United Nations A/HRC/62/45*

General Assembly

Distr.: General
21 April 2026

Original: English

Human Rights Council
Sixty-second session
15 June–10 July 2026
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Unmasking the chilling effects of the digital surveillance ecosystem: the erosion of assembly and association rights

Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Gina Romero**

Summary

In the present report, the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Gina Romero, addresses the threats to these rights posed by digital surveillance. Building on the previous work of the mandate, the report documents and reveals chilling effects associated with such surveillance, detailing the extensive interference with the effective exercise of assembly and association rights. It sets out how chilling effects should be incorporated into a human rights law analysis, centred around an acknowledgement of compound harms, and the prevailing surveillance ecosystem.

* Reissued for technical reasons on 21 May 2026.

** The annexes to the present document are circulated as received, in the language of submission only.

Please recycle

I. Introduction

1. In the present report, the Special Rapporteur on the rights to freedom of peaceful assembly and of association asserts the serious impact of digital surveillance[1] on the rights to freedom of peaceful assembly and of association, focusing specifically on surveillance-related chilling effects. By detailing these impacts, the report goes beyond the right to privacy and/or freedom of expression narratives that dominate existing research. This focus does not diminish the impact on those rights; rather, it identifies how chilling effects on public freedoms simultaneously affect a range of interconnected and interdependent rights, causing compound harm. Foregrounding the specific impacts on assembly, association and participation is essential, given their centrality to the effective functioning of democratic societies.[2]

2. Evidence for the present report was drawn from a global study[3] that included interviews and consultations with diverse participants across distinct contexts and jurisdictions. A total of 152 activists, human rights defenders, public defenders, lawyers, journalists and civil society actors across all regions[4] were interviewed to identify common and/or cross-cutting experiences of digital surveillance. One consultation was convened in the Middle East and North Africa region, two in Latin America, three in South-East Asia and two in Africa, alongside an online global event. This methodology was designed to produce robust data aimed at countering sceptical views that chilling effects are overly subjective, or difficult to measure effectively. The report is further informed by 62 written submissions – 49 from civil society, academics, international bodies and a major global tech company and 13 from States, and by data gathered in meetings with civil society and victims, during academic visits and on an official country visit. Collectively, this data concerns 84 States and entities, demonstrating the widespread nature of the chilling effects phenomenon.

3. An overview of key activities carried out under the mandate since January 2025 is provided in annex I to the report.

II. Normalization of surveillance

4. Heightened security concerns have been used to justify advances in surveillance systems, including those with dual civil/military capabilities.[5] Combined with increasing

[1] While this is not an exhaustive inventory of current and emerging capabilities, the Special Rapporteur identified growing use of the following surveillance practices: (a) compromised devices – onto which commercial cyberintrusion tools (spyware) such as Novispy, Pegasus and Predator have been loaded, and the use of digital forensic tools such as Celebrite, and International Mobile Subscriber Identity catchers to monitor mobile devices and owners' activities; (b) software and network-based intrusion – including the compromising and infiltration of communication platforms such as WhatsApp and Signal and of email accounts and communication lines, social media cyberpatrolling, and network manipulation, including Google Domain Name System interference; (c) biometric identification technologies – such as facial recognition technology, and gait and behavioural analytics that are often combined with other datasets to identify and monitor people and activities; (d) the adaptation of existing surveillance infrastructure – involving creep of urban surveillance camera networks and the repurposing of "smart city" initiatives (both of which are often managed through public-private partnerships), the use of aerial vehicles (drones) and of geospatial device tracking, and the leveraging of administrative data for surveillance purposes; and (e) State-administered digital platforms – including service provision apps that in some cases facilitate peer-to-peer reporting or serve as mechanisms for digital entrapment.

[2] The Special Rapporteur acknowledges support from the Queen Mary Centre for International Law at Queen Mary University of London; the Department of Sociology, Social Policy and Criminology at the University of Southampton; and UK Research and Innovation's Future Leaders Fellowship MR/T042133/2. She is also grateful for support provided by research assistants, volunteers and interns.

[3] "Pushed into the shadows: evidencing digital surveillance chilling effects and the erosion of the rights to freedom of assembly and of association", available at https://www.ohchr.org/en/special-procedures/sr-freedom-of-assembly-and-association/pushed-shadows.

[4] See annex II for a detailed methodology.

[5] See https://shorturl.at/0vEby and https://shorturl.at/68IL2.

global securitization and militarization of law enforcement and policing, these technologies exacerbate the complexity and severity of the threat to public freedoms.

5. Intrusive, expansive and high-risk digital systems, often inherently incompatible with human rights obligations, are often inappropriately justified through security[6] and crime prevention narratives – with broad claims invoked regarding national security, sovereignty, terrorism, public safety, transnational crime, cybersecurity, hate crimes, "moral crimes", disinformation and similar. Civic and political activism is increasingly used as an opportunity for surveillance. Associations and assemblies are often labelled as "national security threats", "foreign agents", "criminals" or "terrorists".[7] Authorities employ a blend of covert, hidden and online monitoring (including data scraping) strategies, alongside more overt visible forms (such as surveillance drones).

6. This normalizes the development of intrusive surveillance infrastructures (including in democracies). These are vulnerable to repurposing and surveillance "creep".

7. The normalization of digital surveillance is frequently anchored in security and crime-prevention justifications that lack empirical evidence regarding necessity or effectiveness. States have adopted overly broad measures that expand surveillance while circumventing transparency, public oversight and human rights safeguards. This shift toward a pre-emptive paradigm fundamentally erodes the presumption of innocence and due process; by forcing individuals to prove that they pose no threat, the State effectively reverses the burden of proof. This framework facilitates the wide-scale criminalization of activists, transforming the digital environment into a space of permanent suspicion.

8. The normalization of indiscriminate and pervasive surveillance undermines the core requirements of necessity and proportionality applicable to limitations on freedom of peaceful assembly and association.[8]

9. International counterterrorism and cybercrime frameworks lacking human rights safeguards contribute to the expansion and potential misuse of digital surveillance, facilitating transnational repression.[9] Instead of strengthening human rights-compliant legal frameworks, trends towards multilateral and national soft law regulation of powerful surveillance tools (such as commercial spyware) further the normalization of these tools.

III. Surveillance ecosystems in the digital era

10. Society-wide surveillance is a pervasive threat inherent to the modern digital environment. Digital tools and online-hosted processes are now central to basic human social, professional and economic activities. At the same time, social and economic processes rely on the processing of digital data. These factors increase the vulnerability of everyone to digital monitoring. The modern digital environment results in a step change in State and non-State actors' surveillance capability, including that of malicious entities, and enables "digital authoritarianism".

11. Digital surveillance occurs remotely, is largely invisible, involves multiple sources and is characterized by an inherent opacity and lack of transparency. This means that although individuals may be aware of the potential for surveillance, they do not – and often cannot – know if, when and how, surveillance is being practised, or by whom. This results in new power asymmetries, undermining the ability to challenge surveillance through public scrutiny or political or legal means.

12. Given the centrality of digital infrastructure to modern life, opting out of, or avoiding, surveillance is not feasible; this creates an unavoidable state of digital enclosure, framed as if surveillance were an accepted new normal.

[6] See A/HRC/52/39.
[7] A/HRC/56/49, para. 23: "The designation of LGBT groups as extremist or a threat to national security is another discernible trend."
[8] See A/HRC/55/60.
[9] See A/HRC/52/39 and https://tinyurl.com/2fs6frur.

13. Everyday digital devices have the capacity to be co-opted into powerful tools for surveillance: wearable fitness devices can be used to indicate a person's heart rate (or stress level) at a particular moment in time, electronic cards can trace journeys across public transport, and Wi-Fi or telecom network access can pinpoint an individual's presence at a specific location at a particular time.

14. Surveillance infrastructure is incorporated into most urban locations, including schools and workplaces. Many advanced surveillance tools are software-enabled and can be integrated into, and expand, existing surveillance infrastructures. Often introduced to address legitimate objectives, these tools are easily repurposed, including to suppress grass-roots activism, associations and peaceful assemblies.

15. Surveillance tools and practices are increasingly interoperable. Rather than distinct elements, they act in concert to amplify capabilities. For example, biometric identification may be applied to video feeds, be connected to complex data architectures (including social media intelligence, administrative records and commercial data broker profiles) and be analysed using artificial intelligence (AI). This marks a decisive shift from "data minimization", where only strictly necessary information is extracted, to "data maximization", where all available information is acquired, analysed and leveraged.

16. Digital surveillance facilitates algorithmic/AI analysis, unlocking its considerable power. This surveillance-assisted analysis can be used, for example, to track or monitor (an almost infinite number of) individuals, to generate pattern-of-life profiles, to identify "suspicious" activity, or to exercise control over individuals and populations. These tools can generate alerts when individuals enter or leave a particular area ("geofencing") or meet with specific people. These alerts serve as new data points, facilitating further investigation or real-time physical intervention.

17. This multiplies the degree of intrusion and facilitates the inference of information – for example on individuals' political views, affiliations with associations, participation in activities, sexual orientation, and health – as well as the locating and targeting of individuals.

18. Digital surveillance also extends into the private realm. Spyware is a prominent example; other forms of invasive surveillance include access to Internet communication records or to communications metadata.

19. Considered together, this transforms legitimate participation in associations, including civil society groups, or attendance at assemblies, into high-risk activities, especially for marginalized populations.

