THE IMPACT OF COUNTER-TERRORISM MEASURES ON CIVIL SOCIETY AND CIVIC SPACE:

Response to the call for input from the Special Rapporteur on counter-terrorism and human rights

February 2023

privacyinternational.org

Privacy International, European Centre for Not-for-Profit Law, International Network of Civil Liberties Organizations (INCLO), Agora, Canadian Civil Liberties Association, Centro de Estudios Legales y Sociales, Irish Council for Civil Liberties, KontraS, Legal Resources Center, and Liberty respond to the call for input to the Global Study on the Impact of Counter-Terrorism Measures on Civil Society and Civic Space

January 2023

Introduction

Privacy International (PI), the European Center for Not-for-Profit Law (ECNL), International Network of Civil Liberties Organizations (INCLO), Agora, the Canadian Civil Liberties Association, Centro de Estudios Legales y Sociales in Argentina, the Irish Council for Civil Liberties, KontraS in Indonesia, the Legal Resources Center in South Africa, and Liberty in the UK welcome the opportunity to provide input to the global study of the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism.

Civic spaces where everyone is free to develop, protest, express themselves, share ideas and preserve their integrity and autonomy are increasingly under threat as new surveillance technologies are radically transforming the ability of authorities to monitor them.[1] In the name of countering terrorism, the deployment of surveillance technologies and measures has been accelerating around the globe, often abusively, without being effectively regulated or subject to accountability mechanisms.

We believe that this forthcoming study could put to the forefront the continued and increasing misuse of counter-terrorism laws and policies against civil society and civic space and demonstrate the importance

[1] PI, "Protecting Civic Spaces" (2019) https://privacyinternational.org/long-read/2852/protecting-civic-spaces

of the meaningful participation of diverse civil society**.** The submitting organisations trust that the global study could counter narratives of securitisation driving ongoing counterterrorism policies and inform future counterterrorism strategies. It could further assist states, companies, and other actors to cease counterterrorism efforts that undermine the role and work of civil society across the globe, and to take the necessary measures to protect civil society against abuse.

The following sections provide submitting organisations' information and analysis of some of the topics listed in the call for submission.[2]

1. (Mis)use of Technologies in Emergency Responses: Global lessons from the Covid-19 pandemic

In the months following the beginning of the Covid-19 pandemic, more than half the world's countries enacted emergency measures. With these measures came an increase in executive powers, a suspension of the rule of law, and an upsurge in security protocols – with subsequent impacts on fundamental human rights. Within this broader context, we have seen a rapid and unprecedented scaling up of governments' use of technologies to enable widespread surveillance. Surveillance technologies exacerbated the impacts of Covid-19 emergency measures on civic space by allowing governments to collect fine-grained data about individuals while also working across large scales of information, in a way that has been unprecedented in the history of global pandemics.

ECNL, INCLO, and PI joined together and conducted a broad survey of the Covid-19 surveillance technology and measures adopted in the 15 countries where INCLO members operate and then engaged more deeply with organizations and researchers in six countries[3] to track the negative impacts of those measures. We have identified specific measures highlighting how responses to the Covid-19 pandemic were informed by existing frameworks and resources that had originally been introduced for counter-terrorism efforts and how, three years later, surveillance measures introduced as a response to the pandemic are now being repurposed for counter-terrorism purposes. Further information on trends and examples below can be found in our report.[4]

1.1 The repurposing of existing security measures

In order to quickly roll out Covid-19 surveillance measures, some governments took advantage of existing frameworks and resources that had originally been introduced for counter-terrorism efforts, including drawing upon existing legislation, deploying military technologies, and calling upon national intelligence services. We observed an overall trend in which laws, technologies and agencies that had previously been associated with counter-terrorism and national security pivoted to the new objective of fighting the

[2] OHCHR, Call for inputs: Global Study on the Impact of Counter-Terrorism Measures on Civil Society and Civic Space (2022) https://www.ohchr.org/en/calls-for-input/2023/call-inputs-global-study-impact-counter-terrorism-measures-civil-society-and

