March 2026

Privacy International's submission to the UN High Commissioner for Human Rights on the protection of human rights defenders in the digital age

Introduction

Privacy International (PI) is a non-governmental organisation that conducts research and advocates globally against government and corporate abuses of data and technology.[1] It exposes harm and abuses, mobilises allies globally, campaigns with the public for solutions, and pressures companies and governments to change.

We welcome the opportunity to inform the report of the UN High Commissioner for Human Rights pursuant to HRC resolution 58/23 on "Human rights defenders and new and emerging technologies: protecting human rights defenders, including women human rights defenders, in the digital age".[2]

PI has been observing the increasing use of digital surveillance technologies to target and monitor human rights defenders (HRDs) in the digital age. We also note that a surveillance ecosystem characterised by the increased capacity of law enforcement, security and intelligence agencies to surveil the population at large, invariably affect the activities of HRDs. In recent years PI conducted a range of surveys with different categories of HRDs (as described in the examples below) documenting how HRDs are increasingly concerned by being monitored by state agents and how this is evidentially having a chilling effect on the exercise of freedom of expression, assembly and association and other rights. In the sections below we identify some key trends, with examples, responding to some of the questions posed in the call for submission.

Digital communications

Which risks do internet shutdowns, network interferences, geo-blocking or other forms of restrictions of connectivity and communications pose to HRDs' work and safety?

SOCMINT

Social Media Intelligence **(**SOCMINT) refers to the techniques and technologies that enable actors to monitor social media networking sites.[3] This includes the monitoring of user-generated content such as public posts, comments as well as private messages. It also includes metadata and interactions such as who someone is friends with or follows, the types of posts they share or like, the groups they are part of who they tag in photographs, and the time and location something was shared. The type

[1] See: https://privacyinternational.org/about
[2] See: https://www.ohchr.org/en/calls-for-input/2026/call-inputs-protection-human-rights-defenders-digital-age
[3] Ibis. At 4.

of personal information that is collected and analysed includes sensitive data revealing people's political opinion, religious belief, health conditions, sexual orientation and gender identity. As the OHCHR confirmed "social media intelligence ranges from the investigation of specific users to dragnet collection, storage and analysis of vast amounts of data."[4]

SOCMIT has been deployed at scale, particularly in contexts such as border management, migration control and counterterrorism, in ways that seem to target sections of population rather than individuals.[5] However, in many instances SOCMINT has been used against HRDs, as highlighted in research by PI, its partners and the media. In 2019, it was reported that London's Metropolitan Police monitored around 9000 activists using data scraped from social media platforms. Secret dossiers were compiled on each activist, despite many of them having no criminal background.[6] In the US it was reported that police in Memphis reportedly used SOCMINT to collect information on Black Lives Matter Activists.[7]

In 2022, PI conducted a survey with climate activists and environmental defenders with the purpose of understanding their perception and experiences of surveillance.[8] One third stated that they feared or thought about surveillance in the context of their activism. Nearly 60% of respondents highlighted that they suspected that they had been surveilled by way of social media monitoring.[9] As a result of these concerns PI produced guidance for activists and environmental defenders on how to better protect themselves from social media monitoring.[10]

In Colombia, our partner Dejusticia have also documented the use of SOCMINT by Colombian authorities to build secret dossiers on over 130 people ranging from politicians to activists, journalists and trade unionists.[11]

What forms of technology-facilitated attacks do HRDs face on social media platforms and digital communications services? How do these online attacks intersect with offline events?

