March 2026

Privacy international's submission to the UN Working Group on the Use of Mercenaries on the Use of Technology in the Operations and Activities of Mercenaries, Mercenary-Related Actors and Private Military and Security Companies

Introduction

Privacy International (PI) welcomes the call for inputs of the UN Working Group on the Use of Mercenaries (the Working Group) to inform its upcoming report on the use of technology in the operations and activities of mercenaries, mercenary-related actors and private military and security companies to be submitted to the 63rd Session of the Human Rights Council in September 2026.[1]

PI[2] is a London-based non-profit, non-governmental organisation (Charity Number: 1147471) that researches and advocates globally against government and corporate abuses of data and technology. Within its range of activities, PI investigates how peoples' personal data is generated and exploited, and how it can be protected through legal and technological frameworks. It has advised and reported to international and regional organisations, including bodies and agencies of the United Nations, the Council of Europe, the European Union, and the Organisation of American States.

The decision to examine the role of technology in mercenary and private military and security companies (PMSCs) operations couldn't be timelier.[3] This inquiry follows the Working Group's seminal 2021 report on mercenaries and cyberspace,[4] and reflects the acceleration of the technology landscape since then. PI submits this contribution on the basis of its direct

[1] Call for inputs - The use of technology in the operations and activities of mercenaries, mercenary-related actors and private military and security companies, https://www.ohchr.org/en/calls-for-input/2026/call-inputs-use-technology-operations-and-activities-mercenaries-mercenary

[2] https://privacyinternational.org/

[3] UN Human Rights Council Resolution 60/5 (2024).

[4] UN Working Group on the Use of Mercenaries, 'Report to the General Assembly: Mercenaries and Cyberspace', A/76/151 (15 July 2021).

research and expertise in surveillance, data exploitation, and the intersection of private security actors within the global surveillance ecosystem.

In the following sections, we highlight the role of the surveillance ecosystem as an infrastructure for mercenary and PMSCs operations (section 1); the rise of private surveillance services (section 2); the harm chain from privacy to other human rights (section 3); the barriers to access to remedies (section 4) and conclude with recommendations to the Working Group.

1. The Surveillance Ecosystem as Enabler for Mercenary and PMSCs Operations

Effective regulation of mercenary and PMSCs activities in the technology domain requires a comprehensive understanding of the ecosystem that enables mercenary and PMSCs operations, including developers, vendors and providers of artificial intelligence (AI) systems, cloud services, and spyware technologies. These actors do not merely supply the tools: they constitute the structural infrastructure on which surveillance-enabled operations depend.[5] The surveillance industry is a complex, opaque ecosystem of vendors, integrators, resellers, and data intermediaries that collectively provide mercenaries and PMSCs with capabilities that they would not have had access otherwise.[6]

From the PI and DCAF report, we can identify at least four categories of private surveillance providers whose products and services intersect with mercenary and PMSCs operations: intelligence-gathering companies (that includes communications operators that provide signals intelligence (SIGINT), open-source intelligence (OSINT), and communications interception tools); interception and monitoring companies (that produce spyware, IMSI catchers, and network interception platforms); data analytics companies (that provide AI-driven profiling, predictive analytics, and large-scale data fusion); and infrastructure providers (including cloud hosting, content delivery networks, and platform APIs that enable the above to operate at scale).[7] Some of these actors could also fall under the categories of mercenary or PMCSs actors on their own right.

[5] Méryl Schwitzguébel (DCAF) and Ilia Siatitsa (Privacy International), 'When Surveillance Goes Private', *Opinio Juris Symposium on PMSCs: The Business of Security* (15 July 2025) https://opiniojuris.org/2025/07/15/symposium-on-pmscs-when-surveillance-goes-private/

[6] *ibis.* See also Privacy International and DCAF – Geneva Centre for Security Sector Governance (DCAF), 'Understanding Private Surveillance Providers and Technologies', Policy Paper (2022), https://privacyinternational.org/report/5255/understanding-private-surveillance-providers-and-technologies, pp 4–7.

