexander, and Yuliya Talmazan. "Who Is Belarusian Dissident Journalist Roman Protasevich?" NBC News, May 26, 2021. https://www.nbcnews.com/news/world/who-roman-protasevich-why-fighter-jet-belarus-intercepted-his-flight-n1268614.

83 United Nations Security Council. Resolution 2396, Pub. L. No. S/RES/2396 (2017). https://undocs.org/S/RES/2396(2017).

the governments of Senegal and Côte d'Ivoire to create national biometric identity registries.[84] Our research partners in Jordan[85] identified evidence of international funding from the United States. In Uganda,[86] technology from China and Russia was extended to the government, while some municipalities in Mexico[87] use facial recognition software developed by a Chinese company that has been accused of targeting Uyghurs, an ethnic minority group.[88]

Within a climate where international bodies are actively encouraging and funding the spread of biometric technology,[89] it is especially critical to consider the potential dangers of introducing this technology to countries whose governments may repurpose biometric data against their citizens or use the pretext of counter-terrorism to suppress legitimate political expression and dissent. Given the risks associated with these technologies, **international organisations should be particularly cautious about exporting them to states with weak rule of law, where there is a higher risk that they may be misused or abused, or to governments with known histories of human rights infractions. International funding must be tied to human rights safeguards and due diligence process of granting, monitoring, and reporting of its use**.

Biometric surveillance of protestors

One of the most concerning trends identified by our research partners is the use of biometrics for surveilling protestors and dissidents. Reports from India,[90] Mexico,[91] Türkiye,[92] and Uganda[93] indicate that facial recognition has been used in connection with at least one political protest. In addition, our research partnets from Thailand[94] and Ukraine[95] noted that politicians have proposed the use of facial recognition for monitoring protests, though it is unclear whether those claims have been acted upon. Facial recognition is sometimes applied real-time, though it is often done retroactively

84 Creta, Sara. "EU Funds for African IDs: Migration Regulation Tool or Data Risk?" euronews, July 30, 2021. https://www.euronews.com/2021/07/30/european-funds-for-african-ids-migration-regulation-tool-or-privacy-risk.

85 Case Study Jordan: Section Notable uses of biometric technology

86 Case Study Uganda: Section Data-sharing between private companies and the state

87 Case Study Mexico: Section Notable uses of biometric technology

88 Villoror, P, F. & Robles, P. (2020, November 11). Biometric surveillance: Coahuila's tortuous path to facial. Quinto Elemento. recognition. https://quintoelab.org/project/vigilancia-biometrica-reconocimiento-facial-coahuila

89 UN Security Council. (2017, December 21). Un security council resolution 2396. https://www.un.org/securitycouncil/content/sres23962017 ; UN Security Council. (2021, December 30). UN Security Council Resolution 2617. https://documents-dds-ny.un.org/doc/UNDOC/GEN/N21/424/08/PDF/N2142408.pdf?OpenElement

90 Case Study India: Section Notable uses of biometric technology

91 Case Study Mexico: Section Notable uses of biometric technology

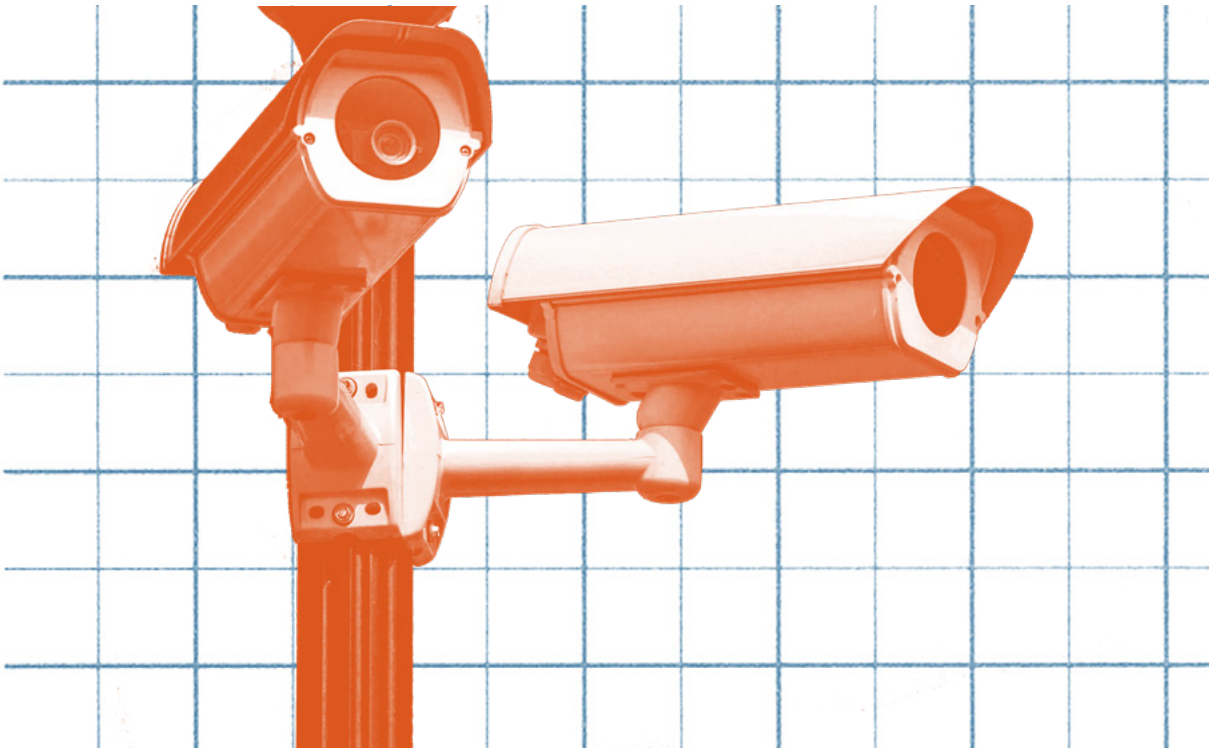
92 Case Study Türkiye: Section Notable uses of biometric technology