[3] Particularly, Daniel Ospina Celis, Lucia Camacho, Juan Carlos Upegui (Dejusticia in Colombia), Bastien Le Querrec (La Quadrature du Net in France), Amber Sinha (Pollicy in India), Nadine Sherani, Rozy Sodik, Auliya Rayyan (KontraS in Indonesia), Martin Mavenjina (Kenya Human Rights Commission in Kenya), Sherylle Dass, Devon Turner (Legal Resources Centre in South Africa). PI, ECNL, INCLO, "Under Surveillance: (Mis)use of Technologies in Emergency Responses Global lessons from the Covid-19 pandemic" (2022) https://privacyinternational.org/sites/default/files/2022-12/ECNL%2C%20INCLO%2C%20PI-COVID-19-Report-Final.pdf

[4] *ibid.*

spread of Covid-19. We found evidence that cybercrime laws were expanded to censor critical voices and persecute people accused of spreading misinformation about the pandemic in Bangladesh, Indonesia, Kenya, Niger, and Saudi Arabia.[5]

Counter-terrorism frameworks are notorious for sidestepping human rights, for unlawfully targeting civil society groups, ethnic, religious, and other minorities (and Muslim men in particular in some jurisdictions), for lack of transparency, and for covert or unaccountable practices. These same concerns apply when counter-terrorism laws and technologies are repurposed for new objectives. This kind of repurposing was encouraged by the private sector. A Reuters investigation[6] identified "at least eight surveillance and cyber-intelligence companies attempting to sell repurposed spy and law enforcement tools" to governments by repackaging their products as tools for tracking the virus and enforcing quarantines.

1.2 The repurposing of Covid-19 measures and the normalization of surveillance beyond the pandemic

The majority of Covid-19 surveillance measures were introduced during the first year of the pandemic. At the time of writing of our report in the second half of November 2022, we observed how some of these extraordinary measures had been extended, or how data collected under the pretext of fighting Covid-19 has been used for other purposes, including counter-terrorism efforts. Our major concern is that the pandemic has provided an entry point for invasive government surveillance to become normalized even after the threat from the virus has receded. We need to consider the repurposing of Covid-19 infrastructure in relation to a larger tendency towards overbroad government surveillance after national emergencies, under the fallacy that security can only be achieved by accumulating more and more information. The most notable example of this tendency is the expansion of governments' surveillance powers after the 9/11 terrorist attacks in the US, which established a worldwide infrastructure of invasive data collection still present 20 years later, despite reports of little to no counter-terrorism benefit.

1.3 Successful civil society actions to challenge Covid-19 surveillance measures

Throughout the pandemic, civil society organizations have played an important role as watchdogs. We are indebted to these organizations for monitoring the ongoing crisis and documenting the impacts of Covid-19 surveillance measures on human rights and fundamental freedoms. In the report, we highlight a few indicative examples of strategic litigation efforts and other advocacy campaigns led by civil society to resist unlawful surveillance in and of their communities.

- In France, May 2020, two civil society organisations, La Quadrature du Net (LQDN) and La Ligue des Droits de l'Homme, filed a successful lawsuit to block the use of drones to enforce Covid-19 lockdown in Paris.

[5] PI, ECNL, INCLO, "Under Surveillance: (Mis)use of Technologies in Emergency Responses Global lessons from the Covid-19 pandemic" (2022) https://privacyinternational.org/sites/default/files/2022-12/ECNL%2C%20INCLO%2C%20PI-COVID-19-Report-Final.pdf

[6] Joel Schectman, Christopher Bing, Jack Stubbs , Special Report: Cyber-intel firms pitch governments on spy tools to trace coronavirus, *Reuters* (2020) https://www.reuters.com/article/us-health-coronavirus-spy-specialreport/special-report-cyber-intel-firms-pitch-governments-on-spy-tools-to-trace-coronavirus-idUSKCN22A2G1

- In Colombia, a challenge by journalists and others with the support of civil society, including Dejusticia,[7] reinforced the obligation to respect the right to privacy even during a national state of emergency.[8]

- In Israel, the Association for Civil Rights in Israel (ACRI) submitted a successful petition to the High Court of Justice, that found that Shin Bet was "not constitutionally authorized to collect, process and use 'technological information'" of Covid-19 patients.[9]