Increasingly HRDs are facing abuse online, particularly if they are defending or from marginalised communities. The Digital Health and Rights Project (DHRP) consortium formed of social scientists, human rights lawyers, health advocates, rights advocates, and communities living with and affected by HIV, were formed to gather empirical evidence of the effects of the digital transformation on young adults living with HIV and young key populations in low- and middle-income countries. DHRP conducted research to collate the concerns of young people in the digital age from Colombia, Viet

[4] U.N. Doc. A/HRC/51/17, para 35.
[5] For an overview and recent examples, Privacy International, Social Media Surveillance, https://privacyinternational.org/learn/social-media-surveillance .
[6] Freedom House, Freedom on the Net 2019 Key Finding: Governments harness big data for social media surveillance, https://freedomhouse.org/report/freedom-on-the-net/2019/the-crisis-of-social-media/social-media-surveillance
[7] George Joseph, Memphis Police Collected Black Lives Matter Activists' Private Facebook Posts, 27 July 2018, https://theappeal.org/memphis-police-collected-black-lives-matter-activists-private-facebook-posts/
[8] Privacy International, How to avoid social media monitoring: A Guide for Climate Activists, 2022, https://privacyinternational.org/long-read/5000/how-avoid-social-media-monitoring-guide-climate-activists
[9] Ibid.
[10] Privacy International, How to avoid social media monitoring: A Guide for Climate Activists, 2022, https://privacyinternational.org/long-read/5000/how-avoid-social-media-monitoring-guide-climate-activists
[11] Dejusticia, State intelligence gathering on the internet and social media: the case of Colombia, January 2024, https://www.dejusticia.org/en/publication/state-intelligence-gathering-on-the-internet-and-social-media-the-case-of-colombia/

Nam, Ghana and Kenya.[12] They reported abuse of frontline HIV activists and outreach workers who were advocating online via social media. In Bogota, during focus groups with transgender participants they shared that they had organised a protest to demand police action on violence against transgender women, some participants described how police monitored social media posts of activists and used this information in court.[13] DHRP highlighted that these individuals are key partners in the global HIV response given the rapid loss of global actors that have led provision of life-saving interventions - including access to medicines for people living with HIV, due to changes in US international aid policy and closure of United States Agency for International Development (USAID).

What specific risks do women HRDs and HRDs from groups affected by marginalisation and discrimination face on online platforms and communications services?

In 2024, PI conducted a survey to gather the experiences and risks that sexual and reproductive justice (SRJ) activists experience in the digital age. 63% of respondents shared fears of being subject to surveillance, with additional comments reflecting that these fears correlated with working in jurisdictions where abortion is criminalised.[14] Among those worried about surveillance, most were concerned about surveillance from opposition groups/adversaries (44%), government actors (38%) and/or law enforcement (38%).[15] One respondent mentioned how feminist groups had been subject to government surveillance in Mexico, and several respondents raised concerns about opposition groups, particularly regarding harassment on social media.[16]

Specifically in the US, these experiences reflect a stark rise in surveillance and prosecution following the overturn of *Roe v. Wade*.[17] With digital evidence increasingly used in abortion-related prosecutions law enforcement officials have seized personal electronic devices while investigating people seeking abortion care in states or countries where it is restricted or criminalised.[18] Those in opposition to abortion are also increasingly using data exploitative tactics to suppress and curtail access to abortion, for example by targeting people seeking sexual and reproductive healthcare with fake online ads.[19] Sexual and reproductive health information shared by HRDs and organisations providing care are claiming their content is deliberately censored on online platforms.[20] HRDs are therefore finding themselves operating in an increasingly hostile environment on online platforms and fears of having their communications seized. As a result, SRJ defenders have been forced to rethink how they conduct their work and activism online to protect themselves and the individuals

[12] Digital Health and Rights Project Consortium, Paying the costs of connection: Human rights of young adults in the digital age in Colombia, Ghana, Kenya and Vietnam, 2025, https://digitalhealthandrights.com/wp-content/uploads/2025/05/2025-DHRP-Paying-the-costs-report.pdf

[13] Ibid., pg. 37.

[14] Privacy International & Women on Web, Securing Reproductive Justice: A Guide to Digital Privacy for Sexual and Reproductive Justice Activists, 2026, https://privacyinternational.org/long-read/5742/privacy-international-women-web-securing-reproductive-justice-guide-digital-privacy

[15] Ibid.