93 Uganda Case Study: Section Notable uses of biometric technology

94 Case Study Thailand: Section Notable uses of biometric technology

95 Case Study Ukraine: Section Notable uses of biometric technology

to identify people who appear in video footage after the event. Since photos and videos can be analysed remotely or after-the-fact by facial recognition algorithms, protestors and activists may be unaware if their arrest was linked to a facial recognition system. Furthermore, because facial recognition can be applied to old video footage, this poses a potential risk for CSO members in countries where there is widespread CCTV camera recording, even if those countries do not currently have facial recognition capabilities.



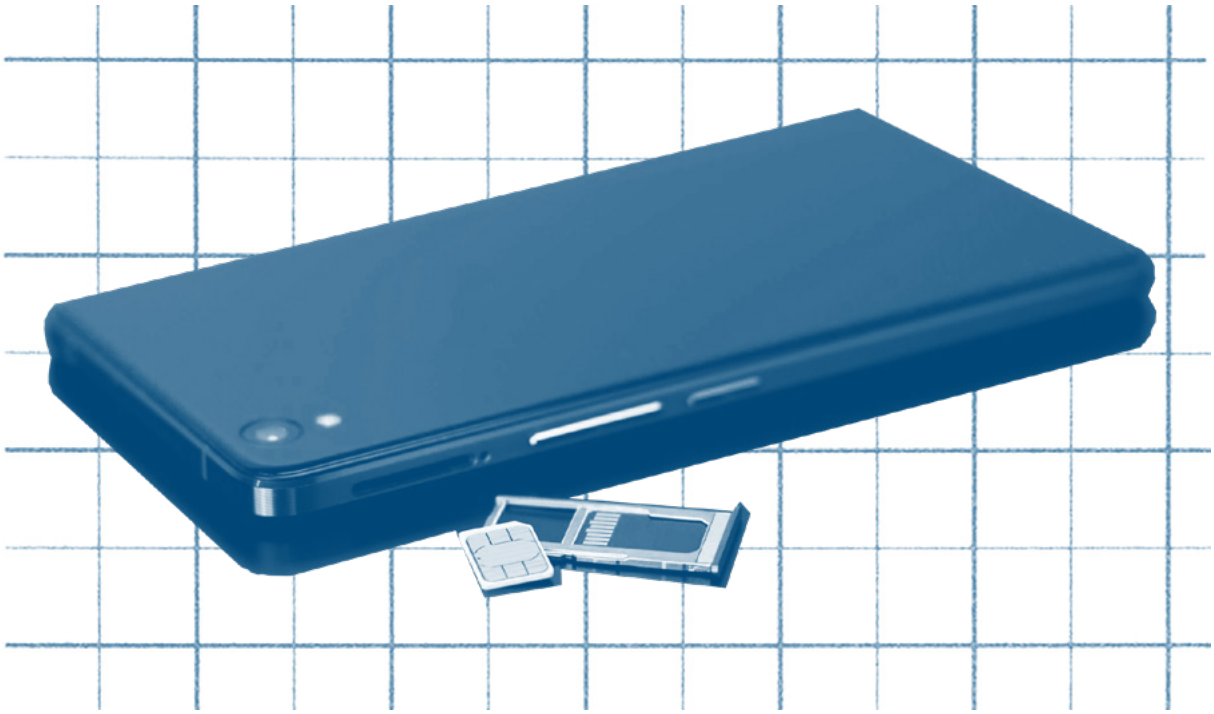
The use of facial recognition to identify protestors represents an enormous risk to CSO members' rights to privacy, freedom of expression, and freedom of assembly and association, among other rights. Even in the case where people fear that facial recognition might be used against protestors, this potential threat could be enough to provide a chilling effect on political expression and people's willingness to engage in public protest.[96] For instance, in his research on the surveillance of the Uyghur population, anthropologist Darren Boyler cautioned that an AI-driven facial recognition system "cannot keep up with the faces of all the jaywalkers" nevertheless "it is the threat of surveillance, rather than the surveillance itself, that causes people to modify their behaviour."[97]