The report by ECNL, INCLO, and PI proposes key recommendations to states, companies, and civil society to ensure more human rights-centred technological responses to future emergencies that the submitting organisations urge the UN Special Rapporteur to consider including in her study.[10]

2. Targeted and mass surveillance, including of journalists and human rights defenders

2.1 Mass surveillance

In the absence of an internationally agreed definition, submitting organisations hold that "targeted" surveillance is surveillance in circumstances where there is reasonable suspicion[11] that a specific target has committed or is likely to commit a criminal offence or is engaging in acts amounting to a threat to national security, including terrors. Conversely, mass surveillance is surveillance that is not 'targeted' and involves systems or technologies, such as interception of information, that collect, analyse, and/or generate data on indefinite or large numbers of people instead of limiting surveillance to individuals about which there is reasonable suspicion of wrongdoing or those who are not of any legitimate interest to the security and intelligence agencies.[12]

[7] Dejusticia, "Lack of transparency around contact-tracing app" in: PI, ECNL, INCLO, "Under Surveillance: (Mis)use of Technologies in Emergency Responses Global lessons from the Covid-19 pandemic" (2022) https://privacyinternational.org/sites/default/files/2022-12/ECNL%2C%20INCLO%2C%20PI-COVID-19-Report-Final.pdf

[8] See also Karisma, "CoronApp, Medellín me Cuida y CaliValle Corona al laboratorio -O cómo se hackea CoronApp sin siquiera intentarlo-" (2020) https://web.karisma.org.co/coronapp-medellin-me-cuida-y-calivalle-corona-al-laboratorio-o-como-se-hackea-coronapp-sin-siquiera-intentarlo/

[9] The Association for Civil Rights in Israel, The Association for Civil Rights in Israel, "*We Won: HCJ Sides with ACRI Petition Against Shin Bet Tracking Civilians*" (2020) https://www.english.acri.org.il/post/__154; The Association for Civil Rights in Israel, "*GSS Tracking as a Part of the Struggle Against Corona – Fifth Petition"* (2021) https://www.english.acri.org.il/post/__385

[10] PI, ECNL, INCLO, "Under Surveillance: (Mis)use of Technologies in Emergency Responses Global lessons from the Covid-19 pandemic" (2022) https://privacyinternational.org/sites/default/files/2022-12/ECNL%2C%20INCLO%2C%20PI-COVID-19-Report-Final.pdf

[11] While we make a distinction between targeted and mass surveillance, and focus on the widespread (mis)use of the latter for its privacy infringements, we also call attention to ways that conceptions of crime and reasonable suspicion even in practices of targeted surveillance also threaten human rights, particularly of already marginalised communities. In the UK, Liberty successfully challenged the Metropolitan Police use of the Gangs Violence Matrix, a secretive database that was found to discriminate against Black people, and breached privacy rights. The Matrix was also used in conjunction with other police tactics, such as stop and search, which despite having 'reasonable suspicion' safeguards attached to its use, is wielded disproportionately against Black communities, with spurious reasonable suspicion grounds fuelled by racism and classism. See Liberty, "Met to overhaul 'racist' Gangs Matrix after landmark legal challenge" (2022) https://www.libertyhumanrights.org.uk/issue/met-to-overhaul-racist-gangs-matrix-after-landmark-legal-challenge/

[12] PI, "Mass Surveillance" https://privacyinternational.org/learn/mass-surveillance

Governments continue to rely on mass surveillance, often justifying it on national security grounds. The undersigned organisations believe that mass surveillance threatens the essence of the right to privacy and fails to comply with the principles of necessity and proportionality putting at risk core democratic principles and the rule of law. We also note that when challenged before independent courts, mass surveillance programmes have been found in breach of the right to privacy and other human rights. Many of these cases have revealed instances where civil society organisations, activists, lawyers and journalists have been under surveillance as a result of mass surveillance measures.