[7] PI and DCAF Policy Paper (2022), note above, p 9.

1.1. Spyware vendors as mercenary-related actors

Companies such as NSO Group (developer of Pegasus), Intellexa (developer of Predator), and Candiru operate as commercial entities that sell intrusion and surveillance capabilities to state and non-state clients.[8] These companies exhibit structural characteristics analogous to mercenary-related actors: they operate across jurisdictions, their clients are diverse (including authoritarian governments and non-state actors), their contractual chains are deliberately opaque, and their products are used to commit or facilitate human rights violations.[9] Their corporate structures are opaque and designed to evade oversight and accountability: holdings companies, offshore subsidiaries, and frequent restructuring are used to distance parent entities from the operational use of their products.[10] This mirrors the use of shell companies and layered contracting in traditional PMSCs structures, and poses identical challenges for attribution, accountability, and remedy.

1.2. Cloud services and online platforms infrastructure

Beyond spyware vendors, mercenary and PMSC operations increasingly depend on a wider digital infrastructure. For instance, cloud service providers host sensitive data and provide infrastructures for further processing of this data. This layer of their operations is frequently invisible in discussions around mercenaries operations, yet it is foundational. As the recent conflicts have shown, without cloud computing and platform data access, the analytical and operational capabilities of many actors, including modern PMSCs and mercenary-related, would be severely constrained.[11] The providers of this infrastructure should therefore be engaged as such in any regulatory framework.

1.3. Artificial Intelligence and autonomous systems

The integration of AI and machine learning into the operations of mercenary actors and PMSCs represents a qualitative shift in their capabilities — and in the severity of the human

[8] Forbidden Stories and Amnesty International Security Lab, 'The Pegasus Project' (July 2021). See also Report of the Office of the United Nations High Commissioner for Human Rights on the right to privacy in the digital age, A/HRC/51/17 (4 August 2022) https://docs.un.org/en/A/HRC/51/17

[9] European Parliament, PEGA Committee, 'Report on the Use of Pegasus and Equivalent Surveillance Spyware', A9-0189/2023 (May 2023) https://www.europarl.europa.eu/doceo/document/TA-9-2023-0244_EN.html

[10] Amnesty International, SOMO, and PI, 'Operating from the Shadows: Inside NSO Group's Corporate Structure' (June 2021), https://www.privacyinternational.org/report/4531/operating-shadows-inside-nso-groups-corporate-structure See also, PI and DCAF Policy Paper (2022), note above, pp 10–12.

[11] See among various recent developments, Sam Biddle, 'Data centers are military targets now', *The Intercept* (20 March 2026) https://theintercept.com/2026/03/20/ai-data-centers-military-targets-iran-war/ ; Atlantic Council, 'The coming compute war in Ukraine: Why compute infrastructure will decide the next phase of the conflict' (16 March 2026), https://www.atlanticcouncil.org/content-series/the-big-story/the-coming-compute-war-in-ukraine/; 'Swiss Foreign Ministry reviewing Palantir over concerns tied to Gaza operations', *EUPAC* (23 December 2025), https://www.eupac.org/swiss-foreign-ministry-reviewing-palantir-over-concerns-tied-to-gaza-operations/

rights risks they generate.[12] AI and machine learning systems are increasingly deployed to automate the analysis of surveillance data, identify targets, and predict behaviour. These systems can process data from multiple sources — communications intercepts, location tracking, biometric databases, social media — and produce targeting intelligence at speed and scale.[13] When such systems are deployed by or on behalf of mercenary actors or PMSCs, the human rights implications are severe. The automation of targeting decisions reduces accountability: it becomes harder to identify which human actor made a decision, on the basis of what data, and under whose authority. Errors, relating particularly to identification, or classification, can have detrimental consequences and are often with no mechanism for challenge or redress.[14]