96 FRA. (2019).Facial recognition technology: fundamental rights considerations in the context of law enforcement. https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-facial-recognition-technology-focus-paper-1_en.pdf; Privacy International. (n.d.). Protest Surveillance. Privacy International. https://privacyinternational.org/learn/protest-surveillance

97 Byler, Darren. "Ghost World." Logic Magazine, May 1, 2019. https://logicmag.io/china/ghost-world/.

Biometrics and mobile phone registration

In countries like Thailand[98] and Uganda[99], a person must register their biometric information to obtain a mobile phone connection or SIM card. A similar obligation existed in Mexico, until it was ruled unconstitutional by the country's Supreme Court in April 2022.[100] The rationale for registration is often explicitly linked to counter-terrorism. In Mexico, authorities claimed that biometric registration for mobile phones was necessary to fight against gangs and organised crime.[101] In Thailand, the government alleges that SIM cards are used by terrorists to detonate bombs.[102] **Mandatory biometric registration for obtaining a mobile phone number is a new but expanding global trend, particularly in countries with poor human rights records**



98 Case Study Thailand: Section Notable uses of biometric technology

99 Karanicolas, M. (2019, November 8). Yale Law School. Serious Concerns Around Uganda's National Biometric ID Program https://law.yale.edu/isp/initiatives/wikimedia-initiative-intermediaries-and-information/wiii-blog/serious-concerns-around-ugandas-national-biometric-id-program

100 The Supreme court on April 22th, 2022 decided that the Biometric Data Base of Mobile Phone Users (PANAUT in Spanish) was unconstitutional because it violates the right to privacy, the regulation has therefore been canceled. https://www.debate.com.mx/politica/Suprema-Corte-declara-al-Panaut-inconstitucional-va-contra-el-derecho-a-la-privacidad-20220427-0061.html

101 Anonymous. (2009, Feburary 9). Mexico to fingerprint phone users in crime fight. Reuters. https://www.reuters.com/article/idUSN09529514

102 Anonymous. (2017, May 25). Thailand to require biometric checks for pre-paid SIM cards in troubled south. Reuters. https://www.reuters.com/article/us-thailand-telecoms-idUSKBN18L1R2

and/or weak rule of law.[103] Along with Thailand and Uganda, biometric registration is required for mobile phone access in Afghanistan, Bahrain, Bangladesh, Benin, China, United Arab Emirates, Mozambique, Nigeria, Oman, Pakistan, Peru, Saudi Arabia, Singapore, Tanzania, Tajikistan, and Venezuela.[104]

Privacy International, a digital rights organisation, cautions that mobile SIM card registration creates significant risks to individual privacy, free expression, and freedom of movement, since this information would allow state authorities to "identify the owner of a SIM card and infer who is likely to be making a call, sending a message, in a particular location at any particular time, or making a particular financial transaction through a money transfer app."[105] For example, Mexican digital rights activist Luis Fernando García warns, "It's not unreasonable to fear that the information provided to the [mobile phone biometric] database would end up being used by this administration [in Mexico] or by future administrations that are not committed to human rights at all."[106]

Biometrics and financial services

In India[107] and Mexico,[108] biometric registration is required to access banking and/or other financial services. In Mexico, a person must hand over their biometric information to open a bank account or acquire a credit loan. In India, our research partners found that CSO members are required to provide their Aadhaar number, linked to the national biometrics database, to receive foreign donations. Biometric registration in exchange for financial services is often justified with the claim that "biometric technologies may also be increasingly helpful for countering the financing of terrorism," as noted in a recent analytical brief released by the UN Security Council Counter-Terrorism Committee Executive Directorate.[109]

103 Privacy International. (n.d.). Sim Card Registration. Privacy International. https://privacyinternational.org/learn/sim-card-registration

104 Villanueva, Dora. "México, uno de los 18 países que exigen registro de datos biométricos." La Jornada, April 14, 2021. https://www.jornada.com.mx/notas/2021/04/14/economia/mexico-se-une-a-18-paises-que-piden-datos-biometricos/.

105 Privacy International. "Africa: SIM Card Registration Only Increases Monitoring and Exclusion," August 5, 2019. http://privacyinternational.org/long-read/3109/africa-sim-card-registration-only-increases-monitoring-and-exclusion.