Among others, the Investigatory Powers Tribunal (IPT), the judicial body responsible for monitoring UK intelligence and security agencies, has found that all three agencies – Government Communications Headquarters (GCHQ), Security Service (MI5) and Secret Intelligence Service (SIS) – were unlawfully holding data relating to Privacy International and the Security Service had even accessed it.[13] The case was brought by PI, challenging the acquisition, use, retention, disclosure, storage, and deletion of bulk personal datasets (BPDs) and bulk communications data (BCD) by the UK security and intelligence agencies which was deemed unlawful by the IPT.[14]

PI has been involved in other similar legal challenges as well. Most notably:

- On 4 February 2021, the Constitutional Court of South Africa declared that bulk interception by the South African National Communications Centre is unlawful and invalid after a complaint brought by the amaBhungane Centre for Investigative Journalism NPC and investigative journalist Stephen Patrick Sole who was under surveillance.[15]

- On 25 May 2021, the Grand Chamber of the ECtHR confirmed that the UK's mass surveillance laws breached the rights to privacy and freedom of expression.[16] Sixteen different civil society organisations, journalists, and activists were applicants to this case, including Liberty in the UK, the American Civil Liberties Union (ACLU), the Canadian Civil Liberties Association (CCLA), the Egyptian Initiative For Personal Rights (EIPR), the Hungarian Civil Liberties Union (HCLU), the Irish Council For Civil Liberties (ICCL), the Legal Resources Centre in South Africa.[17]

- Following the above-mentioned case, the UK government settled a separate claim with four applicants (Human Rights Watch, an activist, a lawyer and a journalist), acknowledging that the UK previous investigatory powers regime was not compliant with Article 8 of the European Convention on Human Rights, and in relation to the treatment of confidential journalistic material, Article 10 of the Convention.[18]

[13] PI, "Bulk Personal Datasets & Bulk Communications Data challenge" https://privacyinternational.org/legal-action/bulk-personal-datasets-bulk-communications-data-challenge
[14] PI, "Briefing on Legal Case: Privacy International v Secretary of State for Foreign and Commonwealth Affairs and others" (2021) https://www.privacyinternational.org/sites/default/files/2021-07/BPD-BCD%20Briefing%20%28summary%20and%20timeline%29%20July%202021%202.pdf
[15] PI, "amaBhungane and Sole challenge" https://privacyinternational.org/legal-action/amabhungane-and-sole-case-south-africa
[16] PI, "UK mass interception laws violates human rights and the fight continues..." (2021) https://privacyinternational.org/long-read/4526/uk-mass-interception-laws-violates-human-rights-and-fight-continues
[17] Liberty, "Human rights groups win landmark mass surveillance ruling" (2021) https://www.libertyhumanrights.org.uk/issue/human-rights-groups-win-landmark-mass-surveillance-ruling/
[18] PI, "UK mass interception laws violates human rights and the fight continues..." (2021) https://privacyinternational.org/news-analysis/4818/uk-government-acknowledges-past-violations-individuals-rights-and-fight

2.2 Government hacking

Further, certain surveillance methods which governments proclaim to be 'targeted' result in violations of the right to privacy of individuals, as well as other human rights.

This is notably the case with regards to government hacking. Hacking has been used to target human rights defenders, journalists, and political opponents in ways that violate their human rights, as most prominently revealed in the Pegasus/NSO cases uncovered by researchers, journalists, activists, and others.[19]

Government hacking is unlike any other form of existing surveillance technique. Government hacking can be far more privacy intrusive than any other surveillance technique, permitting to remotely and secretly access personal devices and the data stored on them as well as to conduct novel forms of real-time surveillance, for example, by turning on microphones, cameras, or GPS-based locator technology. Hacking also allows governments to manipulate data on devices, including corrupting, planting or deleting data, or recovering data that has been deleted, all while erasing any trace of the intrusion.

It not only poses unique privacy interference to the intended targets, but it often affects the privacy and security of others in unpredictable ways. Hacking is about causing technologies to act in a manner the manufacturer, owner or user did not intend or did not foresee. It often depends on exploiting vulnerabilities in systems to facilitate surveillance objectives. It is therefore fundamentally at cross-purposes with digital security aims: in the surveillance context, the government identifies vulnerabilities, not to secure systems through testing and coordinated disclosure, but to exploit them in order to facilitate a surveillance objective. This approach only undermines the security of the target system but also of other systems.[20]

2.3 Examples of surveillance targeting human rights defenders

Because of its covert nature, lack of authorisation or oversight, and the lack of notification mechanisms, it is notoriously difficult to document examples of surveillance of individuals. However, such instances are