1.4. Biometric surveillance

Biometric surveillance systems — including facial recognition, gait analysis, voice recognition, and behavioural profiling — are increasingly embedded in the operational environments where PMSCs and mercenary actors operate: checkpoints, border crossings, urban surveillance grids, and conflict zones.[15] Biometric data is sensitive personal data, capable of revealing of individual's characteristics and identity. As such it has the potential to be gravely abused. Identification system relying on biometric data are also vulnerable to security breaches, whose consequences for the individuals concerned, and for the overall security of society are extremely grave.[16] These systems are disproportionately inaccurate for racialised minorities, women, and older people, generating systematic discrimination at the point of identification. They also create large biometric databases that, once collected, persist beyond their original operational purpose and can be repurposed for persecution, profiling, or sale.[17] PI notes with concern the lack of any specific regulatory framework governing the collection and use of biometric data by private military and security actors.

---

[12] PI's Response to the Call for Input on Human Rights Implications of New and Emerging Technologies in the Military Domain (November 2024) https://privacyinternational.org/advocacy/5244/pi-submission-human-rights-implications-new-and-emerging-technologies-military-domain

[13] *ibid*. On autonomous weapons systems capabilities, see UN Secretary-General, 'Report on Lethal Autonomous Weapons Systems', A/79/88 (1 July 2024) https://docs.un.org/en/A/79/88

[14] OHCHR, Briefer on Human Rights and Artificial Intelligence in the Military Domain, https://www.ohchr.org/sites/default/files/documents/issues/digitalage/artificial-intelligence-military-domain-briefer-1-en.pdf ; See also PI's Response to the Call for Input on Human Rights Implications of New and Emerging Technologies in the Military Domain, note above

[15] PI's Response to the Call for Input on Human Rights Implications of New and Emerging Technologies in the Military Domain, note above. PI has documented the use of commercial facial recognition systems in border management and post-conflict settings that are often operated by PMSCs and similar contractors. See for example in the UK, Privacy International's response to the UK Home Office consultation on facial recognition technology (5 March 2026) https://privacyinternational.org/advocacy/5741/privacy-internationals-response-uk-home-office-consultation-facial-recognition

[16] See report of the UN High Commissioner for Human Rights, A/HRC/39/29 (3 August 2018).

[17] PI, 'Responsible use and sharing of biometric data in counter-terrorism' (July 2020) https://privacyinternational.org/sites/default/files/2020-07/Responsible%20use%20and%20sharing%20of%20biometric%20data%20in%20counter-terrorism.pdf

1.5. Drones and other military-grade equipment

The use of drones and other military-grade equipment by PMSCs and mercenary actors represents a further dimension of the technology ecosystem that requires urgent regulatory attention. Sophisticated and highly intrusive technologies are becoming an integral part of PMSC operations: from drones equipped with high-resolution cameras and sensors capable of monitoring large areas and capturing real-time footage, to advanced biometric systems used to identify or authenticate individuals.[18]

Drones illustrate the blurring of lines between military and civilian technology. Commercial drones, originally developed for recreational or business purposes, are increasingly repurposed for military and security operations. Conversely, military-grade drones designed for battlefield surveillance have been deployed in civilian law enforcement and border management contexts.[19] In both directions of transfer, the deployment of these technologies by private actors typically occurs without the legal frameworks, human rights safeguards, or oversight mechanisms necessary to ensure compliance with international human rights law.

A significant structural feature of this market is the ownership overlap between the arms industry and the surveillance sector. Corporate Watch and PI have documented that many surveillance companies — including those providing drone technology and biometric systems — are part-owned by large arms producers.[20] A well-known security company responsible for building mass biometric databases in West Africa, for example, is part-owned by arms producers including Thales, Airbus DS, and Safran.[21] This integration means that the PMSC technology supply chain is, in many cases, inseparable from the conventional arms industry — yet subject to far weaker regulatory oversight.