20. Rather than focus on specific tools and practices, it is more accurate to characterize these developments as constituting a surveillance ecosystem.

21. Surveillance ecosystems are composed of digital and data infrastructures operated by both State and non-State actors. Non-State actors, including commercial entities, possess detailed data on individuals that may be exploited for surveillance. In addition, the collection and sale of data has itself become a product. State access to telecom and digital data owned by private companies significantly extends the power and reach of authorities. Such access typically occurs through (formal or informal) sharing agreements or through law enforcement orders, sometimes exploiting regulatory gaps or national security exceptions. This State/non-State interaction lacks transparency, resulting in a lack of foreseeability which undermines the principle of legality.

22. The expansion of digital surveillance is also driven by the unchecked power of digital platforms and service providers, whose business models often rely on the mass extraction of personal data. By designing architectures that prioritize data harvesting, private tech actors have created the very infrastructure that States now exploit for surveillance. This public-private alignment facilitates a seamless transition from commercial data collection to State-led monitoring. When these companies prioritize profit or State compliance over user protection, they become complicit in the chilling effects that erode civic space.

IV. International normative framework relevant to technology and surveillance

23. The General Assembly and the Human Rights Council have consistently urged States to refrain from unlawful or arbitrary surveillance,[10] and to ensure that human rights are respected and fulfilled throughout the entire life-cycle of digital technologies, including AI. This includes pre-design, design, development, evaluation, testing, deployment, use, sale, procurement, operation and decommissioning. States must implement effective measures to prevent, mitigate and remedy adverse human rights impacts [11] through appropriate oversight.[12] These obligations are grounded in international human rights law, including the International Covenant on Civil and Political Rights and the Guiding Principles on Business and Human Rights.

24. Strict compliance with international human rights law, including adequate safeguards, is a prerequisite for the use or transfer of digital technologies. The Human Rights Council has affirmed that technologies should not be deployed if they cannot comply with human rights law or pose undue risks, and biometric recognition technologies should not be employed for mass surveillance. [13] These requirements reflect long-standing recommendations by the mandate and by regional bodies.[14]

25. Any digital surveillance technologies interfering with rights must conform with the principles of legality, necessity and proportionality. Their use must be based on an accessible and precise legal framework that clearly defines authorized purposes and the categories of persons targeted. Interference with the rights to freedom of peaceful assembly and association is permissible only in exceptional, limited cases, when strictly justified to pursue legitimate aims stipulated in articles 21 and 22 of the International Covenant on Civil and Political Rights. Surveillance must be limited in scope and duration – including for national security purposes – and applied only when "necessary in a democratic society". Any restrictions must be exceptional, the least intrusive, and preserve the essence of these rights. Surveillance measures require prior authorization, adequate and independent "end-to-end" oversight (assessing necessity and proportionality at every stage), and independent ex post facto review.[15] The Special Rapporteur asserts that a holistic evaluation of surveillance-related compound harms must be mandatory.

26. Effective human oversight of AI systems is essential to prevent or mitigate human rights risks, and to ensure that systems remain safe, ethical and accountable.[16]

27. However, these standards are frequently undermined by broad counter-terrorism and cybercrime measures, and national security exemptions in global, regional and national frameworks, alongside a lack of political will to regulate high-risk surveillance technologies, some of which may be per se incompatible with States' human rights obligations.[17] This is often driven by opaque State-corporate collaborations that disregard human rights obligations, and coercive pressure from both States and corporations to remove guardrails preventing abuse or misuse.[18]

[10] General Assembly resolution 78/213 and Human Rights Council resolution 59/4.
[11] General Assembly resolution 78/213.
[12] General Assembly resolutions 77/211, 78/213 and 80/215.
[13] Human Rights Council resolution 58/23.
[14] See https://shorturl.at/Xb3cW.
[15] European Court of Human Rights, *Ekimdzhiev and Others v. Bulgaria,* Application No. 70078/12, Judgment, 11 April 2022; *Green Alliance v. Bulgaria*, Application No. 6580/22, Judgment, 17 February 2026; *Big Brother Watch and Others v. the United Kingdom*, Applications Nos. 58170/13, 62322/14 and 24960/15, Judgment, 25 May 2021; and Inter-American Court of Human Rights, *Members of the "José Alvear Restrepo" Lawyers Collective v. Colombia,* Judgment, 18 October 2023.
[16] General Assembly resolutions 79/175 and 78/265; and European Union Artificial Intelligence Act.
[17] Fionnuala Ní Aoláin, "One step forward? Agreement on spyware regulation in the Pall Mall Process", 9 May 2025.
[18] See https://tinyurl.com/4jmf86aa, https://tinyurl.com/ycxxhkjm, https://tinyurl.com/e6mu9x9u and https://tinyurl.com/rtch62xu.

28. Under international human rights law, States must ensure that surveillance, including digital surveillance, does not unduly interfere with freedom of peaceful assembly and association. These legal obligations remain applicable during public emergencies, where surveillance measures must never unduly interfere with public freedoms.[19] Likewise, digital surveillance and the development and use of new and emerging technologies in the military domain must comply with international human rights law and humanitarian law throughout its entire life cycle.[20]

V. Core elements of assembly and association rights relevant to digital surveillance

29. The centrality of association and assembly to a vibrant democracy is widely recognized.[21] Civil society[22] – and the media[23] – serve as "public watchdogs" essential to democratic processes, therefore any interference with these rights also directly impacts the right to participate in public affairs.[24] Given the enabling and interconnected nature of the rights to freedom of peaceful assembly and association, undue interference diminishes the ability to advocate for all human rights. This undermines human dignity, stifles democratic agency, and restricts the pursuit of just and peaceful societies – ultimately stalling progress in critical areas such as sustainable development, climate justice, security and peace.[25]

30. In the present report, the Special Rapporteur addresses the core elements of the rights to freedom of peaceful assembly and of association, emphasizing their effective protection in practice. The Special Rapporteur focuses on those components that enable individuals, associations, social movements and assemblies to act freely, in pursuit of their set objectives. Specifically, she focuses on the ability to organize, mobilize, access and manage resources (including foreign funding), and on other essential and legitimate activities such as planning, choice of strategy and/or objectives, dissemination of information, communication and expression, free movement, and access to solidarity.[26]

31. Organizing and mobilizing for civic or political activism depends on sustained engagement by individuals and/or groups.[27] Easy communication is essential for disseminating information, accessing resources, mobilizing participants and supporters and securing protection and justice. Here, resilience and trust are fundamental.[28] Any undermining of resilience hinders the ability to build and sustain collective action, and to generate and share knowledge or maintain collective memory and solidarity. Similarly, the erosion of interpersonal trust results in desocialization, restricting individuals' and groups' ability to communicate freely and act effectively.[29] This reinforces isolation and increases

[19] See A/HRC/50/42 and https://shorturl.at/BYrPy.

[20] General Assembly resolution 79/239 and A/C.1/80/L.46.

[21] Human Rights Committee, general comment No. 37 (2020), paras. 1 and 12; A/HRC/20/27, paras. 24 and 51; A/77/171, paras. 5, 8 and 36; A/HRC/31/66, para. 5; Yogyakarta Principles on the Application of International Human Rights Law in relation to Sexual Orientation and Gender Identity, principle 20; Committee on the Rights of the Child, general comment No. 25 (2021), para. 64; and European Court of Human Rights, *Gorzelik and Others v. Poland*, Application No. 44158/98, Judgment, 17 February 2004, para. 93.

[22] European Court of Human Rights, *Magyar Helsinki Bizottság v. Hungary*, Application No. 18030/11, Judgment, 8 November 2016, para. 167; and *Szabo and Vissy v. Hungary*, Application No. 37138/14, Judgment, 6 June 2016, para. 38.

[23] European Court of Human Rights, *Jersild v. Denmark*, Application No. 15890/89, Judgment, 23 September 1994, para. 31.

[24] A/HRC/59/44, para. 1; and Human Rights Committee, general comment No. 25 (1996).

[25] See A/HRC/59/44 and A/78/246.

[26] Human Rights Committee, general comment No. 37 (2020), para. 33; A/HRC/53/38/Add.4, para. 7; and A/77/171, para. 4.

[27] Human Rights Committee, general comment No. 37 (2020), para. 33.

[28] A/77/171, para. 52; and Daragh Murray, Pete Fussey, Kuda Hove, Wairagala Wakabi, Paul Kimumwe, Otto Saki and Amy Stevens, "The chilling effects of surveillance and human rights: insights from qualitative research in Zimbabwe and Uganda", *Journal of Human Rights Practice*, vol. 16, issue 1 (February 2024).

[29] A/77/171, para. 52.

vulnerability to stigmatization, repression or unjust closure.[30] Trust and social fabric is deeply affected also when service-provision apps promote peer-to-peer reporting, such as in China and Venezuela (Bolivarian Republic of).[31]

32. The rights to freedom of association and of peaceful assembly apply without discrimination to everyone – including citizens, non-citizens[32] and children[33] – and State obligations to facilitate these rights are "content-neutral".[34] The independence of associations must be protected.