106 Hellerstein, Erica. "In Mexico, a Controversial New Law Requires Cell Phone Users to Hand over Sensitive Information to the Government." Coda Story, April 29, 2021. https://www.codastory.com/authoritarian-tech/mexico-biometric-cell-phone-law/.

107 Case Study India: Section Notable uses of biometric technology

108 Aguirre, S. (2020, January 26). What are the biometric data that the Government wants and why you should take care of them. Animal Politico. https://www.animalpolitico.com/elsabueso/que-son-datos-biometricos-seguridad-gobernacion-ine/

109 United Nations Security Council, Counter-Terrorism Committee Executive Directorate (CTED). "CTED Analytical Brief: Biometrics and Counter-Terrorism," December 10, 2021. https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Dec/cted_analytical_brief_biometrics_0.pdf. ;

The linkage between financial surveillance and biometrics can expose sensitive information about an individual's associations and movements.[110] According to the CSO American Civil Liberties Union, financial surveillance "can create a detailed picture of our most private political, social, romantic, and religious activities."[111] In a case of financial surveillance for counter-terrorism (though not with the use of biometric technologies), our research partners from Uganda found that CSOs accused of participating in terrorism financing, such as the National NGO Forum and the Uganda Women's Network, had their bank accounts frozen.[112]

Data acquisition via private companies

The justification of counter-terrorism can grant governments broad access to data held by private companies. As such, governments are increasingly obtaining biometric and other personal data through partnerships with private companies who collect information about their users.[113] **Individuals may be unaware that by giving consent to private companies to collect their *sensitive* personal data, their biometric data is also shared with government actors.**

Research partners identified patterns of public-private data sharing in Mexico,[114] Jordan,[115] and Uganda,[116] In Mexico, mobile phone companies and banks were responsible for collecting biometric data on behalf of the government until a decision by the Supreme Court in 2022 deemed it unconstitutional.[117] In Jordan, the government has access to data about people's movements through partnerships with ride-sharing apps.[118] In Uganda, the government collaborates with private companies to gather

110 ECNL. (2022, August 31). Fintech: New Technology, Perpetual Challenges, https://ecnl.org/publications/fintech-new-technology-perpetual-challenges

111 ACLU. "Financial Privacy." American Civil Liberties Union. https://www.aclu.org/issues/privacy-technology/consumer-privacy/financial-privacy.

112 Anonymous. (2020, December 13). The Independent, 'CSOs condemn gov't for freezing NGO accounts,' https://www.independent.co.ug/csos-condemn-govt-for-freezing-ngo-accounts

113 Huszti-Orbán, K.& Ní Aoláin, F. (2020, July). Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?. pg. 29. Human Rights Center, University of Minnesota. https://law.umn.edu/human-rights-center/research/use-biometric-data-identify-terrorists

114 Case Study Mexico: Section Notable uses of biometric technology

115 Case Study Jordan: Section Data-sharing between private companies and the state

116 Case Study Uganda: Section Data-sharing between private companies and the state

117 Supreme Court Judgement: Suprema Corte Acción de inconstitucionalidad 82/2021. (2021, April 16). https://www.internet2.scjn.gob.mx/red2/comunicados/noticia.asp?id=6863

118 Freedom House. (2021). Freedom on the Net 2021. Freedom House Online. https://freedomhouse.org/country/jordan/freedom-net/2021

"strategic intelligence" and has proposed a large-scale initiative with major Telecom companies to track criminals and suspected terrorists.[119]

The increased ability for governments to demand sensitive data from private companies under the auspices of counter-terrorism suggests that our monitoring efforts should take note of data collection and biometric registration by private companies, not only government agencies. Private-public data sharing is often voluntary. In a report on biometrics and human rights from the UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism and the University of Minnesota Human Rights Center, the authors noted that "Governments also enter diverse partnerships with businesses in the context of which one party may provide the technology while the other the data to feed into the algorithm."[120]

119 Mpagai, C. (2018, April 9). Privacy at stake as Uganda targets telecom users in bid to stop crime. The East African. https://www.theeastafrican.co.ke/tea/business/privacy-at-stake-as-uganda-targets-telecom-users-in-bid-to-stop-crime--1387782

120 Huszti-Orbán, Krisztina, and Fionnuala Ní Aoláin. "Use of Biometric Data to Identify Terrorists: Best Practice or Risky Business?" University of Minnesota Human Rights Center, 2020. https://www.ohchr.org/Documents/Issues/Terrorism/biometricsreport.pdf.