[18] Schwitzguébel and Siatitsa, note above. See also, Thalif Deen, 'A Remotely-Piloted Weapon That Targets Civilians in War Zones' (18 March 2026) https://www.ipsnews.net/2026/03/a-remotely-piloted-weapon-that-targets-civilians-in-war-zones/; Corporate Watch and PI, 'Investigating dual-use technology and the darker side of innovation' (2025-26) https://privacyinternational.org/long-read/5705/investigating-dual-use-technology-and-darker-side-innovation

[19] PI, 'Challenging the Militarisation of Tech' (2025) https://privacyinternational.org/campaigns/militarisation-of-tech

[20] Corporate Watch and PI, note above.

[21] PI, 'Here's how a well-connected security company is quietly building mass biometric databases in West Africa with EU aid funds' (10 November 2020) https://privacyinternational.org/news-analysis/4290/heres-how-well-connected-security-company-quietly-building-mass-biometric

The deployment of drones in contexts where mercenaries and PMSCs operate raises specific concerns under international human rights law. The principles of legality, necessity, and proportionality apply to drone-based surveillance in both conflict and non-conflict settings.[22]

1.6. Data brokerage, ad-tech and the facilitation of surveillance-for-hire

A critical and insufficiently regulated vector of surveillance-enabled harm is the commercial data broker and advertising technologies ecosystem. This ecosystem enables the mass collection, aggregation, and sale of personal data — including precise location data, communications metadata, and behavioural profiles — without the knowledge or consent of the individuals concerned.[23] Investigations have documented the procurement of mobile advertising data — originally generated by smartphone applications for commercial targeting purposes — by intelligence contractors and government agencies.[24] The implications for the Working Group's mandate are direct. PMSCs and mercenary actors procure and acquire commercial data products that enable surveillance and targeting without ever deploying a dedicated surveillance tool subject to export controls. The regulatory gap is profound: data protection law does not cover national security buyers in most jurisdictions; export controls do not apply to data flows; and the intermediaries who supply data products face no due diligence obligation regarding their end-users.[25]

2. Surveillance as a service and data processing in operations

The growing role of PMSCs in physical security operations — and the human rights concerns this raises, particularly around the use of force — has received considerable attention over the past two decades. What has attracted far less scrutiny is the parallel and equally significant shift in the nature of private security services themselves. Rapid technological advancement has led PMSCs to increasingly prioritise private surveillance, data harvesting, and cyber operations over more traditional security functions.[26] This submission considers this shift to

[22] International Humanitarian Law has little to say when drones are equipped solely with surveillance technology; in those circumstances, it is international human rights law that provides the applicable framework. PI's Response … in the military domain, note above.

[23] PI, 'Uncovering the Hidden Data Ecosystem', https://privacyinternational.org/campaigns/data-brokers

[24] Joseph Cox and Dhruv Mehrotra, 'The Murky Ad-Tech World Powering Surveillance of US Military Personnel', *Wired* (11 February 2025) https://www.wired.com/story/rtb-location-data-us-military/

[25] PI's submission to the UN High Commissioner for Human Rights' report on the practical application of the United Nations Guiding Principles on Business and Human Rights to the activities of technology companies' (February 2022) https://privacyinternational.org/sites/default/files/2022-04/2022.02.23%20-%20PI%20Submission%20to%20OHCHR%20Report%20on%20UNGPs%20and%20Tech%20Companies.pdf

[26] Ilia Siatitsa, 'Exploring the Privatisation of Surveillance and its Human Rights Implications', *Private Security Considerations: The responsible security forum, ICOCA* (2026), https://blog.icoca.ch/exploring-the-privatisation-of-surveillance-and-its-human-rights-implications/

be of serious concern, precisely because it has occurred largely outside the regulatory frameworks developed to govern PMSCs conduct.