33. Human rights law clearly recognizes the importance of unobstructed civic space – both physical and digital – for the exercise of these rights.[35] Within this space, the ability to act anonymously or to selectively reveal aspects of one's identity is vital for enabling individuals to participate in public life[36] and pursue their chosen objectives. Furthermore, the importance of spontaneity in responding to urgent community needs, and the inherently disruptive nature of peaceful assemblies, are also recognized and protected.[37]

34. Access to justice is integral to the effective exercise of these freedoms. A lack of transparency around digital surveillance, and inadequate legal safeguards, prevent accountability, interfering with the effective exercise of these rights.[38]

A. Intersectional harms

35. Digital surveillance, and its chilling effects, give rise to clear intersectional harms. These impacts amplify pre-existing sociopolitical vulnerabilities and historical discrimination.

36. As has been reported by the mandate, stigmatization[39] routinely targets women and marginalized activists through digital surveillance techniques involving spyware, social media monitoring, or "doxxing". These efforts, aimed at causing reputational harm and prompting withdrawal, frequently involve sexualized attacks, including deepfakes, or the forced "outing" of LGBTQI+ activists. Such tactics weaponize technology to silence diverse voices within civic space.

37. Public space surveillance erodes sociocultural life. Fear of being labelled "foreign agents", "criminals", "terrorists" or "troublemakers" or being given some other label deters individuals from appearing in public. Impacts are accentuated in repressive contexts, especially for criminalized associations, protest groups, and individuals with uncertain migration status. Furthermore, surveillance carried out near service providers restricts access to social care, including healthcare, while surveillance at academic institutions harms children and youth, interfering with their education, self-esteem, identity and career development. Similarly, surveillance-introduced chilling effects disproportionately harm marginalized and racialized communities, and individuals or groups challenging the status quo, speaking truth to power, demanding justice and accountability for human rights violations and/or leading anti-corruption agendas.

38. The discriminatory impacts of AI surveillance tools, including facial recognition and predictive algorithms, are well documented.[40] This has been corroborated by inputs

[30] A/80/219, para. 86.
[31] See https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=29302.
[32] Human Rights Committee, general comment No. 37 (2020), para. 5.
[33] Convention on the Rights of the Child, art. 15.
[34] Human Rights Committee, general comment No. 37 (2020), para. 21.
[35] Ibid., paras. 1 and 53; CCPR/C/108/D/1948/2010 and CCPR/C/108/D/1948/2010/Corr.1, para. 7.4; and A/77/171, para. 53.
[36] Human Rights Committee, general comment No. 37 (2020), para. 60; and A/HRC/44/24, para. 24.
[37] Human Rights Committee, general comment No. 37 (2020), para. 47.
[38] See A/HRC/47/24 and A/HRC/53/38/Add.4.
[39] See A/79/263.
[40] See, for example, Simone Browne, *Dark Matters: On the Surveillance of Blackness* (Duke University Press, 2015).

documenting how biased AI systems disproportionately affect, among others, people of African descent, ethnic and religious minorities, and children.

B. Human rights due diligence and digital surveillance technologies

39. To fulfil human rights obligations, States and corporations must conduct rigorous due diligence to assess digital surveillance impacts. A robust "necessity" analysis requires a holistic evaluation of the utility versus harm. This holistic "compound harm" approach is essential, as evaluations are too often limited to privacy or freedom of expression; while critical, these represent only part of the picture. Comprehensive human rights impact assessments must explicitly include freedom of assembly and association, alongside any other rights engaged. Assessing utility and harm must be evidence-based, and context- and/or tool-specific, consider intersectional harms, and adopt interdisciplinary methods.[41]

40. Human rights impact assessments are critical for emerging technologies, where the full extent of human rights consequences is often not immediately foreseeable and tends to compound over time.

VI. Introduction to chilling effects

41. Surveillance-induced chilling effects arise when individuals change their behaviour due to concerns about the consequences of actual, suggested or perceived monitoring. Chilling effects are diverse, influencing social media engagement, websites visits, search queries, and meeting attendance (including online). They impact who people talk to, what they say, their public or private social activities, and if (or how) they participate in democratic processes and political activities, among other things. Chilling effects may deter individuals or collectives from organizing or participating in assemblies, from associating or engaging with specific actors (e.g. authorities, donors, partners, communities, victims, journalists, lawyers and others) or from engaging in activities.

42. Chilling effects are not exclusively binary. They are varied and nuanced, including in intensity and impact. They extend beyond routine practices designed to preserve privacy and anonymity, such as virtual private network use or robust organizational security cultures. They may induce changes to intended activity. For instance, assemblies or associations may adopt a "softer" or more "acceptable" approach to communication, while associations may choose to operate in less visible ways.

43. In the present report, the Special Rapporteur details how people subjected to surveillance and the threat of surveillance often face serious consequences and high levels of repression, including stigmatization, intimidation, criminalization, arbitrary detention, threats to life, and others.

44. Chilling effects extend far beyond the targets of surveillance (real or perceived), impacting family members, communities, social movements and society. Surveillance chilling effects are long-lasting and apply beyond any actual or suggested monitoring activity, sometimes over generations.

45. Chilling effects arise from many sources and are inspired by assumed consequences of direct and visible manifestations of surveillance, and more remote and ambiguous suggestions of surveillance.

46. In some cases, digital surveillance activities are clandestine, and in other cases they are openly pursued and instrumentalized with the explicit intention to deter and chill activism and dissent. Both exert profound chilling effects.

47. Remote and invisible digital monitoring brings constant ambiguity over whether surveillance is occurring. This is compounded by insufficient transparency regarding surveillance activities, data processing and retention, opaque access restrictions regarding captured information, and the complex (and often undeclared) nature of who owns, operates

[41] A/HRC/55/60, para. 24.

and manages surveillance systems and gathers data. Existing laws are often inadequate, granting broad, permissive powers, lacking safeguards and offering inadequate accountability. Individuals often have little choice but to operate under the permanent assumption of surveillance.

48. While chilling effects are widely recognized by human rights bodies and in case law,[42] the chilling effects arising from today's digital surveillance have not yet been incorporated into an effective human rights law analysis. To date, human rights jurisprudence has primarily addressed more long-standing forms of surveillance[43] or the chilling effects of these.[44] By failing to account for the distinct nature of digital surveillance, current legal frameworks struggle to fully acknowledge overall harm to human rights and freedoms.

VII. Chilling effects-related interference with the rights to freedom of assembly and of association

49. The trends detailed here are indicative of the experiences of those who provided evidence for the present report (152 diverse actors across the world; 62 written submissions[45]) – their quotes are representative of widely shared experiences present in the data. Each reference is therefore not an exhaustive list of those experiencing each issue. Depending on participant consent, and safety concerns, some submissions or quotes are referred to by country or region, rather than organization or other direct identifier, to preserve anonymity.[46]

50. Digital surveillance has reshaped the ability to remain anonymous in public. Technologies, particularly facial recognition technology, enable the rapid, precise identification and tracking of individuals participating in public assemblies and in associations' activities. Activists from all regions consulted documented how real-time monitoring of crowds and retrospective identification of individuals from captured images heightened chilling effects, depleted anonymity, led to arbitrary, preventive and mass arrests and reduced public participation at assemblies.[47] Expanding surveillance capabilities critically affects the ability to participate in civic space, including in labour rights actions as digital surveillance has been used to target trade union members and organizations.

51. State and non-State actors' increasing use of covert surveillance to monitor peaceful assemblies fundamentally alters the presumption of innocence and the ability to participate without interference. Participants in university-based pro-Palestine solidarity movements worldwide reported intensified campus surveillance, including new cameras, facial recognition systems and enhanced social media monitoring.[48] One academic placed under covert surveillance prior to giving a lecture at one university in the United Kingdom of Great Britain and Northern Ireland explained: "You're supposed to be innocent until proven guilty ... But they started investigating me ... because of my scholarship. I am a Palestine scholar. What am I supposed to study and teach about to avoid this unwarranted, unfair and unjust scrutiny and surveillance?"[49] This resonates with the wider practice of British universities

[42] Human Rights Committee, general comments No. 37 (2020) and No. 34 (2011); A/HRC/27/37; A/HRC/56/50; A/HRC/23/40; Inter-American Court of Human Rights, *Members of the "José Alvear Restrepo" Lawyers Collective v. Colombia,* Judgment, 18 October 2023; and European Court of Human Rights, *Glukhin v. Russia*, Application No. 11519/20, Judgment, 4 October 2023.

[43] Pete Fussey and Daragh Murray, *Facial Recognition Surveillance: Policing and Human Rights in the Age of Artificial Intelligence* (Oxford University Press, 2025); and European Court of Human Rights, *Catt v. the United Kingdom*, Application No. 43514/15, Judgment, 24 April 2019, para. 123.

[44] European Court of Human Rights, *Navalnyy v. Russia,* Applications Nos. 29580/12, 36847/12, 11252/13, 12317/13 and 43746/14, Judgment, 15 November 2018, para. 103; and *Baka v. Hungary*, Application No. 20261/12, Judgment, 23 June 2016, para. 173.

[45] See annex 2.

[46] See the global study, available at https://www.ohchr.org/en/special-procedures/sr-freedom-of-assembly-and-association/pushed-shadows.

[47] Second, third and fourteenth interviews, first South-East Asia consultation, first Africa consultation, and civil society written submissions from the United Kingdom of Great Britain and Northern Ireland, Serbia and Georgia.

[48] See https://tinyurl.com/mrbdx9ku.