[16] Ibid.

[17] Privacy International, All Eyes on my Period? Period tracking apps and the future of privacy in a post-Roe world, May 2025, https://privacyinternational.org/long-read/5593/all-eyes-my-period-period-tracking-apps-and-future-privacy-post-roe-world

[18] Abortion Rights, The Scarlet Google Search: the use of digital data as evidence in criminal conduct for abortions, June 2023, https://abortionrights.org.uk/the-scarlet-google-search-the-use-of-digital-data-as-evidence-in-criminal-conduct-for-abortions/

[19] Rachel Schraer, Anti-abortion groups target women with misleading ads, *BBC News*, May 2022, https://www.bbc.co.uk/news/health-61320202

[20] Maryam Zakir-Hussain**,** 600 women's health leaders warn of social media censorship, *The Independent,* March 2026, https://www.independent.co.uk/news/health/women-health-censorship-fertility-menopause-b2933549.html

they assist. To address this, PI and Women on Web developed a practical guide offering guidance to SRJ activists.[21]

Digital restrictions to privacy

What risks have emerged for HRDs with the increasing procurement, use and abuse of digital surveillance tools, including spyware and interception technologies, by State and non-State actors?

States continue to develop surveillance tech within their own agencies as well as procure tools on the international surveillance market from the private sector.[22] We outline some examples below.

IMSI Catchers

IMSI catchers, also known as stingrays, function by mimicking nearby mobile cell towers, enabling them to intercept communications and location data transmitted by personal devices.[23] It is increasingly being used by law enforcement and intelligence agencies during protests, permitting authorities to record everyone who attended and interfere with their communications. We recently responded the UN Special Rapporteur on freedom of peaceful assembly and of association regarding the upcoming thematic report "Impact of digital and AI-assisted surveillance on assembly and association rights, including chilling effects."[24] We highlighted several examples of IMSI catchers being used at protests and HRDs including to target Black Lives Matter protesters in the US.[25]

Spyware

While marketed as a counterterrorism and crimefighting tool, spyware has been deployed to conduct secret, intrusive surveillance of HRDs inferring with their privacy and other rights. The covert nature of the spyware, usually entirely undetectable, creates a pervasive sense of uncertainty, making it nearly impossible for individuals such as HRDs and journalists, who have reasons to believe to be targeted, to ascertain whether they are under constant surveillance. This uncertainty fuels self-censorship and alters behaviours, as individuals pre-emptively restrict their expression or association to avoid potential repercussions, and creating an environment of fear that deters civic engagement and weakens democratic accountability. In recent years the use of spyware to surveil HRDs has been consistently raised by numerous UN and regional human rights experts and bodies.[26] We outline

[21] See: https://privacyinternational.org/sites/default/files/2026-03/Privacy1_0.pdf
[22] Citizen Lab, Communities @ Risk: Targeted Digital Threats Against Civil Society, November 2014, pp 8-11, https://targetedthreats.net/media/1-ExecutiveSummary.pdf
[23] Privacy International, IMSI catchers: PI's legal analysis, 2020, https://privacyinternational.org/report/3965/imsi-catchers-pis-legal-analysis
[24] See: https://www.ohchr.org/en/calls-for-input/2025/call-input-hrc62-thematic-report-impact-digital-and-ai-assisted-surveillance & Privacy International, Submission to the UN Special Rapporteur on freedom of peaceful assembly and of association regarding the thematic report "Impact of digital and AI-assisted surveillance on assembly and association rights, including chilling effects", November 2025, https://privacyinternational.org/advocacy/5740/privacy-internationals-submission-impact-digital-and-ai-assisted-surveillance
[25] CBS News, Activists Say Chicago Police Used 'Stingray' Eavesdropping Technology During Protests, 6 December 2014, https://www.cbsnews.com/chicago/news/activists-say-chicago-police-used-stingray-eavesdropping-technology-during-protests/
[26] Human Rights Watch, 'The Persecution of Ahmed Mansoor, 27 January 2021, https://www.hrw.org/report/2021/01/27/persecution-ahmed-mansoor/how-united-arab-emirates-silenced-its-most-famous-human; Human Rights Watch, 'UAE: Ahmed Mansoor's 15-Year Sentence Upheld', 7 March 2025, https://www.hrw.org/news/2025/03/07/uae-ahmed-mansoors-15-year-sentence-upheld