Highly intrusive surveillance technologies are now a standard feature of PMSCs operations. Companies are equipping themselves with drones fitted with high-resolution cameras and sensors capable of continuous area monitoring, advanced facial recognition systems for individual identification and authentication, and a growing array of other high-end surveillance tools.[27] The spread of these capabilities beyond state actors is already producing documented harms in civilian contexts: in the United States, facial recognition technology has been used by private companies to exclude individuals identified as unwanted from public venues;[28] in the United Kingdom, the Facewatch facial recognition network has raised serious concerns about the role of private operators in conducting biometric surveillance of the public without adequate legal basis or oversight.[29] At the early stages of the war in Ukraine, Clearview AI offered its services at the Ukrainian ministry of defense – this is the same company investigated and condemned by multiple data protection authorities around the world for unlawful processing of personal data of millions of people.[30] These examples illustrate a broader pattern of advanced surveillance technologies being deployed by private actors in an unrestrained and largely unregulated manner.

Beyond physical surveillance equipment, many PMSCs now market cybersecurity services — monitoring digital communications and networks ostensibly to detect threats and protect clients' infrastructure. In practice, these arrangements frequently grant PMSCs broad and largely unchecked access to personal data, with no clear limits on the scope of data collected, retained, or further processed. The same companies may additionally offer advanced data management and analytics services, enabling the processing of data at a scale and depth that goes well beyond what any defined security purpose would require.[31]

The intrusive character of these activities is compounded by the fact that data processing has become a commercial service in its own right, not simply a means of delivering security. As data-driven technologies and AI and machine learning capabilities have matured, the accumulation and retention of large datasets have become a commercial priority for many PMSCs, independent of any specific client contract or operational need. The data involved

[27] Security drones to the rescue in SA, ITWebs (2024) https://www.itweb.co.za/article/security-drones-to-the-rescue-in-sa/P3gQ2qGAg2D7nRD1 See further Section 2 above.
[28] Max Zahn, 'Controversy illuminates rise of facial recognition in private sector', abcNEWS (7 January 2023) https://abcnews.com/Business/controversy-illuminates-rise-facial-recognition-private-sector/story?id=96116545
[29] PI, 'Facewatch: the Reality Behind the Marketing Discourse' (2020) https://privacyinternational.org/long-read/4216/facewatch-reality-behind-marketing-discourse
[30] PI, 'The Clearview/Ukraine partnership - How surveillance companies exploit war' (2022) https://privacyinternational.org/news-analysis/4806/clearviewukraine-partnership-how-surveillance-companies-exploit-war
[31] PI and DCAF Policy Paper (2022), note above.

frequently includes categories that attract heightened legal protection — biometric data, information on political or religious opinions, data relating to sexual orientation — precisely because exposure of such data carries acute risks of discrimination, persecution, and serious personal harm.[32]

The regulatory challenge posed by these developments is substantial. Surveillance and data processing services are difficult to trace and monitor: unlike the deployment of armed personnel, they do not require a company's physical presence in the territory where its clients operate. Clients and vendors may be located in different jurisdictions, data may transit through third countries, and the contractual chains linking service providers to end-users may be deliberately obscured. The growing dependence of both public and private actors on PMSC-provided surveillance and data services, combined with the inherently transnational character of these operations, makes the development and application of robust international regulatory standards not merely desirable but urgent.[33]

3. Surveillance as a Gateway to Human Rights Violations: The Harm Chain

Privacy is a gateway right, essential for the enjoyment of other human rights.[34] Infringements of the right to privacy by private surveillance providers and technologies result in chains of cause and effect on other rights, such as the right to life.[35] If left unregulated, private surveillance can seriously impact the rights to privacy and data protection and further enable infringements on other human rights. This section sets out the primary human rights impacts that PI has documented in its research. privacy violations provide a gateway to the violations of other human rights.

Privacy violations are rarely a stand-alone harm. They provide the means through further violations is enabled: targeted persecution, mass discrimination, suppression of dissent, election manipulation, and physical harm up to and including extrajudicial killings.