[49] Submission from Liberty Investigates.

and their peers in the United States of America contracting private intelligence companies to investigate pro-Palestine activists in advance of protests, often under companies' pressure.[50]

52. Increased monitoring of physical locations has influenced the appeal of online assemblies, which have become a vital lifeline, especially for exiled activists. Yet, this transition creates a further dilemma: in some cases, scrutiny from street-based surveillance may be reduced by moving online, but then vulnerability, visibility and exposure increase through less perceptible digital surveillance. Participants face blanket censorship, intrusive surveillance, targeted harassment and arrest. Authorities use digital spaces as tools of surveillance and control, tracking individuals' online activity to identify, locate and detain those engaged in activism. One Afghan woman activist described an experience of "authorities weaponizing the digital space against them; Taliban officials track down activists via their online activity and arrest them".[51]

53. Online associations and assemblies are also disproportionately at risk of blanket Internet shutdowns. These apply to specific phases of protest, as seen throughout 2026 in the Islamic Republic of Iran, and routinely at critical events, including Human Rights Day, Cinco de Mayo and others.[52]

A. Restricted engagement and "desocialization"

54. Digital surveillance is linked to the limiting of individuals' and organizations' contact with each other. Reported measures taken in response include avoiding meetings involving digital technology; limiting communications regarding strategy, organization or advocacy; and general isolation from personal and professional connections. This affects targets of surveillance and, vicariously, those fearing guilt by association or increased surveillance targeting through association. Such self-isolation necessarily restricts access to advocacy channels, funding and protections, exacerbating seclusion and diminishing the ability to pursue strategic objectives.

55. Surveillance exerts a clear deterrent effect, undermining participant and supporter (including volunteer) mobilization, staff recruitment, and – among other effects – discouraging people from joining or sustaining their engagement with sociopolitical groups.[53] This creates a process of desocialization and reduction of collective activity where chilling effects "amount to a de facto dissolution of organizational spaces"[54] and elimination of political engagement.[55]

56. Surveillance chilling effects force movements towards decentralization in order to counter exposure and avoid compromising partners, making unified collective action less viable.[56] Many organizations expressed a reluctance to communicate with individuals or organizations with inadequate digital security,[57] while others had suspended their membership in solidarity movements that attracted high levels of State scrutiny.[58] Chilling effects induce limitations on organizations; these undermine a core element of movement-building.[59]

[50] See https://tinyurl.com/5ayc7yz7 and https://tinyurl.com/mrbdx9ku.
[51] Civil society written submission from Afghanistan; sixteenth interview (Nigeria); and first Africa consultation.
[52] First Latin America consultation (Cuba). See also A/HRC/47/24/Add.2.
[53] Civil society written submissions from Italy, Pakistan, Spain and the United States of America; first Africa consultation; second South-East Asia consultation; and second and third Latin America consultations.
[54] Civil society written submission from the Centre for Human Rights and Justice, Bolivarian Republic of Venezuela.
[55] First and third South-East Asia consultations.
[56] Second Latin America consultation (Bolivarian Republic of Venezuela); and ninth interview (United States).
[57] Twelfth and thirteenth interviews.
[58] Ninth interview (United States) referencing pro-Palestine movements; and tenth interview.
[59] First South-East Asia consultation.

57. Surveillance chilling effects are enduring and continue long after distinct monitoring activities have concluded. This lasting impact is particularly apparent among victims of spyware attacks. Balkan journalists reported how a colleague whose device had been "infected with Pegasus" became ostracized and regarded as if he were "literally infected".[60] Commonly, spyware victims detailed multilayered chilling effects, such as long-term exclusion, professional demise, and self-imposed censorship to protect others, including beneficiaries.[61]

B. Interfering with the "public watchdog" function

58. Surveillance chilling effects limit access to sources needed to expose human rights violations, fundamentally altering relationships with whistle-blowers,[62] those advocating within excluded communities,[63] labour movements,[64] and journalists seeking to expose human rights harms.[65] Reporting in the context of surveillance has become significantly more complex,[66] involving fewer sources,[67] and with some journalists and protest monitors electing to avoid reporting on demonstrations.[68]

C. Fear of compromising others

59. Professional disassociation to protect others is a direct consequence of digital surveillance. Civil society activists in Algeria described fear of exposing colleagues to national security levels of State surveillance.[69] Activists in Myanmar explained how surveillance chilling effects had forced interactions into limited, highly dangerous and clandestine forms.[70] Activists in Australia, Brazil and the United States, in Europe and across Africa described undertaking constant information-filtering to reduce others' exposure to harm and criminalization.[71] As one Indigenous rights activist described it: "It's harder, and less ethical, to convince communities to speak up."[72]

60. Concern over family members was consistent in each consultation region and across multiple countries, demonstrating how chilling effects consistently extend beyond the direct subjects of surveillance to include unrelated individuals. Family-related collateral chilling effects disincentivized many activists from engaging in peaceful assemblies,[73] particularly after the seizure of devices and subsequent exposure of personal networks.[74]

61. Family-related concerns illustrate the transnational dimension of chilling effects. This dynamic was experienced globally and is demonstrated, for example, by the experiences of exiled Tibetan activists who consistently curtailed activities in destination countries in response to threats to family at home.[75] As digital surveillance has expanded, so has the impact of this effect. Many first-hand accounts detailed transnational repression against exiled Chinese and diaspora communities overseas, affecting peaceful assembly in third

[60] Eighth interview.
[61] Seventh and eighth interviews.
[62] Fourth interview (Serbia).
[63] First Latin America consultation.
[64] Second and third Latin America consultations.
[65] Middle East and North Africa consultation; and fourth Latin America consultation.
[66] Fourth Latin America consultation.
[67] Seventh interview; and second Africa consultation.
[68] Second Latin Amercia consultation (Argentina).
[69] Middle East and North Africa consultation.
[70] First South-East Asia consultation.
[71] Second Latin America consultation; fourth South-East Asia consultatoin (Australia); third interview (Germany); ninth interview; and first Africa consultation.
[72] First Latin America consultation.
[73] Ninth interview; first and third South-East Asia consultations; first Africa consultation; Middle East and North Africa consultation; and second Latin America consultation.
[74] Eleventh interview.
[75] Second and third South-East Asia consultations.

countries, regardless of the human rights protections existing there.[76] Similar first-hand experiences were reported by activists from Bahrain, Ethiopia, Georgia, Uganda, Belarus and Russia and the United Republic of Tanzania, among many others.[77] An Afghan activist described this experience as having "shattered everything in my life",[78] while activists in the Middle East and North Africa region stated that parents, relatives and friends were arrested or disappeared if exiles participated in advocacy abroad.[79]

62. Family-related chilling effects affect individuals in profound ways. These include forced isolation and intentional severing of ties with loved ones – including children – for their protection,[80] and avoiding contact at times of ill-health and bereavement.[81]

D. (Mis)trust and stigmatization

63. Surveillance nurtures a climate of mistrust and undermined solidarity. This involves a constant mental process of recalibrating trust. As one civil society actor explained: "Trust is no longer automatic. It must be negotiated every day."[82] Digital surveillance has transformed civil society security culture, bringing unwarranted suspicion to some groups[83] and forcing others into more complex and resource-intensive forms of communication to establish trustworthiness.[84]

64. Mistrust induced by surveillance chilling effects has a major impact on personal relationships,[85] and "fractured the ability to socialize and have normal human relationships because you can't really be your full self".[86] In more extreme cases, trust becomes highly conditional, such as on a shared willingness to face prison.[87] Mistrust induced by chilling effects also disrupts relationships with intimate partners.[88]

65. Stigmatization efforts deplete the capacity to organize and mobilize.[89] Surveillance serves a dual function: it gathers information to fuel initial stigmatization and then uses the stigmatized status to justify further surveillance. Tactics include leaking private information collected through illegal surveillance – including the monitoring of intimate domestic spaces – to threaten and discredit activists through smear campaigns.[90]

66. Victims of police violence have been singled out for stigmatization efforts.[91] Such tactics serve to discredit future protests and exert a noticeable chilling effect on those on the cusp of organizing or joining movements.[92]

67. Online stigmatization often has a gendered dimension, with abuse and threats of sexual violence against women activists. The use of social media to tarnish the reputations of high-profile civil society actors is a frequent occurrence.[93] Harms may be exacerbated in deeply conservative and discriminatory contexts. In Afghanistan, civil society actors reported

[76] Second South-East Asia consultation; and see https://shorturl.at/fZD5X and https://shorturl.at/OuZ85.
[77] Fifth, fourteenth, sixteenth and seventeenth interviews. Civil society written submissions.
[78] Civil society written submission from Afghanistan, accounts 31 and 32.
[79] Middle East and North Africa consultation.
[80] Civil society written submission from Afghanistan; first and third South-East Asia consultation; fifteenth interview (West Africa); and first Africa consultation.
[81] Civil society written submission from Afghanistan; and first Africa consultation.
[82] Middle East and North Africa consultation.
[83] Fourteenth interview.
[84] Fourth and fifteenth interviews; and second Latin America consultation.
[85] Fifteenth interview; and first South-East Asia consultation.
[86] Ninth and fourteenth interviews.
[87] Fourteenth interview.
[88] First, eleventh and fourteenth interviews.
[89] Fourth South-East Asia consultation; sixth Latin America consulation; and first Africa consultation.
[90] Amy Stevens, Pete Fussey, Daragh Murray et al., "'I started seeing shadows everywhere': the diverse chilling effects of surveillance in Zimbabwe", *Big Data and Society*, vol. 10, No. 1 (2023).
[91] First and second Latin America consultations.
[92] Ibid.
[93] Second South-East Asia consultation; sixteenth interview; and second and sixth Latin America consultations.

how arrested female activists are frequently threatened with the online dissemination of photos or videos of abuse and humiliation taken during their detention if they continue to speak out.[94]

68. Experience of actual and/or attempted infiltration of professional or social networks and associations are common drivers of chilling effects. In many countries, physical and digital coercion work in tandem, with physical confiscation of phones facilitating the infiltration of digitally hosted networks via compromised devices. This, in turn, affects the degree of trust between activists, impairing their ability to freely communicate and to organize.[95]

69. Activists in South Sudan described pervasive and deliberate infiltration designed for the explicit purpose of intimidation. This undermined the ability to organize, mobilize and act. In South-East Asia, the compromising of digital chat groups was so common that activists described private conversations as a "semi-public sphere", with infiltration intended as a means of shutting down discussion – as an "act of disruption".[96] Similar practices are reported in Togo.