Content Moderation

Suppression of activist content via pressure on private companies

Our investigation has found that governments around the world regularly request that platforms remove content that would violate their terms of service or the law. In Europe, through "Internet Referral Units"[121] or legal demands, governments call upon social media platforms to remove content they consider as terrorist or violent extremist. However, in actuality, **government demands to remove content can also appear to be made in order to suppress political critique around the world.** Research partners in India,[122] Jordan,[123] Mexico,[124] Thailand,[125] and Türkiye[126] uncovered evidence of censorship and suppression of political content on social media, with many instances occurring in conjunction with protests and political demonstrations.

Social media platforms publish some of these demands themselves. For example, in its transparency report, Twitter disclosed that it had received numerous requests to remove content of verified journalists between July-December in 2021. The countries that appear in our study were among the top requesters for content removal: Twitter received 114 legal demands to remove journalist content from India, 78 from Türkiye, 2 from Thailand, and 3 from Mexico. In fact, India and Türkiye were among the top 5 countries that made the most legal demands overall to remove content from Twitter.[127]

In some cases, activists feared that their content was "shadow-banned"[128] (i.e. the content was made quasi-invisible but not removed), live-streams of protests were interrupted, or they were blocked from their social media accounts.[129] When this occurs, it is difficult to prove whether these actions were deliberate and/or if they

121 EU Internet Referal Unit flagging terrorist and violent extemist online content and sharing it with relevant partners; Europol. (2022). EU Terrorism Situation and Trend Report (TE-SAT). Europol, https://www.europol.europa.eu/cms/sites/default/files/documents/Tesat_Report_2022_0.pdf

122 Case Study India: Section Notable uses of online content moderation and social media surveillance

123 Case Study Jordan: Section Notable uses of online content moderation and social media surveillance

124 Case Study Mexico: Section Notable uses of online content moderation and social media surveillance

125 Case Study Thailand: Section Notable uses of online content moderation and social media surveillance

126 Case Study Türkiye: Section Notable uses of online content moderation and social media surveillance

127 Twitter Transparency Center. "Removal Requests." https://transparency.twitter.com/en/reports/removal-requests.html#2021-jul-dec

128 Nicholas, G. (2022, April 26). Shedding Light on Shadowbanning. Center for Democracy and Technology. https://cdt.org/insights/shedding-light-on-shadowbanning/

129 Anonymous. (2020, July 29). Facebook Live streams restricted in Jordan during Teachers' Syndicate protests - NETBLOCKS: https://netblocks.org/reports/facebook-live-streams-restricted-in-jordan-during-teachers-syndicate-protests-XB7K1xB7; Mahasneh, I. (2019, June 12). Jordan: Measuring Facebook live-streaming interference during

were conducted based on a platform's independent decision as opposed to pressure from the government.[130] In countries where this kind of suppression of activist content regularly occurs, it's important to keep independent track of such cases to identify patterns, since companies will rarely provide formal notice about why content was removed and whether it was removed in response to a government request.

A related issue that emerged throughout this scoping study (even though it was not outlined in the research questions) is the use of Internet Service Providers (ISPs) to suppress activist content. This was reported by research partners from India,[131] Jordan,[132] and Türkiye.[133] This type of censorship is generally the result of a legal demand to companies providing internet access and can lead to blocking certain websites or livestreams, rather than removing content from social media platforms themselves. For example, Human Rights Watch named India as the global leader in government-led Internet shutdowns in 2020.[134]

Struggles between governments and social media platforms

While our research yielded numerous examples of collaboration between governments and companies, there are also cases of antagonism or struggle between the state and the private sector. This includes passing laws to regulate social media platforms in a more punitive way or disputes between governments and social media companies about what type of content can be posted or not.

Though most online content moderation is done by social media companies on their own volition, an increasing number of governments have enacted legislation that requires and/or incentivises companies to remove types of content.[135] In 2017, Germany

protests. OONI Online. https://ooni.org/post/jordan-measuring-facebook-interference/ ; Spary, S. (2016, April 8). Facebook is Embroiled In A Row With Activists Over "Censorship". Buzzfeed News. https://www.buzzfeed.com/saraspary/facebook-in-dispute-with-pro-kurdish-activists-over-deleted

130 BSR. (2022, September). Human Rights Due Diligence of Meta's Impacts in Israel and Palestine in May 2021 Pg. 5. BSR. https://www.bsr.org/reports/BSR_Meta_Human_Rights_Israel_Palestine_English.pdf.

131 Case Study India: Section Notable uses of online content moderation and social media surveillance

132 Case Study Jordan: Section Notable uses of online content moderation and social media surveillance

133 Case Study Türkiye: Section Notable uses of online content moderation and social media surveillance

134 Human Rights Watch. "Shutting Down the Internet to Shut Up Critics." In World Report 2020, 2020. https://www.hrw.org/world-report/2020/country-chapters/global-5.