[32] PI, Data Protection Guide' https://privacyinternational.org/data-protection-guide
[33] PI and DCAF Policy Paper (2022), note above; Siatitsa (2026), note above.
[34] As recognised by multiple General Assembly and Human rights council resolutions, as well as OHCHR. See for example, UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, *Report on Surveillance and Human Rights*, A/HRC/41/35 (2019) https://www.ohchr.org/en/documents/thematic-reports/ahrc4135-surveillance-and-human-rights-report-special-rapporteur. See further PI's Guide on international law and surveillance (2024) https://privacyinternational.org/report/5403/pis-guide-international-law-and-surveillance
[35] A/HRC/41/35, note above; See also PI's Response … in the military domain, note above.

3.1. The Right to Privacy

The right to privacy is enshrined in Article 17 of the International Covenant on Civil and Political Rights (ICCPR) and reflected in numerous regional instruments. While not an absolute right, any interference must be provided by law, pursue a legitimate aim, and be necessary and proportionate.[36] Private surveillance activities by mercenary and PMSC actors — whether through spyware, communications interception, biometric collection, or data profiling — typically take place without any of these safeguards.

The UN General Assembly has condemned unlawful or arbitrary surveillance and interception of communications as highly intrusive acts that violate or abuse human rights, in particular the right to privacy.[37] The processing of personal data by private security companies must be adequate, relevant, and limited to what is necessary for the purpose for which it is processed.[38] In practice, the operations of mercenary and PMSC actors consistently fall short of these requirements, and regulatory and judicial systems have often failed to hold them to account.

3.2. The Right to Life

Surveillance can be used to spy on, locate, track, and ultimately arrest, kill, or disappear people. Surveillance of specific individuals — often journalists, activists, opposition figures, and others exercising their right to freedom of expression — has been shown to lead to arbitrary detention, sometimes to torture, and possibly to extrajudicial killings.[39] The murder of journalist Jamal Khashoggi in 2018 demonstrated this link in a high-profile documented case: the mobile phones of family members and close friends had reportedly been targeted with Pegasus spyware by NSO Group prior to his extrajudicial execution.[40] The UN High Commissioner for Human Rights has also warned of the dangers of targeted hacking linked to extrajudicial killings. In Libya, the supply of communications surveillance systems by a private technology company to the Gaddafi intelligence services facilitated the targeting,

[36] CCPR, General Comment No 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation, 8 April 1988. See further PI's Guide on international law and surveillance, note above.
[37] See for example, UN General Assembly Resolution on the Right to Privacy in the Digital Age, A/RES/77/211 (15 December 2022) https://docs.un.org/en/A/RES/77/211
[38] PI and DCAF Policy Paper (2022), note above.
[39] PI and DCAF Policy Paper (2022), note above.
[40] Citizen Lab, 'Stopping the Press: New York Times Journalist Targeted by Saudi-linked Pegasus Spyware Operator' (2020) https://citizenlab.ca/research/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator; Report of the Special Rapporteur on extrajudicial, summary or arbitrary executions on the Investigation of, accountability for and prevention of intentional State killings of human rights defenders, journalists and prominent dissidents, A/HRC/41/36 (2019) https://docs.un.org/A/HRC/41/36

arrest, and imprisonment of thousands of people — subsequently leading to criminal proceedings for complicity in human rights abuses.[41]

3.3. The Rights to Freedoms of Expression, Assembly and Association

Private surveillance activities can directly infringe on people's freedom of expression, peaceful assembly, and association.[42] The UN Special Rapporteur on freedom of expression has concluded that interference with privacy through targeted surveillance is designed to repress the exercise of the right to freedom of expression.[43] The mere fact that surveillance is suspected can discourage individuals from meeting, assembling, or exchanging information — a chilling effect that suppresses the exercise of rights even in the absence of any further action by the surveilling actor. When journalists, lawyers, and activists know — or reasonably suspect — that their communications are being monitored, they self-censor. This suppresses the exercise of rights to freedom of expression, association, and assembly even in the absence of any further action by the surveilling actor.[44]