some earlier examples below to illustrate how long-standing and widespread this form of surveillance is.

Spyware has emerged as a critical instrument of transnational repression by Gulf states, enabling governments like Saudi Arabia[27], the United Arab Emirates[28] and Bahrain[29] to surveil, intimidate, and silence dissidents beyond their borders. PI documented the repressive use of spyware against Gulf dissidents, including how pro-democracy Bahraini activists living in Bahrain, the UK and the USA were targeted by FinFisher spyware.[30]

In El Salvador between mid-2020 and late 2021, at least 35 journalists and HRDs were confirmed to have had their mobile phones hacked with NSO Group's Pegasus spyware.[31] The targets included staff of independent national media outlets such as *E Faro*, *GatoEncerrado*, *La Prensa Gráfica*, and others, as well as NGO staff.

In 2020, Myanmar awarded a spyware tender to Cognyte Software Limited**,** an Israeli firm, and issued them an order to supply a lawful interception equipment.[32] The system was reported to allow real-time tapping of calls, monitoring web traffic and text messages, and location tracking of users - including activists, journalists, and pro-democracy activists.[33]

Mobile Phone Extraction

Mobile phone extraction (MPE) involves the extraction of communications data and other content stored on an individual's device, or from the cloud services they use. It essentially involves downloading the content from people's phones or tablets including their messages between their friends and family, and their photos.[34] It has reportedly been used against HRDs to collect and uncover information and intelligence about them as part of wider efforts to crackdown on those speaking out against a government and to suppress dissent.

For example, a MPE tool provided by Israeli-based company Cellebrite[35] was reported to have been used by Hong Kong police to search the device of Joshua Wong, a pro-democracy leader.[36] It has also

[27] Amnesty International, 'UK court says activist can pursue spyware case against Saudi Arabia', 21 October 2024, https://securitylab.amnesty.org/latest/2024/10/uk-court-says-activist-can-pursue-spyware-case-against-saudi-arabia/
[28] Bill Marczak and John Scott-Railton, "The Million Dollar DissidentNSO Group's iPhone Zero-Days used against a UAE Human Rights Defender", *Citizenlab*, 24 August 2016 https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/
[29] Morgan Marquis-Boire, Cora Currier, 'Leaked Files: German Spy Company Helped Bahrain Hack Arab Spring Protesters', *The Intercept*, 7 August 2014, https://theintercept.com/2014/08/07/leaked-files-german-spy-company-helped-bahrain-track-arab-spring-protesters/
[30] Privacy International, 'British spyware used to target Bahraini activists', July 2012, https://privacyinternational.org/blog/1361/british-spyware-used-target-bahraini-activists
[31] John Scott-Railton, Bill Marczak, Paolo Nigro Herrero, Bahr Abdul Razzak, Noura Aljizawi, Salvatore Solimano, Ron Deibert, "Project TorogozExtensive Hacking of Media & Civil Society in El Salvador with Pegasus Spyware", *CitizenLab,* 12 January 2022, https://citizenlab.ca/2022/01/project-torogoz-extensive-hacking-media-civil-society-el-salvador-pegasus-spyware/
[32] Justice for Myanmar, 'ISRAELI SURVEILLANCE FIRM COGNYTE'S BUSINESS IN MYANMAR EXPOSED', 15 January 2023, https://www.justiceformyanmar.org/stories/israeli-surveillance-firm-cognytes-business-in-myanmar-exposed
[33] Ibid.
[34] Privacy International, Mobile Phone Extraction, https://privacyinternational.org/learn/mobile-phone-extraction
[35] Privacy International, Don't Celebrate Cellebrite, Because Your Phone Is at Risk, *Medium*, 2016, https://medium.com/privacy-international/don-t-celebrate-cellebrite-because-your-phone-is-at-risk-b362dc20641
[36] UAB Institute for Human Rights Blog, The Abuse of Facial Recognition Technology in the Hong Kong Protests, 13 February 2025, https://sites.uab.edu/humanrights/2025/02/13/the-abuse-of-facial-recognition-technology-in-the-hong-kong-protests/