135 Tech Against Terrorism. "The Online Regulation Series: The Handbook," July 2021. https://www.techagainstterrorism.org/wp-content/uploads/2021/07/Tech-Against-Terrorism-%E2%80%93-The-Online-Regulation-Series-%E2%80%93-The-Handbook-2021.pdf.

passed the Network Enforcement Act (NetzDG)[136] to address illegal online content (beyond terrorist content). Relatedly, in 2021, the European Union adopted TERREG[137], a regulation that requires companies to take down potentially terrorist content within one hour of receiving a removal notice, or else be subject to penalty. Both regulations can lead to overenforcement of content policies, resulting in censorship. The growth of this type of legislation over the past five years suggests that this is an area to monitor, given the severe implications of such laws on freedom of expression, assembly, and association.

In some countries, the relationship between the government and social media companies is particularly antagonistic. In Thailand,[138] the government has threatened to prosecute companies like Facebook, Google, and Twitter for failing to comply with their requests for content removal. Conversely, Facebook and Twitter removed content that supports the Thai military and critiques insurgent groups in Southern Thailand,[139] against the government's wishes. In July 2022, Twitter filed a lawsuit in the Karnataka High Court in Bangalore, India,[140] challenging an order from the Indian government requesting they remove content and block dozens of accounts, including those of activists, journalists and political dissidents. The case is currently pending in court.

Social media companies' willingness to act against the Thai government indicates that platforms can still represent a powerful force against authoritarian government interests.[141] However, it remains to be seen whether they will continue to exercise this power in other national contexts.

136 Bundesministerium der Justiz (2017, September 1). Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG) Nichtamtliches Inhaltsverzeichnis. https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html

137 Official Journal of the European Union. (2021, May 17). REGULATION (EU) 2021/784 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 29 April 2021 on addressing the dissemination of terrorist content online. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R0784&from=EN

138 Case Study Thailand: Section Notable uses of online content moderation and social media surveillance

139 Anonymous. (2020, October 9). Twitter takes down Thai army IO Network. Bangkok Post. https://www.bangkokpost.com/thailand/general/1999463/twitter-takes-down-thai-army-io-network ; Tanakasempipat, P. (2021, March 3). Facebook removes Thai military-linked information influencing accounts. Reuters. https://www.reuters.com/article/us-facebook-thailand-idUSKBN2AV252

140 Case Study India: Section Relevant laws and legal precedents

141 Anonymous. (2022, July 10). Opinion; Twitter's case against India is crucial to the internet's future. The Washington Post Online https://www.washingtonpost.com/opinions/2022/07/10/twitter-india-lawsuit-free-expression/

Conclusion

The use of technology such as digital surveillance and platforms in the name of counter-terrorism can pose several risks to civil society, with ripple effects on human rights such as freedom of expression, privacy, freedom of assembly and association, right to life, liberty and security, and non-discrimination. **This study has shown that governments can repurpose biometric data to the detriment of people and civil society, and/or suppress and stifle free speech by restricting online content, under the stated purpose of counter-terrorism. This puts members of civil society, especially those from marginalized and vulnerable groups, at severe risk.** Civic space is restricted, as governments and companies suppress legitimate political expression and critique.

In some cases, these harms can seem inadvertent. In other contexts, emerging technologies are used to deliberately target, surveil, and suppress CSOs under the guise of preventing terrorism. What's more, technologies that were originally introduced to protect national security, public health. or combat terrorism, can later be repurposed for domestic surveillance. For instance, data that was originally collected for purposes such as border control or pandemic-tracing can be (re)used to monitor civil society groups.

Our study revealed that **many countries do not yet have the infrastructure necessary to fully deploy emerging technologies for surveillance or censorship purposes. That said, there is already evidence of "low-tech" surveillance with ambitions to 'upgrade' them.** For example, research partners in Uganda[142] and Ukraine[143] documented the extensive use of CCTV cameras and audio recording equipment, which can then enable facial and voice recognition. Given the existing presence of "low tech" devices and the history of government surveillance, we can reasonably assume that there will be algorithmic-driven surveillance in the future. This risk is exacerbated if such technologies are increasingly normalised. The expansion of these technologies in countries that already suffer from weak institutions, with few protections for privacy and other human rights, puts citizens at greater risk of harm.[144]

Unfortunately, there are only limited legal instruments or legal precedents to protect CSOs in the face of surveillance and censorship, and are mostly in the European Union,

142 Case Study Uganda: Section Notable uses of biometric technology

143 Case Study Ukraine: Notable uses of biometric technology

144 Ibezim-Ohaeri, Victoria, Joshua Olufemi, Lotanna Nwodo, Oluseyi Olufemi, and Ngozi Juba-Nwosu. "Security Playbook of Digital Authoritarianism in Nigeria." Action Group on Free Civic Space, December 2021. https://closingspaces.org/the-security-playbook-of-digital-authoritarianism-in-nigeria/.