Many private surveillance companies provide services to states that use them to monitor journalists, human rights defenders, and political opponents. There are increasingly reports on private companies engaging in spying on human rights defenders, including through deceptive practices such as fake astroturfing campaigns on behalf of major polluters.[45] Private security companies have also been involved in election manipulation, directly affecting the right to democratic participation.[46]

3.4. The Right to Non-Discrimination

Surveillance technologies developed and implemented by private companies can be used to target individuals for monitoring, or even detention, based on their social origin, ethnicity, perceived behaviour, or appearance. Biometric surveillance is particularly concerning in this regard: many systems rely on predictive technologies susceptible to human and machine error, and some programmes are inaccurate in identifying members of certain racial, ethnic, or other groups, resulting in further discrimination.[47]

---

[41] PI and DCAF Policy Paper (2022), note above.
[42] PI, 'Privacy International's submission on the impact of digital and AI-assisted surveillance on assembly and association rights' (2026) https://privacyinternational.org/advocacy/5740/privacy-internationals-submission-impact-digital-and-ai-assisted-surveillance
[43] A/HRC/41/35, note above.
[44] *ibid*. See also PI's Response … in the military domain, note above.
[45] PI, 'Briefing: Controlling the UK's Private Intelligence Industry' (5 May 2022) https://privacyinternational.org/report/4850/briefing-controlling-uks-private-intelligence-industry
[46] Siatitsa (2026), note above.
[47] PI and DCAF Policy Paper (2022), note above.

PI is concerned about the use of profiling and automated decision-making for surveillance purposes, including with the aim of predicting behaviour. Many commercially available facial recognition systems have been found to have different error rates depending on race and gender.[48] These technologies are often deployed in particularly precarious situations — for example, at border controls, through which people in vulnerable positions pass every day — without having been adequately tested and without appropriate remedial mechanisms in place.[49]

Surveillance subjects women and LGBTQ+ communities to heightened risks of discrimination and harm. Surveillance targeted at women can have particularly serious effects, given that political, societal, and gender power asymmetries often grant authorities opportunities to weaponise extracted information through defamation, blackmail, and doxxing. Surveillance technologies and services are also used to target LGBTQ+ communities, including in contexts where same-sex relations are criminalised.[50]

4. Barriers to Accountability and Victims Redress

Even where the facts of surveillance-enabled harm are established, victims face profound structural barriers to obtaining attribution, justice, and remedy. These barriers are not incidental features of the current landscape — they are in significant part the product of deliberate design choices by the industries concerned, and they will persist unless specifically addressed through regulatory and procedural reform.

4.1. Corporate structural opacity

The commercial surveillance and private security sectors share a structural characteristic that severely impedes accountability: both are organised in ways that systematically obscure the chain of responsibility. Attribution — the identification of who deployed a surveillance tool, on behalf of which client, and for what purpose — requires access to records, export documentation, and corporate registries that are frequently unavailable to victims, their lawyers, or civil society. For instance, commercial spyware infrastructure is designed for operational security: command-and-control servers use obfuscated routing, ephemeral domains, and layered anonymisation to prevent forensic identification of the deploying

[48] PI, FRT submission (2026), note above.
[49] See for example, PI, 'Biometrics and counter-terrorism: Case study of Israel/Palestine' (May 2021) https://privacyinternational.org/sites/default/files/2021-06/PI%20Counterterrorism%20and%20Biometrics%20Report%20Israel_Palestine%20v7.pdf
[50] PI and DCAF Policy Paper (2022), note above.

actor.[51] Even where forensic analysis can establish that a particular tool was used against a particular target, tracing responsibility through a chain of vendor, reseller, integrator, and state or non-state client may be technically and legally impossible without compelled disclosure — which victims rarely have the procedural standing to obtain.[52]

4.2. Blanket exemptions as a regulatory barrier

Even where domestic legal frameworks exist that might otherwise provide victims with avenues for accountability, these frameworks are routinely rendered inaccessible by broad and poorly defined national security exemptions. PMSCs contracts similarly tend to include broad confidentiality provisions that restrict the disclosure of information about the scope and nature of services provided, the identity of clients, and the operational details of deployments. These provisions have a dual effect: they obstruct victims seeking to understand what was done to them and by whom, and they impede regulators and oversight bodies seeking to assess compliance with applicable legal requirements.