[19] PI, Amnesty International and Centre for Research on Multinational Corporations (SOMO), "Operating from the Shadows: Inside NSO Group's Corporate Structure" (2021) https://www.privacyinternational.org/report/4531/operating-shadows-inside-nso-groups-corporate-structure; The Association for Civil Rights in Israel, "Cease Use of Pegasus Spyware" (2022) https://www.english.acri.org.il/post/__154; Claire Parker, Hungarian activists to launch legal blitz challenging government's use of NSO Pegasus spyware, *The Washington Post* (2022) https://www.washingtonpost.com/world/2022/01/28/hungary-pegasus-legal-action/; Hungarian Civil Liberties Union, "Pegasus Case: Hungarian Civil Liberties Union takes coordinated domestic and foreign legal action", https://hclu.hu/en/pegasus-case; "Canadian Civil Liberties Union (CCLA) calls for moratorium on Royal Canadian Mounted Police surveillance 'tools'" (2022) https://ccla.org/press-release/ccla-calls-for-moratorium-on-rcmp-surveillance-tools/

[20] PI, "Government Hacking and Surveillance: 10 Necessary Safeguards" (2017) https://privacyinternational.org/sites/default/files/2018-08/2018.01.17%20Government%20Hacking%20and%20Surveillance.pdf

increasingly documented, as for example with Pegasus/NSO cases above.[21] Moreover, PI has collected testimonies of human rights defenders in Colombia, Indonesia, Mexico, and South Africa.[22]

Further in 2021, the Defenders Coalition in Kenya published the results of its survey of 56 human rights defenders from across Kenya, who have raised concerns about their mobile phones being tapped and their communication intercepted. As the report notes, these experiences have had a chilling effect on the exercise of their rights and freedoms of expression, association, and assembly.[23]

In the United Kingdom, the Public Order Bill currently making its way through Parliament would introduce Serious Disruption Prevention Orders (SDPOs) and mark a significant expansion of State surveillance over those who protest.[24] A person given an SDPO may be subject to a wide range of onerous requirements, and may even be subject to electronic monitoring. SDPOs are an unprecedented and highly draconian measure that stand to extinguish named individuals' fundamental right to protest, as well as their ability to participate in a political community. They will also have the effect of subjecting individuals and wider communities to intrusive surveillance. This follows a wider trend in the United Kingdom of the government stifling freedom of expression and shutting down avenues for human rights defenders, other civic actors, and the general public, to hold the state to account.

2.4 The role of industry

Although it is possible that some governments manufacture tools to conduct digital surveillance themselves, many states buy the sophisticated technology enabling such surveillance from private companies. They justify the procurement of these technologies as essential for maintaining law and order.[25] Some of these surveillance companies manufacture and sell spyware or other such tools to states, who have, in addition to legitimate purposes, used surveillance to shrink the space for dissent by targeting human rights defenders, in violation of their internationally recognized human rights.[26]

- These companies are often opaque in their structure, activities and clients. PI together with Amnesty International, and SOMO published a briefing to analyse the corporate structure of the NSO group to highlight the human rights risks and corporate dynamics that characterize the

[21] Among others, the Forbidden Stories consortium, a Paris-based journalism non-profit, and Amnesty international gained access to a list of more than 50,000 phone numbers and forensic analysis of numerous infected phones, revealing that at least 189 journalists, 85 human rights defenders, over 600 politicians and government officials were affected as targets. See forbiddenstories, "About The Pegasus Project", https://forbiddenstories.org/about-the-pegasus-project/; https://www.ohchr.org/en/documents/thematic-reports/ahrc5117-right-privacy-digital-age

[22] PI, "Being the Target", https://privacyinternational.org/campaigns/being-target

[23] PI, "Defenders Coalition: Impact of Communication Surveillance on HRDs in Kenya" (2021) https://privacyinternational.org/report/4469/defenders-coalition-impact-communication-surveillance-hrds-kenya