70. Sometimes infiltration is conducted entirely online, often through impersonation or spoofing.[97] Several African civil society organizations suspected State-corporate complicity through the reassignment of and subsequent access to cell phone numbers, and SIM cloning, allowing for surveillance or for the sending of threatening or suspicious messages.[98] This includes reports from Kenyan activists concerning the use of cloned SIM cards to send messages aimed at fostering mistrust between intimates or directing people towards locations where they would face police harassment.[99] Victims of hacking and impersonation report consequences similar to those of individuals affected by spyware, notably long-term ostracization and an inability to maintain professional networks.[100] Intentional intimidation tactics demonstrate how those conducting surveillance understand that chilling effects exist, and that they have a debilitating impact on targets.

71. Some law enforcement agencies, such as in Argentina, Bangladesh and Thailand, use cyberpatrolling to monitor social media and arbitrarily interfere with assemblies, including those held in private.

E. Limits on information retention and sharing

72. Fear of surveillance significantly impairs the flow of information. Activists from conflict and militarized areas, such as Darfur, Sudan, and South Sudan, described how searches, harassment and targeting at frequent physical checkpoints created chilling effects on one's engagement and on the ability to share information.[101]

73. In the Sudan, physically transporting materials risked device seizure, especially at checkpoints, where individuals were frequently coerced into unlocking devices for inspection. Journalists and rights defenders are reportedly singled out.[102]

74. Tibetan activists described how surveillance chilling effects slowed information flows across national borders, severely limiting the capacity of exiled and diaspora civil society organizations.[103] In extreme cases, surveillance chilling effects limited access to basic communication tools. This includes activists abandoning the use of phones following

[94] Civil society written submissions from Afghanistan.
[95] First Africa consultation; Amy Stevens, Pete Fussey, Daragh Murray et al., "'I started seeing shadows everywhere': the diverse chilling effects of surveillance in Zimbabwe"; and second Latin America consultation.
[96] First South-East Asia consultation.
[97] First Africa consultation.
[98] Ibid.
[99] Second Africa consultation.
[100] First Africa consultation; and civil society written submission from Pakistan.
[101] First Africa consultation.
[102] Ibid.
[103] Third South-East Asia consultation.

arrest,[104] and the common practice of blocking all contacts following mobile device seizures.[105]

75. These chilling effects-induced limitations on the ability to communicate exert a long-term impact by undermining the community memory needed to sustain organizations and movements.

76. Labour-intensive alternatives – such as travelling to meetings rather than communicating online, or physical transporting rather than sending data – results in less information sharing and reduced timeliness and relevance of what is shared.[106] Additional labour may also be required to reassemble fragmented information, often at the cost of accuracy. In conflict zones such as Darfur, where information can be a matter of life and death, and verification involves decisions over exposing individuals, civil society organizations relayed how accessing information is complex but necessary to divert people on the move from danger, yet communicating fragments of reports may lead to further risk.[107]

F. Reduced visibility and its impacts

77. Heightened surveillance and stigmatization impact the public visibility of civil society actors, associations, assemblies and journalists, directly limiting their ability to connect, act and communicate freely. Many actors reduced their social media and public presence, severely impacting their outreach, mobilization, and access to resources; therefore, their impact and the reach of their objectives.[108] As representatives from Latin America and Africa civil society explained, "who is going to fund an organization that isn't visible?".[109] In Tunisia, civil society actors described the, "need to work more silently", reporting similar impacts on accessing funding. These chilling effects exert a double disadvantage: the reduced utility of digital tools and civic space, and a perceived need to self-censor against criminalization: "Visibility carries enormous risk … We communicate less publicly, more in the shadows."[110]

78. Organizations in Kenya and Venezuela (Bolivarian Republic of) felt impelled to relocate multiple times and to maximize their distance from State attention, which in turn increased their remoteness from their professional networks.[111]

79. Many organizations dismantled visible public-facing profiles and withdrew from social media. Some in the Bolivarian Republic of Venezuela deleted their own organization's website and repository of online information in the face of government harassment – a self-protective measure that results in the erasure of institutional memory of the sector.[112] In Argentina, many working for human rights non-governmental organizations elected to keep their human rights work secret.[113] Forced erasure of one's social media presence, sometimes losing hundreds of thousands of followers cultivated over a period of years, is common.[114]

G. Resource and operational implications

80. Digital surveillance chilling effects diminish the finances and, hence, the capacity of civil society organizations. In a financially constrained sector,[115] diverting resources to

[104] First Africa consultation; and civil society written submission from Afghanistan.
[105] First interview.
[106] Second and fourth Latin America consultations.
[107] First Africa consultation.
[108] Civil society written submissions from Argentina, India, Indonesia, Italy, Myanmar, Spain, Uganda, United Republic of Tanzania, United States and Venezuela (Bolivarian Republic of).
[109] Third Latin America consultation; and second Africa consultation.
[110] Middle East and North Africa consultation.
[111] Third Latin America consultation; and second Africa consultation.
[112] Third Latin America consultation.
[113] Second Latin America consultation (Argentina).
[114] First interview.
[115] See A/80/219.

mitigate the threat and impact of surveillance necessarily limits the ability of individuals, movements and organizations (including donors) to freely pursue their strategic objectives.

81. The following describes a common experience: "The chilling effect impacts … all the protection measures. [It] requires a lot of effort, time, resources and money."[116] "This level of surveillance is not normal … It has affected, in both the strategic and the operational sense, the way we work. A lot of resources, time and energy are dedicated to … mitigating surveillance."[117]

82. Other direct financial implications involve the need to arrange alternative remittance processes and clandestine forms of financing to pay staff under surveillance in order to maintain secrecy and reduce vulnerability.[118]

83. More costly travel and logistical arrangements are often required in order to build trust and evade surveillance.[119] One Indigenous rights activist noted that, in the Amazon, "due to the politics of fear, 50% of our budget today has to be destined for mobilization; travelling to convince people that it is safe".[120]

84. The problem of diverting resources to mitigate digital surveillance vulnerabilities was reported across all regions, significantly interfering with the ability to act in pursuit of strategic objectives. At an organizational level, heightened security in the face of digital surveillance involves a major strategic investment.[121] This diversion of funds necessitates additional effort to justify the shifting priorities to donors.

85. Organizational resources are also strained in response to spyware attacks. This involves the laborious mapping of victims' networks and contacts to reveal the "surveillance collateral"[122] of such attacks, including the detailing of who may be exposed by infections.[123]

86. Civil society actors across Africa and South-East Asia noted that organizational size dictates capacity to invest in digital security measures, with grass-roots and smaller groups facing the hardest choices and greatest vulnerability,[124] a situation worsened by the change in the financial ecosystem, including the cancellation of funding from the Government of the United States.[125]

87. Disparities in digital security therefore exist between different civil society organizations. For example, remote and smaller groups routinely find themselves more exposed and required to commit a greater percentage of their budget towards this activity when compared to large international civil society groups.[126]

H. Impact of chilling effects on the individual

88. Surveillance-induced chilling effects affecting freedom of association and assembly have profound impacts on the individual. These manifest in several, critical ways, affecting the intimate spheres of life. Beyond economic, cultural and social consequences, they have an impact on people's ability to function in society and to access vital services.

89. Many civil society actors described how the belief of being under surveillance cripples interpersonal trust and social relationships.[127] The mistrust, isolation and fractured social

[116] Third South-East Asia consultation.
[117] Sixth interview.
[118] Second Latin America consultation.
[119] Fourth interview.
[120] First Latin America consultation (Brazil).
[121] Fourth interview.
[122] Daragh Murray and Pete Fussey, "Bulk surveillance in the digital age: rethinking the human rights law approach to bulk monitoring of communications data", *Israel Law Review*, vol. 52, No. 1 (2019).
[123] Third South-East Asia consultation.
[124] Second South-East Asia consultation.
[125] First Africa consultation.
[126] Fourth interview.
[127] Civil society written submissions from Thailand, Uganda and the United States. This accords with academic research on the impact of chilling effects from surveillance on interpersonal trust: see

relations create deep psychological stress, affecting "every aspect of an activist's life". Such intrusion "fundamentally transforms how activists live: every conversation becomes suspect, every relationship potentially compromised, and every private moment subject to unknown observation".[128]

1. Individual psychology and hypervigilance

90. A state of constant hypervigilance in response to perceived surveillance was a common experience among those consulted. This significantly undermines resilience and the ability to sustain long-term engagement.