been reported that Cellebrite's Universal Forensic Extraction Device was used against Mohammed al-Singace, a political activist in Bahrain, and the information collected was used to criminally prosecute him.[37]

What risks have emerged for HRDs with the expansion of biometric surveillance infrastructure and increased monitoring of public and digital spaces?

PI has been monitoring and advocating against the use of biometric surveillance technologies such as facial recognition technologies (FRT) to identify, monitor and track protesters either openly or surreptitiously.[38] In some cases, it is even used to aid the arrest, or detention of those participating in protests, or to build watch lists of protesters for intelligence purposes.[39]

In 2022, PI documented how the surveillance of HRDs participating in protests is being used in criminal proceedings against them.[40] We interviewed activists and HRDs from around the world, who shared their experiences of challenging surveillance evidence used in proceedings across several jurisdictions including Colombia, India and Russia.[41] For example, the executive director of Unwanted Witness, based in Uganda, shared her concerns regarding a significant expansion in the surveillance of activists participating in protests. She noted that the deployment of surveillance during anti-government protests (including through cameras equipped with FRT) was leading to the arrests of large numbers of activists peacefully participating in protests.[42]

In our recent submission to the UN Special Rapporteur on freedom of peaceful assembly and of association[43] we highlighted other similar examples of FRT being deployed at protests interfering with the rights of HRDs such as at climate demonstrations in Vienna in 2023[44] and during Hong Kong's pro-Democracy protests in 2019.[45]

How have technological and regulatory developments relating to encryption eased or exacerbated risks to HRDs?

It has long been recognised, including by UN Human Rights Council resolutions[46], that encryption (particularly end-to-end encryption, E2EE) is a fundamental tool to protect HRDs' capacity to carry

---

[37] Sam Biddle and Fahad Desmukh, 'Phone-Cracking Cellebrite Software Used to Prosecute Tortured Dissident', *The Intercept,* 8 December 2016, https://theintercept.com/2016/12/08/phone-cracking-cellebrite-software-used-to-prosecute-tortured-dissident/

[38] Privacy International, 'How facial recognition can be used at a protest', 2021, https://privacyinternational.org/explainer/4495/how-facial-recognition-technology-can-be-used-protest

[39] Ibid.

[40] Privacy International, Protest surveillance into court, 2024, https://privacyinternational.org/report/5468/protest-surveillance-court

[41] Privacy International, Prosecuted for Protesting, 2025, https://privacyinternational.org/long-read/5460/prosecuted-protesting

[42] Ibid. at 39.

[43] Privacy International, Submission to the UN Special Rapporteur on freedom of peaceful assembly and of association regarding the thematic report "Impact of digital and AI-assisted surveillance on assembly and association rights, including chilling effects", November 2025, https://privacyinternational.org/advocacy/5740/privacy-internationals-submission-impact-digital-and-ai-assisted-surveillance

[44] Vol.at, 'Data Protection Advocates Criticize Use of Facial Recognition at Climate Demonstration in Vienna', 25 June 2025, https://www.vol.at/data-protection-advocates-criticize-use-of-facial-recognition-at-climate-demonstration-in-vienna/9504071