such as the GDPR.[145] Moreover, other recent online content regulations in Europe which ar seemingly public interest-driven, such as the German NetzDG[146] and EU TERREG can also adversely impact civic freedoms. Of concern is the fact that European regulation can lead to 'copycat' laws around the world, creating severe risks to civic freedoms, such as privacy, freedom of expression, association, and assembly. The risks of copying this laws without proper safeguards is heightened in countries with authoritarian regimes and poor human rights records. In its 2020 report on Germany, the United Nations Human Rights Committee called out the chilling effects of NetzDG on freedom of expression, with repercussions around the world.[147] Relatedly, a report by the CSO Justitia noted the influence of European laws, like NetzDG, on legislation enabling censorship and surveillance in dozens of other countries, many of which are outside of Europe.[148] Indeed, many of the states in this report proposed or have recently passed data protection and online content regulation with harmful impacts on civic space and human rights. Examples in this study include recent legislation in India[149] and Türkiye.[150]

145 General Data Protection Regulation. (2018, May 25). https://gdpr-info.eu/; European Commission Websitre. The Digital Services Act. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

146 Bundesministerium der Justiz (2017, September 1). Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG) Nichtamtliches Inhaltsverzeichnis. https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html

147 United Nations. (2021, November 30). CCPR/C/DEU/CO/7: Concluding observations on the seventh periodic report of Germany https://www.ohchr.org/en/documents/concluding-observations/ccprcdeuco7-concluding-observations-seventh-periodic-report

148 Mchangama, J & Alkiviadou, N. (2020, September). Justitia. "The Digital Berlin Wall: How Germany (Accidentally) Created a Prototype for Global Online Censorship - Act Two." https://justitia-int.org/wp-content/uploads/2020/09/Analyse_Cross-fertilizing-Online-Censorship-The-Global-Impact-of-Germanys-Network-Enforcement-Act-Part-two_Final-1.pdf

149 Ministry of Electronics and Information Technology Government of India. (2008). Information Technology Act. https://www.meity.gov.in/content/information-technology-act

150 amending Law No. 5651. (2017, July 29). https://perma.cc/KW9B-L8DR ; Law no. 561 on Regulating Internet Publications and Combating Crimes Committed by Means of Such Publications. (2007, May 4). https://perma.cc/T97C-AM9H

General Findings

National identity databases. Research partners did not find any evidence that national identity databases were repurposed for counter-terrorism in the countries of research in this study, but have voiced concerns of the risks and highly likelihood thereof.

Biometric border control. All researched countries have been found to use biometric systems to enforce national borders. This poses a threat to civil society members, whose movements can be tracked or who could be prevented from traveling.

International funding for biometrics development. International bodies are actively encouraging and funding the spread of biometric technologies, yet much of that funding is opaque.

Biometric surveillance and protests. Biometric systems are either used or encouraged to monitor and stifle protests in all countries.

Biometrics and mobile phone registration. Mandatory biometric registration to obtain a mobile phone number is a new but concerning global trend.

Biometrics and financial services. Public-private data sharing exists in the financial industry, potentially exposing sensitive information of an individual's associations and movements. Human rights safeguards are generally not incorporated in how banks profile customers and share data.

Data acquisition via private companies. Governments have increased authority to demand sensitive data from the private sector, including from social media companies, under the auspices of counter-terrorism.

Suppression of activist content via pressure on private companies. Governments regularly demand that social media platforms remove content that is seen as terrorist, extremist, or unlawful. In the researched countries, demands to remove content often appear to be made to covertly suppress political dissent.

Struggles between governments and social media platforms. Though most content governance is carried out by social media companies on their own volition, an increasing number of governments have passed legislation that requires and/or incentivises companies to over-comply with content moderation policies, pressuring them to remove content. This can create antagonism between governments and social media, especially when the latter push back against government demands.

Other emerging issues

The research questions formulated for this scoping study aimed to map key trends and risks related to the use of biometric surveillance and social media platforms in the counter-terrorism context. However, some of these questions could not be fully analysed and understood in this preliminary research and require further investigation. Regarding questions on biometric surveillance, the main issue seemed to be the lack of available data, either because biometric technologies were not (yet) operational in their countries or because of a lack of transparency about their use. In terms of content governance and social media platforms, the lack of transparency around how platforms enforce their content policies remains a key challenge.

While not in scope for this study, note findings by several groups that the COVID-19 pandemic has produced an influx of new surveillance technologies, many of which were introduced in a "state of emergency," similarly to how counter-terrorism measures evolved.[151] ECNL, in collaboration with Privacy International, the International Network of Civil Liberties Organizations, and local partners based in the Global South, researched the impact of these technologies on privacy and other human rights in their 2022 report.[152] The report documents concerns of misuse and repurposing of digital technologies in the context of COVID-19, similar to concerns outlined in this study.