91. Many participants had serious reasons for their state of heightened alert. In South Sudan, activists believe biometric surveillance was used to identify and murder people involved in protests.[129] In Ethiopia, hypervigilance followed direct intimidation, including burglaries encountered when arriving at undisclosed safe houses.[130] The psychological toll of being physically followed, compounded by digital surveillance, was a common experience in all global regions. Levels of vigilance also increased following pressures to outwardly act "normally".

92. Many activists felt surveillance was constant and ubiquitous: "Everyone feels that they're surveyed, that someone is following them."[131]

93. The significant and intrusive presence of hypervigilance in the mental landscape of activists was a common experience. Representative accounts included: "I became a little bit paranoid, but I think it's good paranoia"[132] and "It was very weird … I'm not paranoid but it was just this huge gut feeling that something is wrong";[133] and being gaslit into questioning one's own sanity: "You're always in a situation when you don't know when you're alone and when you're not alone ... Are you paranoid just?"[134] One Ethiopian activist described how such hypervigilance became normalized into a habitual state of anxiety: "I can't go out in public … because you're paranoid all the time, especially if you have children … you're always paranoid."[135] Others described the absence of respite at home: "I try to control it to some extent, but then these invasive thoughts, negative feelings, you know, fear that something might happen, are still there, so it's difficult to deal with it."[136]

94. Several reasons underpin the enduring nature of hypervigilance. One is the belief that surveillance will happen irrespective of any personal actions to mitigate it. Commenting on the rapid spread of facial recognition technology in Brazil, participants noted that "São Paulo is a city marked by anxiety and hypervigilance".[137] Linked to this is the sense that surveillance is ubiquitous and inescapable, and the uncertainty of never truly knowing whether people are being targeted. This is especially true in networks where members have been targeted by spyware: "This makes you double guess everything you're doing."[138]

2. Health and mental health

95. The mental health impacts of persistent surveillance are well documented in psychology, epidemiology and other fields of medicine.[139] While many of these studies focus on the impact of clear and visible forms of surveillance such as neighbourhood overpolicing,

---

Amy Stevens, Pete Fussey, Daragh Murray et al., "'I started seeing shadows everywhere': the diverse chilling effects of surveillance in Zimbabwe".

128 Civil society written submission from Pakistan.

129 First Africa consultation.

130 Twelfth and fourteenth interviews.

131 Fifth interview.

132 First interview.

133 Eighth interview.

134 Fourth interview.

135 Fourteenth interview.

136 Second interview.

137 First Latin America consultation.

138 Second interview.

139 See https://shorturl.at/25MEV.

the era of digital technology and the growth of remote and barely perceptible intrusive monitoring tools expand the mental health impact of surveillance.

96. Mental exhaustion and burnout were consistently experienced in every region studied, as reflected in accounts given by activists themselves and in the observations of people working in mental health services. One organization reported that more than 60% of activists struggled with depression, burnout and other issues, adding that "of course, there are other contributing factors to these mental health struggles as well, but repression constitutes a major factor".[140] Mental health is impacted by multiple additional factors routinely experienced by civil society, including constant targeting "by smear campaigns day in and day out. It drains you mentally, physically and socially if you are monitored online, offline, around the clock", which has led many to leave activism.[141]

97. Psychological and emotional exhaustion was cited by almost all activists from the Middle East and North Africa region,[142] consistently linked to a sense of defeat by authoritarian surveillance.[143] One spyware victim described "a complete loss – powerlessness",[144] while activists in Afghanistan explained that "it would be hard to overstate the level of hopelessness that online surveillance … has brought. It's really having a chilling effect."[145]

98. Others described the unattainability of sanctuary,[146] including the sense that nowhere is safe, as chilling effects invade intimate spheres of human experience.[147] Casual in-the-moment comments can lead to hours of psychological re-evaluation.[148] Here, chilling effects extend beyond self-censorship, they invoke an enduring distress caused by self-questioning.[149]

99. Many advanced surveillance tactics exert wide-ranging and indiscriminate psychological effects and also amplify intersectional disadvantage. For example, the state of constitutional emergency applied in Araucanía, Chile, has subjected Mapuche communities to extensive surveillance since 2021. Constant surveillance by manned and unmanned aircraft (drones) has led to alarming "increases in cases of anxiety, insomnia, depression and post-traumatic stress" reported among community members, especially children.[150] Similar to the experiences of schoolchildren in areas subjected to aerial surveillance in Brazilian favelas[151] are documented cases of children losing concentration, expressing anxiety and seeking refuge indoors upon hearing a drone.

100. Surveillance experiences are commonly described as genuine and significant trauma,[152] with many sufferers medically diagnosed with trauma-related conditions.[153] Many devote significant parts of their income to mitigating these effects through therapy.[154] This occurs to such an extent that therapy explicitly developed to address this problem has become a distinct and growing field.[155]

101. Young protesters globally face limited access to justice for violations, which amplifies the acute trauma. Pervasive surveillance further weaponizes this stress, aiming to silence their support for victims and their legitimate quest for accountability.

[140] First South-East Asia consultation.
[141] Ibid; and fourth interview.
[142] Middle East and North Africa consultation.
[143] Fourth interview.
[144] Fourth and thirteenth interviews
[145] Civil society written submission from Afghanistan.
[146] First South-East Asia consultation; and Middle East and North Africa consultation.
[147] Fourth South-East Asia consultation.
[148] First Africa consultation.
[149] Eleventh interview.
[150] See A/HRC/62/45/Add.1.
[151] Second Latin America consultation.
[152] Third Latin America consultation.
[153] First interview; and third Latin America consultation.
[154] First Africa consultation.
[155] Thirteenth interview.

VIII. Chilling effects and the surveillance ecosystem

102. For those subject to surveillance, surveillance measures are not one-off, isolated activities. For example, the use of facial recognition at assemblies, spyware targeting activists, public surveillance camera infrastructures, the deployment of automated number plate recognition, police presence in the vicinity of an event, or the infiltration of WhatsApp groups and so on are not seen as discrete occurrences, even if they are targeted at different groups. Instead, they form a surveillance ecosystem. Uncertainties surrounding the relationship between State and non-State actors, particularly with respect to the sharing of data, further exacerbate the impacts associated with the interconnected environment of surveillance.

103. Surveillance activities, even if discrete, exist across a continuum and persist over time, leaving deep, long-term society-wide impacts. They undermine essential trust in democratic institutions, including governance and community policing – for which trust is essential – and exacerbate chilling effects. This ecosystem-related impact plays a decisive role in the degree to which chilling effects are experienced by different individuals and groups. These impacts are enhanced for marginalized and vulnerable communities, and for those engaged in sociopolitical activities challenging the status quo.

104. This challenges traditional human rights law analysis, as ecosystem-related chilling effects are not typical "cause and effect" harms whereby a specific incident leads to a defined harm. Unless the surveillance ecosystem is addressed, its impacts on broader civic space will be ignored or underestimated, skewing the "necessary in a democratic society" test when assessing restrictions. This will result in a bias favouring harmful surveillance activities and tools, which will, in turn, further exacerbate the chilling effects.

IX. Compound harm

105. Chilling effects impact the right to privacy *and* the right to freedom of expression *and* the right to freedom of peaceful assembly *and* the right to freedom of association *and* the right to non-discrimination *and* other associated rights.[156] Chilling effects impact these rights simultaneously, and interfere with their interconnected and interdependent interplay. In this sense, they exert compound human rights harm. To date, chilling effects impacts are unaddressed,[157] or are examined on a restrictive right-by-right basis; for example, impacts on freedom of expression are addressed in isolation from impacts on other rights.[158]

106. Importantly, compound harm does not just refer to simultaneous harm to multiple human rights. By interfering with the interconnected and interdependent nature of the affected rights, the harm itself is compounded and intensified. For example, taken together, freedom of peaceful assembly, association, expression and privacy protect individuals' identity development as well as the functioning of democratic society.[159] As such, chilling effects not only interfere with the underpinning rights, but also undermine individuals' and collectives' ability to freely develop and express their identity and to participate in social, cultural and political life. The scope of the harm is made more acute considering the "enabling function" of freedom of peaceful assembly and of association. Chilling effects therefore undermine the very ability to advocate for and defend rights. Compound harm refers to this overall harm arising from the chilling effects of surveillance.

107. This compound harm must be incorporated into any due diligence and human rights impact assessments.

[156] See https://committees.parliament.uk/writtenevidence/148179/pdf.

[157] European Court of Human Rights, *Glukhin v. Russia,* Application No. 11519/20, Judgment, 4 October 2023, para. 88.

[158] European Court of Human Rights, *Catt v. the United Kingdom*, Application No. 43514/15, Judgment, 24 April 2019, para. 123.

[159] Ronit Matar and Daragh Murray, "Rethinking international human rights law's approach to identity in light of surveillance and AI", *Human Rights Law Review*, vol. 25, issue 3 (June 2025).