[45] UAB Institute for Human Rights Blog, The Abuse of Facial Recognition Technology in the Hong Kong Protests, 13 February 2025, https://sites.uab.edu/humanrights/2025/02/13/the-abuse-of-facial-recognition-technology-in-the-hong-kong-protests/

[46] UN Human Rights Council Resolution on the Right to Privacy in the Digital Age, UN Doc A/HRC/RES/48/4 (7 October 2021). See also, UN General Assembly Resolution on the Safety of Journalists and the Issue of Impunity, UN Doc A/RES/74/157 (18 December 2019).

out their activities, by mitigating the risks of their communications from surveillance. Therefore, States' attempts to implement measures to break E2EE violates human rights such as privacy, opinion and expression. [47] A recent example illustrating these concerns which could have implications for the work of HRDs is the UK government's attempts to break E2EE through their reported secret order (Technical Capability Notice, TCNs) to force Apple to undermine iCloud's advanced encryption.[48] This was also followed by a second order against Apple.[49] PI is currently challenging both the lawfulness and the secrecy of the legal regime governing TCNs following the apparent use of one by the UK Home Office to require Apple to maintain the capability to provide access to all data stored on iCloud.

Recommendations

Because of the role they play in society, HRDs face risks of unlawful surveillance, and state security agents often, without effective safeguards, use existing digital technologies to violate their human rights. Hence all the limitations and safeguards - such as principles of legality, necessity and proportionality, prior judicial authorisation, independent oversight and access to effective remedy – that human rights law requires for the use of surveillance technologies are relevant. That is why states should include in their human rights due diligence an assessment of the risks of abuse, including risks of function creep and repurposing, and identify mitigating measures.

In addition, there are some measures that are particularly relevant to the protection of the activities of HRDs, notably in relation to the confidentiality of their communications and personal data, and during any legal proceedings against them.

For these reasons, PI suggests the High Commissioner for Human Rights makes the following recommendations:

To states:

- Refrain from using certain intrusive surveillance technologies to surveil HRDs and those participating in protests;
- Strictly regulate surveillance technologies in relation to the conditions under which they can be used;
- Promote encryption and other anonymity tools and refrain from taking measures that limit their availability, including the imposition of mandatory general client-side scanning;
- Ensure that social media monitoring is only carried out in accordance with laws that clearly limit its use to the investigation of crimes, provides for independent authorisation, effective oversight and complies with modern data protection principles;
- Refrain from using, selling or transferring spyware or other intrusive hacking tools, in view of the widespread, long-term instances of abuses of these tools to target HRDs;

[47] For an outline of the issues, the main human rights affected and the techniques used, see: https://privacyinternational.org/sites/default/files/2022-09/SECURING%20PRIVACY%20-%20PI%20on%20End-to-End%20Encryption.pdf

[48] Privacy International, Our challenge against UK's secret TCN powers, 2025, https://privacyinternational.org/long-read/5547/our-challenge-against-uks-secret-tcn-powers

[49] Privacy International, The Second Order: The UK Government's new secret order still strikes at Apple's security, 2025, https://privacyinternational.org/news-analysis/5685/second-order-uk-governments-new-secret-order-still-strikes-apples-security

- Adopt appropriate procedural safeguards to ensure the protection of the rights to privacy and fair trial throughout the investigative phase and across all criminal procedures to mitigate the risk that evidence obtained through unlawful surveillance is used against HRDs; and
- Provide transparency regarding the capabilities of the surveillance technologies employed, including data to assess the impact of these technologies on human rights.

To business enterprises:

- Adopt a high level of security and confidentiality of any communications they transmit and personal data they process, including by offering end-to-end encryption in devices, messaging services, networks and platforms for data in-transit; and
- Carry out human rights due diligence prior and during any development, sale, transfer and use of surveillance technologies identify and mitigate the potential risks these technologies pose to HRDs.