[24] SDPOs are a new civil order that can be imposed on individuals who have carried out (or contributed to someone else carrying out) activities related to at least two protests within a five-year period, whether or not they have actually been convicted of a crime. SDPOs are effectively 'protest banning orders,' with the potential to ban named individuals from protesting, associating with certain people at certain times, and even using the internet in certain ways. See Liberty's Briefing on the Public Order Bill for Committee Stage in the House of Lords, (2022) https://www.libertyhumanrights.org.uk/wp-content/uploads/2019/03/Libertys-briefing-on-the-Public-Order-Bill-for-Committee-Stage-in-the-House-of-Lords-November-2022.pdf

[25] See among others PI, "Global Surveillance Industry report" (2018) https://privacyinternational.org/explainer/1632/global-surveillance-industry

[26] PI, "Protecting Civic Spaces" (2019) https://privacyinternational.org/long-read/2852/protecting-civic-spaces

broader surveillance industry, and to support civil society in their efforts to seek accountability for abuses.[27]

- Further, in May 2022, PI reported on the rise of the private intelligence industry where some governments and private actors increasingly resort to conducting surveillance. The report details the use of hacking techniques, monitoring of environmental and other activists, and running fake 'astroturfing' campaigns for big polluters and examines the gap in the current UK legal regime.[28]

3. Use of biometrics for identification and authentication

PI has covered extensively in other submissions the uses of biometrics, including in digital ID systems.[29] Here, we focus on the specific concerns raised by the use of biometrics for counter-terrorism purposes.

In its December 2021 analytical briefing on biometrics and counter-terrorism, the United Nations Counter-terrorism Committee Executive Directorate (CTED) notes how "the use of biometrics for counter-terrorism purposes – notably in the context of border management and security – has become increasingly widespread."[30] That is a direct result of UN Security Council resolutions imposing legally binding obligations on all UN member states to develop biometric technologies for counter-terrorism purposes, paired with the strong promotion of these technologies by some, mostly Western states and by powerful industry players.[31]

PI documented in three case studies (covering Afghanistan and Iraq, Israel/Palestine, and Somalia) the human rights implications of the use of biometric technologies for counter-terrorism purposes. While the contexts are different, the main trends are very similar:[32]

- Biometric technologies, coupled with large, centralized databases, can seriously undermine the human right to privacy and have an irreversible impact on individuals. In this context, relatively fixed and unchangeable physical features – such as fingerprints – are turned into machine-readable identifiers. Human rights experts are increasingly questioning whether some of these

[27] PI, Amnesty International and Centre for Research on Multinational Corporations (SOMO), "Operating from the Shadows: Inside NSO Group's Corporate Structure" (2021) https://www.privacyinternational.org/report/4531/operating-shadows-inside-nso-groups-corporate-structure

[28] PI, "Briefing: Controlling the UK's Private Intelligence Industry" (2022) https://www.privacyinternational.org/report/4850/briefing-controlling-uks-private-intelligence-industry For other examples, see PI, "Surveillance industry", https://www.privacyinternational.org/learn/surveillance-industry

[29] PI, Submission to the report on the right to privacy in the digital age by the UN High Commissioner for human rights (2022), https://privacyinternational.org/sites/default/files/2022-06/PI%20submission%20to%20OHCHR%202022%20report%20final.pdf

[30] UN Security Council Counter-Terrorism Committee Executive Directorate (CTED), Analytical briefing: Biometrics and Counter-terrorism (2021) https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Dec/cted_analytical_brief_biometrics_0.pdf

[31] PI, "Briefing on the Responsible Use and Sharing of Biometric Data in Counter-terrorism" (2020) https://privacyinternational.org/advocacy/4064/briefing-responsible-use-and-sharing-biometric-data-counter-terrorism

[32] PI, "Biometrics collection under the pretext of counter-terrorism" (2021) https://privacyinternational.org/long-read/4528/biometrics-collection-under-pretext-counter-terrorism

technologies, notably live facial recognition in public spaces,[33] can ever be deployed in ways that do not violate the right to privacy and other human rights, such as freedom of peaceful assembly;

- There is a rising danger of "function creep", notably the gradual widening of a technology use beyond its original, intended purpose;

- Biometric technologies can exacerbate exclusion and reproduce racial, ethnic, gender, social class, and other inequalities, as noted by the UN Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism[34] and the UN Special Rapporteur on contemporary forms of racism;[35]