X. Conclusion

108. **In the present report, the Special Rapporteur highlights the complex and multi-faceted chilling effects of digital surveillance, demonstrating that these effects exist, and that impacts are commonly experienced, irrespective of country or context. Chilling effects exert a profound sociopolitical impact and directly interfere with the ability of individuals, groups, associations and assemblies to effectively exercise fundamental freedoms, to act politically and to participate in public life. Pervasive surveillance exacerbates the chilling effects of stigmatization and criminalization.**

109. **Chilling effects exert tangible real-life impacts on those directly and indirectly affected. When public spaces are emptied or actions are "softened" for safety, when words disappear from advocacy, reports and donors' projects, when human rights work is rebranded as "aid", when resources are spent on digital security rather than advocacy – all to evade surveillance and further repercussions – the effects are severe. These factors undermine resilience and the possibility of sustained engagement in civic and political activism. The normalization of surveillance results in institutional violations of fundamental freedoms. In effect, it suppresses activism and inclusive democratic participation.**

110. **The gravity and systematic nature of chilling effects that have been evidenced, which are amplified by digitally facilitated and AI-powered surveillance techniques, present a stark wake-up call for global unified action. The impact of chilling effects on civic space, resulting from these surveillance techniques, can no longer be ignored. While States have a responsibility to ensure national security and public safety, they must do so while protecting and facilitating fundamental freedoms. As such, chilling effects and the associated interference with the rights to freedom of peaceful assembly and of association must become a core element of human rights law assessments, litigation, law, and policy development. This extends to the design, deployment and sale of digital tools.**

111. **Safety and preventing and mitigating chilling effects must be ensured by design to prevent potential misuse and abuse for targeting and silencing democratic participation, public scrutiny and political activism. Unobstructed civic participation, both online and offline, is vital for democratic development and inclusive participation, valuing all members, including children.**

XI. Recommendations

112. **States, the United Nations and all stakeholders should ensure a rights-enabling environment and protect civic space from chilling effects. They should:**

(a) **Refrain from stigmatizing and criminalizing legitimate civic activism, and from using surveillance and digital technologies to suppress political dissent and civil society actions. The use of digital technology for these objectives must be prohibited;**

(b) **Protect civic space through the promotion and protection of strong encryption, including the integrity of end-to-end encryption, and refrain from criminalizing legitimate measures to maintain anonymity;**

(c) **Ensure a human rights-compliant legal framework to regulate all digitally facilitated surveillance activities, in line with the requirements of legality, necessity, proportionality and non-discrimination. Chilling effects should be incorporated into the necessity analysis. Any exceptions, including national security, should be narrowly construed, and strictly limited. In light of the pace of technological change, any legislation should restrict surveillance powers rather than being permissive, and should be subject to regular review. The sale, transfer and brokering of digital surveillance tools, and technical support for them, should be subject to a similar legal framework;**

(d) **Ensure that surveillance measures, including through digital tools and AI, are subject to robust human rights safeguards – mandating that any surveillance**

measures are strictly time-bound, and are subject to compulsory prior judicial authorization and independent effective oversight, and that remedy is provided;

(e) **Implement mandatory human rights due diligence and human rights impact assessments with respect to all digital surveillance activities. These processes should be evidence-based, incorporate potential chilling effects, and examine compound harm, considering intersectional gravity. Due diligence must necessarily be an ongoing process;**

(f) **Establish a distinct institutionalized due diligence process focused on evaluating the surveillance ecosystem. Evaluate regularly the "necessity" of the State's overall surveillance activity, addressing diverse intersectional and compound risks and impacts. This process must be mandatory, especially prior to the deployment of new surveillance technologies, when contexts change, and prior to democratic processes (such as elections);**

(g) **Ensure effective human oversight and accountability:**

(i) **Ensure public transparency and inclusive broad consultation regarding the acquisition, transfer and deployment of surveillance systems, including collaborations with companies;**

(ii) **Ensure independent, effective and resourced oversight, empowered to audit surveillance systems, their interference with rights and freedoms and their intersectional chilling effects, to investigate complaints, and to suspend or sanction State and non-State actors for non-compliance;**

(iii) **Ensure appropriate law enforcement and judicial capacity to investigate and prosecute all responsible in the decision-making chain for unlawful surveillance, including that linked to violations of freedom of peaceful assembly and of association, and to associated chilling effects;**

(iv) **Ensure specific, victim-centred and supportive complaint and remedy mechanisms enabling all, including children and marginalized groups, to safely report surveillance abuses, and to obtain and challenge information held about them, including by non-State actors;**

(v) **Provide appropriate remedies, considering intersectional harms, including the destruction of unlawfully collected data;**

(h) **Ensure the development of gender- and intersectional-responsive policies, noting the differentiated impact of digital surveillance and digital technologies. Particular attention should be paid to the misuse of personal data, including reproductive health data, and to online gender-based violence;**

(i) **Strictly prohibit the following:**

(i) **Uses and transfer of intrusive digital tools failing to comply with human rights protections, including highly invasive spyware (whose functionality cannot be limited or whose use cannot be independently audited);**

(ii) **Arbitrary, indiscriminate and mass surveillance used for law enforcement purposes, including biometric and AI applications, such as facial recognition technology, AI systems that create or expand facial recognition databases through the untargeted scraping of facial images from the Internet or CCTV footage, and AI systems for social scoring;**

(iii) **The use of surveillance technologies and data collection for arbitrary and discriminatory predictive and profiling purposes, including predictive policing, and for purposes not warranted;**

(iv) **Uses of militarized surveillance technologies and techniques for law enforcement purposes, especially in the context of freedom of peaceful assembly and association rights, and the use of civilian activism data for military purposes;**

(v) **Immediately ban the transfer and use of technologies and products implicated in facilitating in serious human rights violations, including when there is a risk of them being employed for such purposes;**

(vi) **Refrain from employing digital surveillance in education and workplaces;**

(vii) **In general, technologies that have a higher coercive potential, including capability for military use, must have a higher threshold for authorisation and use in order to avoid compound harm.**

113. **The United Nations and the international community should:**

(a) **Adopt human rights-centred, binding legal standards and global governance mechanisms regulating digital surveillance technologies and AI, addressing potential chilling effects;**

(b) **Ensure that global crime prevention frameworks, including for counter-terrorism and cybercrime prevention, do not exert chilling effects on the exercise of public freedoms. Urgently address these considerations in the context of the ongoing process of updating the United Nations counter-terrorism framework;**

(c) **Support the establishment of a global truth and justice commission to address the systemic and widespread impact of digital surveillance, including of intersectional chilling effects;**

(d) **Ban the sale, transfer and use of commercial technology facilitating unlawful surveillance and serious undue restrictions on public freedoms, and sanction violations effectively;**

(e) **Hold companies accountable for human rights abuses arising from transfer and use of their products, including for chilling effects.**

114. **The business sector (developers, social media, service providers, digital platforms, telecom companies, and others involved in surveillance, including big tech) must implement stringent human rights due diligence across the full life cycle of surveillance technologies. This due diligence assessment should consider chilling effects and should meaningfully engage diverse civil society actors. The business sector should:**

(a) **Ensure that inclusive design and digital features do not enable unlawful (including disproportionate, indiscriminate and biased) monitoring;**

(b) **Resist State demands for surveillance data, unless subject to judicial order, and regularly publish comprehensive transparency reports detailing government requests;**

(c) **Ensure that contracts with States include clear human rights obligations, auditing rights, and due diligence processes;**

(d) **Refrain from selling surveillance technologies when there are risks that adverse human rights impacts will result.**

115. **Donors should provide sustained financial support to activists and associations to enhance security, to mitigate impacts, and to defend against surveillance through litigation, psychosocial support, community-led documentation, and legal defence capacity-building.**

Annex I

I. Key activities conducted from 1 January 2025 to 31 May 2026

1. The period from 2025 through the first quarter of 2026 has been a pivotal era for the defence of the freedoms of association and peaceful assembly. Throughout this timeframe, the mandate faced significant global challenges, yet also witnessed important advances fuelled by the tireless action of civil society, social movements, community leaders, and international actors.

2. The Special Rapporteur expresses her sincere gratitude to: i) her supporting staff at the OHCHR; ii) her external advisors, specially Sonya Merkova, Felipe Caicedo and Luz Avendaño; iii) interns from the Master of Advanced Studies International Humanitarian Law and Human Rights, at the Geneva Academy; iv) all the volunteers that have supported her mandate extensively ; v) Prof. Pete Fussey and Dr. Daragh Murray, for their generosity and wisdom; vi) and all the other individuals, associations, including pro-bono groups, governments, international bodies and donors, among others, that have engaged with the mandate.

3. The Special Rapporteur shares a warm recognition in solidarity with: i) all civil society colleagues and friends who have experienced one of the toughest years on record, due to the deadly combination of funding cuts, a shifting financial landscape, the accelerated closing of civic space worldwide, a deep crisis in multilateralism, and the rise of conflicts, wars and genocides; and to ii) the victims of the violations of the right to freedom of peaceful assembly and of association worldwide, especially the youth that have been at the forefront of the defence of human dignity. For their courage, these two groups have been stigmatized, vilified, harassed, surveyed, detained, punished, harmed and even killed. My heart is with you, and my actions are for you.

4. The Special Rapporteur also wishes to acknowledge most of her fellow Special Procedures mandate holders, who even in the mist of reforms (including the disappearance of the Special Procedures Branch at the OHCHR), defunding, a lack of appropriate support, and constant attacks, remain deeply committed to advancing their mandates and protecting human rights. A special acknowledgment to Francesca Albanese, Special Rapporteur on the Occupied Palestinian Territories, who has been subjected to the most outrageous attacks and profound lack of protection from the organization and member States, despite her privileges and immunities.