Two other issues, which were not explicitly stated in the research questions, emerged organically from the submitted reports and warrant further research. First, there's a need to investigate the partnerships between private companies and national governments. Second, the role of international governments and donors is underexplored and merits attention.

151 Tactical Tech. "Technologies of Hope and Fear: 100 Pandemic Technologies," 2020. https://techpandemic.theglassroom.org/; Privacy International. (n.d). Tracking the Global Response to COVID-19 page. https://privacyinternational.org/examples/tracking-global-response-covid-19; OHCHR. (n.d). COVID-19 and Special Procedures https://www.ohchr.org/en/special-procedures-human-rights-council/covid-19-and-special-procedures

152 ECNL, INCLO & Privacy International. (2022, December 14). Under Surveillance: (Mis)use of Technologies in Emergency Responses, https://ecnl.org/publications/under-surveillance-misuse-technologies-emergency-responses

Annex 1: Research Questions

Our partners were given the questions below to guide their research. The italicised questions are those that remain unresolved, either because our research partners were not able to access the necessary information to answer the question, or they concluded the phenomenon was not yet observable in their country. See the 'Conclusion' section of this report for commentary on the formulation of these research questions and recommended areas for future research.

Biometrics

- What types of biometric technologies are proposed or deployed as tools for security purposes or countering terrorism/anti-money laundering purposes in your country?
- Do you see any evidence of (or plans to build) interoperable or integrated databases of biometric data?
- Are you aware of any risk assessments/human rights impact assessments (HRIAs) implemented by the State to avoid security breaches of these databases or otherwise protect against misuse? Are you aware of any HRIAs conducted by companies to mitigate adverse human rights impacts by those who deploy surveillance technologies?
- Are organisations, CSO representatives, human rights defenders, activists, or journalists required (or pressured) to give their biometrics to operate? Are they put on counter-terrorism watchlists?
- Do you see any evidence of CSO representatives, human rights defenders, activists, or journalists who have been identified, monitored, detained, or criminalised through the use of biometric technology?
- Have they been prevented from traveling or falsely accused of terrorism due to errors/inaccuracy in the system, or subjected to discriminatory profiling, preventing them from carrying out their work?
- Is there any incident where a protester has been identified (including falsely) through the use of a facial recognition system?
- Have there been court cases challenging the use of these tools or related data protection laws?

Is the existing domestic remedial framework adequate? For instance, is it possible for CSOs to assert standing rather than individuals, and are there any jurisdictional difficulties if the complainant individuals are migrants, at border, or overseas?

Online content moderation

- Have any civil society actors been deplatformed, shadow-banned, or had their content removed and/or downranked, because social media platforms considered them "terrorists" or "extremist groups"?
- People often post pictures or content online that documents human rights abuses. When this content is removed, it can often hinder documentation and preservation of evidence. Have social media platforms taken any measure to secure this information for future trials or justice?
- Are any civil society actors on social media platforms' lists of dangerous, violent, extremist or terrorist groups, and what are the reason for including them on that list?
- Have you seen any specific bias or discrimination towards one group (e.g., based on race, ethnicity, religion, etc.)?
- Were the individuals or groups whose accounts or content was removed on grounds of CT able to appeal the decision? Did they appeal internally (i.e., at the platform level) or get judicial review? How was their experience?
- What was the outcome of the appeal? Has the content or account been restored? Are you aware of any other remedies available?
- Has the social media platform subsequently taken measures to prevent the undue blockage of accounts and/or content on grounds of security, counter-terrorism, border control, or anti-money laundering?

Annex 2: Glossary of key terms

Biometrics

Technologies that measure parts of the body, such as fingerprints, irises, or facial geometry. These measurements are often leveraged for the purposes of identifying people.

Deplatforming

The practice of permanently suspending a user or organisation from a social media platform.

Internet referral unit

An EU government agency that reports unlawful and terrorist content to social media companies so that companies will remove the content under their own terms of service.

Jawboning

The practice of government officials using informal channels (as opposed to laws) to pressure companies to remove social media content they consider unlawful or harmful.[153]

Shadow-banning

The practice of reducing the visibility of a user's profile or content without blocking the user from the social media platform or removing their content, to such a level that their content is barely visible in practice. Shadow-banning is often done without officially notifying the user.[154]

153 Lakier, Genevieve. "Informal Government Coercion and The Problem of 'Jawboning.'" Lawfare, July 26, 2021. https://www.lawfareblog.com/informal-government-coercion-and-problem-jawboning.

154 Clark, Corinne. "What Is Shadow Banning?" IMGE, July 15, 2020. https://imge.com/shadow-banning-on-twitter/.

European Center for
Not-for-Profit Law

European Center for Not-for-Profit Law Stichting
5 Riviervismarkt
2513 AM, The Hague
Netherlands

www.ecnl.org
@enablingNGOlaw