- Many governments rely on the private sector to develop and implement technologies for state surveillance. Industries are well placed to influence government policies and to create the demand for tech solutions. Resulting public private partnerships can introduce vast biometric programs, which are often developed without adequate due diligence and prior human rights impact assessment;[36]

- The rapid deployment of biometrics technologies has not been met by commensurate changes at the level of law or policy in counter-terrorism context. National regulatory and legal frameworks continue to lag behind and, where they do exist, they are rarely effectively enforced, unable to properly safeguard against the hazards and potential misuses of biometrics. The 2021 CTED briefing notes the inadequacy of national legal frameworks, including on data protection and oversight and accountability mechanisms, and states that legislation establishing safeguards "must be developed prior to the implementation of biometric systems".[37]

A forthcoming report from ECNL also highlights problematic trends in the use of biometric technology for counter-terrorism and their impact on civic space and human rights defenders in India, Jordan, Mexico, Thailand, Turkey, Ukraine, and Uganda. The report documents the use of biometric systems to monitor and stifle protests and warns against the danger of repurposing biometric technologies, often developed with the encouragement and funding of international bodies, including the UN, to suppress legitimate expression and critique under the guise of counter-terrorism.

[33] International Network of Civil Liberties Organizations (INCLO) "In Focus: Facial recognition tech stories and rights harms from around the world " (2021) https://www.inclo.net/pdf/in-focus-facial-recognition-tech-stories.pdf

[34] Statement by Ms. Fionnuala ní Aoláin, Special rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (2021) https://www.ohchr.org/Documents/Issues/Terrorism/SR/Statementtransformative%20technologies_25Juin2021.docx

[35] "Report of the Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia and related intolerance, E. Tendayi Achiume on contemporary forms of racism, racial discrimination, xenophobia and related intolerance", A/75/590 (2020) https://undocs.org/A/75/590

[36] PI, "Safeguards for Public-Private Surveillance Partnerships" (2021) https://privacyinternational.org/our-demands/safeguards-public-private-surveillance-partnerships

[37] UN Security Council Counter-Terrorism Committee Executive Directorate (CTED), Analytical briefing: Biometrics and Counter-terrorism (2021) https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Dec/cted_analytical_brief_biometrics_0.pdf

Conclusions

As the above sections illustrate, there are significant concerns regarding the impact of terrorism and counter-terrorism or preventing or countering violent extremism conducive to terrorism measures on civil society and civic space.

Despite repeated recommendations by this mandate among others to review, amend or enact national laws to ensure respect and protection of civil society and civic spaces, national laws are often inadequate and do not regulate, limit or prohibit surveillance powers of government agencies, as well as data exploitative practices of companies.

Even when laws are in place, they are seldom enforced. In fact, the undersigned organisations note how it is often only following legal challenges in national or regional courts that governments are forced to act. This is not a sustainable position: CSOs, journalists, and human rights defenders often do not have the capacity (or legal standing) to challenge governments or companies' actions, they may face threats if they so (including of the same unlawful surveillance that they are challenging) and in many jurisdictions there are no independent avenues of effective redress.

The governments and companies introduced surveillance measures as emergency responses to the Covid-19 pandemic not only repurposed measures already in place for counter-terrorism purposes but also seem intent to continue using data-intensive and highly intrusive surveillance measures for other purposes, putting civil society and civic spaces further at risk.

Some surveillance technologies, such as live facial recognition technologies and hacking, are unlikely to ever meet the tests of legality, necessity and proportionality under international human rights law. The fact that in the name of countering terrorism, governments seem intent on taking measures that put the security and confidentiality of all our communications in jeopardy, and as a result threaten the enjoyment of all our human rights.[38]

Companies continue to offer surveillance and data analysis technologies to governments, not only feeding but encouraging a demand for data intensive solutions that usher the introduction of public private partnerships without adequate human rights due diligence and accompanying safeguards. Companies also continue to exploit our personal data by taking advantage of lack of regulation or enforcement.

[38] PI, "Privacy matters", https://privacyinternational.org/learning-resources/privacy-matters

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom

+44 (0)20 3422 4321

privacyinternational.org