5. The Special Rapporteur also expresses her appreciation to those Member States that supported the mandate – including its core group – and those that have actively engaged with and provided information in response to requests. She highlights that a global debate is most fruitful when all parties participate actively. For this new cycle, she expresses her hope that all governments will increase their commitments to human rights by transforming words into real actions, including the genuine protection of multilateralism. In a world that is losing its strongest advocates for human rights, we need new leadership – one deeply rooted in respect for human dignity and our shared human values.

6. The Special Rapporteur also expresses her appreciation to Switzerland for the provision of a Junior Professional Officer to support the mandate; and reiterates that greater contributions are required from member States to fulfil the objectives of her mandate.

II. On-the-ground activities and country visits

7. During this reporting period, the Special Rapporteur emphasized face-to-face connections and the prioritization of local realities in her actions. She conducted a total of 249 engagements, meeting with more than 1,753 people in person out of approximately 3,503 people reached across both physical and digital spaces.

8. The Rapporteur's mobility was central to the mandate's effectiveness, spending more than 100 days on the road across 17 different countries and 19 cities. These visits encompassed 1 official visit (to Chile), as well as 2 travels to present reports (New York and Geneva) and to 17 different countries to attend meetings and events organised by civil society organizations or within educational and research environments.

9. A significant focus of these engagements remained on victims and civil society, who constituted 73% of all interactions. Through over 100 dedicated meetings, the Rapporteur engaged with over 2,200 individuals from these groups to ensure their voices remained the primary focus of the mandate's work. These efforts were balanced with over 80 high-level meetings with government representatives and international organizations to share information, advocate for legislative and policy reforms, and to ask for accountability, justice and reparation.

III. Reports

10. The Special Rapporteur presented two thematic reports: one to the Human Rights Council addressing the lessons learned from the "super election" cycle and the resulting impact on civic space (A/HRC/59/44), and one to the General Assembly focused on the existential threats currently facing the rights to freedom of peaceful assembly and of association and the critical role of human solidarity in the current global context (A/80/219).

IV. Communications

11. Between 1 January 2025 and 31 March 2026, the Special Rapporteur joined or led over 300 communications. In terms of regional distribution, Asia accounted for the largest share with 73 communications. Africa and the Americas followed with a similar volume of 51 and 45 communications, respectively. Europe accounted for 35 communications, while Oceania recorded the lowest number with 2 communications. The Special Rapporteur led 37 of these communications. These interventions were primarily driven by a systematic pattern of repression against peaceful protesters, civil society activists, and human rights defenders. Key reasons for these communications included the excessive and disproportionate use of force by security forces, frequently leading to extrajudicial killings, widespread injuries, and the detention of peaceful demonstrators. A persistent pattern of arbitrary arrests and detentions used to criminalize dissent, which in some instances resulted in enforced disappearances. Finally, the implementation of restrictive laws and police and officials actions, such as internet shutdowns, the acquisition and deployment of "less lethal weapons" for crowd control or of surveillance tools and strategies, used to curtail the rights to assembly and expression.

12. The Special Rapporteur also sent letters to around 15 other stakeholders including universities, social media and tech companies.

13. The Special Rapporteur issued two special statements: i) Civic space must be protected and expanded in anti-corruption efforts: Urging States parties to the UN Convention against Corruption (UNCAC) to strengthen the inclusiveness and transparency of the Convention's review mechanism,[160] and ii) Streets must be spaces of freedom, not of fear: A call to protect women's right to protest this March 8th.[161]

14. The Special Rapporteur published four newsletters with information of her action: May 2024 and January 2025–February–Apr 2025–May–July 2025–August–October 2025 – 2025 summary.

[160] United Nations, "Joint statement by a group of Special Procedures mandate holders:* Civic space must be protected and expanded in anti-corruption efforts: Urging States parties to the UN Convention against Corruption (UNCAC) to strengthen the inclusiveness and transparency of the Convention's review mechanism" (22 August 2025), available at www.ohchr.org/sites/default/files/statements/20250822-stm-uncac-cop-sr-assembly.pdf.

[161] See https://us10.campaign-archive.com/?u=92a2c63767a801e0d97cf1568&id=a46cb60268.

V. Technical assistance and cooperations

15. The Special Rapporteur has been providing ongoing technical assistance to different actors involved in the mutual evaluations and other activities held in relation with the Financial Action Task Force (FATF). This collaboration, that includes governments and civil society, aims to ensure that the country recommendations provided by the Task Force are fully aligned with international human rights standards and do not inadvertently jeopardize citizens' rights to freedom of peaceful assembly and of association.

16. The Special Rapporteur provided comments in the following processes:

(a) Corte Interamericana de Derechos Humanos, Caso Ramos Durand y otros vs. Perú. – May 2025;

(b) Comisión Interamericana de Derechos Humanos, Peritaje caso Diego Lamagna y familia, Marcelo Gastón Riva y familia vs Argentina;

(c) United Kingdom of Great Britain and Northern Ireland Parliament's inquiry on Human rights and the regulation of AI.

17. The special Rapporteur coordinated different actions with regional bodies such as:

(a) Joint declaration about the prolonged detention of human rights defenders with the UN Special Rapporteur on the situation of human rights defenders; the UN Special Rapporteur on Environmental Defenders under the Aarhus Convention; the African Commission on Human and Peoples' Rights, Special Rapporteur on Human Rights Defenders, Focal Point on Reprisals and Focal Point on the Independence of the Judiciary in Africa; and the Inter-American Commission on Human Rights and Rapporteur on Human Rights Defenders and Justice Operators.

(b) Joint Declaration on Protecting the rights to freedom of peaceful assembly and of association from criminalization amid intensified existential threats, with the Special Rapporteur on Freedom of Expression of the Inter-American Commission on Human Rights (IACHR), the Commissioner Rapporteur for Human Rights Defenders of the IACHR, and the Special Rapporteur on Human Rights Defenders and focal point for reprisals in Africa of the African Commission on Human and Peoples Rights (ACHPR).

(c) Joint Statement on the Recognition of the Right to Care and the Freedom of Association of Women Workers, 01 May 2025, with the Rapporteur on the Rights of Women of the Inter-American Commission on Human Rights (IACHR); and the Special Rapporteur on Economic, Social, Cultural and Environmental Rights (REDESCA) of the IACHR.

(d) Peer review of ODIHR opinions on:

(i) Cyprus: Urgent Opinion on the Law 151(I) of 2025 on Public Gatherings and Parades;

(ii) Urgent opinion on the amendments to the law on assemblies and demonstrations, the code of administrative offences and the criminal code of Georgia (as adopted on 6 February 2025);

(iii) Opinion on the draft act on the registration of foreign agents in Bulgaria (as of 11 November 2024).

Annex II

Methodology and sources

1. Evidence for this report was drawn from a global study,[162] that included interviews, consultations and focus groups with 152 activists, human rights defenders, public defenders and other lawyers, journalists and civil society actors across all regions of the world. Diverse participants, across distinct contexts and jurisdictions were interviewed to identify common and/or cross-cutting experiences of digital surveillance. These participants advocated across the spectrum of issues including indigenous rights, environmental activism, gender equality, LGBTQIA+ rights, racial justice and the range of concerns related to democratic participation. One consultation was convened in the MENA region, two in Latin America (composed by six different meetings), three in Southeast Asia, two in Africa and a further global event hosted online. This methodology was aimed at countering sceptical views that claim chilling effects are overly subjective, or difficult to measure effectively. Further informing the report are 63 written submissions: 49 from civil society, academics, international bodies, a major global tech company, and 13 State submissions. In addition, the Rapporteur included information she received during her term in victims' sub-missions, meetings with civil society, academic visits and an official country visits. Collectively, this data concerns 84 States and other entities, demonstrating the widespread nature of the chilling effects phenomenon.

2. Participants contributing to this report were from the following States and other entities: Afghanistan, Algeria, Argentina, Armenia, Australia, Azerbaijan, Bahrain, Bangladesh, Belarus, Bhutan, Brazil, Cambodia, Canada, Chile, China, Colombia, Côte d'Ivoire, Cuba, Czechia, Denmark, Ecuador, Egypt, El Salvador, Eritrea, Eswatini, Ethiopia, France, Georgia, Hungary, Honduras, India, Indonesia, Iran (Islamic Republic of), Iraq, Ireland, Israel, Italy, Jordan, Kenya, Kuwait, Lebanon, Libya, Malaysia, Mexico, Morocco, Myanmar, Nepal, Nicaragua, Niger, Nigeria, Oman, Pakistan, Paraguay, Peru, Philippines, Poland, Russian Federation, Saudi Arabia, Serbia, South Africa, South Sudan, Spain, Sri Lanka, Sudan, State of Palestine, Switzerland, Syrian Arab Republic, United Republic of Tanzania, Thailand, Tunisia, Türkiye, Uganda, Ukraine, United Arab Emirates, United Kingdom of Great Britain and Northern Ireland, United States of America, Uzbekistan, Venezuela (Bolivarian Republic of), Viet Nam, Yemen, Zambia, Zimbabwe.

[162] See the Global Study, available at https://www.ohchr.org/en/special-procedures/sr-freedom-of-assembly-and-association/pushed-shadows.