Data protection laws, which might in other contexts provide individuals with rights of access, correction, and redress in relation to the processing of their personal data, is similarly undermined by national security exemptions in most jurisdictions.[53] At least 137 countries have enacted data protection legislation, yet many of these laws contain exemptions for processing carried out for national security purposes — precisely the context in which the most serious PMSCs and mercenary surveillance activities occur.[54]

4.3. The transnational nature of operations and jurisdictional gaps

Mercenaries and PMSCs actors often operate across many different countries. Surveillance technologies can further enable them to operate from a distance. A typical surveillance operation may involve a vendor incorporated in one state, operating infrastructure hosted in a second, serving a client government in a third, targeting individuals in a fourth, and processing the resulting data in a fifth. Each element of this chain may fall under a different legal regime, with different rules on jurisdiction, disclosure, and liability — and with no single authority having visibility over the operation as a whole.

[51] EDRi, 'Spyware and state abuse: The case for an Eu-wide ban' (June 2025) https://edri.org/wp-content/uploads/2025/06/EDRi_Spyware-position-paper.pdf
[52] A/HRC/41/35, note above.
[53] PI, 'Responsible use of biometrics…', note above.
[54] Tara Davis, 'Data Protection in Africa: A look at OGP Member Progress', altAdvisory and Open Government Partnership (August 2021) https://www.opengovpartnership.org/wp-content/uploads/2021/08/OGP-Data-Protection-Report.pdf

Existing instruments — the UN Guiding Principles on Business and Human Rights, the Montreux Document, the International Code of Conduct for Private Security Service Providers[55] — while they provide useful guidance with regard to the international standards, are non-binding and do not create enforceable jurisdictional rules. Proposals for a binding treaty on business and human rights, and for a specific instrument on PMSCs, have not yet resulted in agreed frameworks.[56]

5. Recommendations

The convergence of surveillance technology industry with mercenary and PMSCs activity represents one of the most significant and underregulated human rights challenges of the current period. PI's submission has sought to demonstrate that the technology enabling these actors — spyware vendors, AI profiling systems, data brokers, cloud infrastructure — constitutes an integrated ecosystem of enablement, and that privacy violation within this ecosystem is not the only harm but the mechanism through which further violations is produced. The Working Group's forthcoming report has an opportunity to establish, for the first time, a comprehensive and authoritative account of how this ecosystem operates, who its actors are, what harms it generates, and what regulatory frameworks are required to address it.

PI encourages the Working Group to make the following recommendations to states to:

- Recognise the significant role of the surveillance industry — including spyware vendors, data brokers, and analytics companies in the operations of PMSCs and mercenary actors, and that their activities must be brought within the scope of applicable human rights and private security governance frameworks;
- Address the absence of specific regulatory guidance on drone deployment by private actors, and to call for states to clarify the rules and restrictions applicable to surveillance services provided by PMSCs using drone technology, including in the context of armed conflict;
- Address the data brokerage ecosystem as an enabling infrastructure for mercenary and PMSCs activity, and to call for regulatory frameworks that impose end-use restrictions and due diligence obligations on data brokers comparable to those applicable to arms and dual-use goods exporters;

[55] International Code of Conduct for Private Security Service Providers (ICoC), Geneva (2010); Montreux Document on Pertinent International Legal Obligations and Good Practices for States related to Operations of Private Military and Security Companies in Armed Conflict (2008).

[56] Open-ended intergovernmental working group on a possible legally binding instrument on private military and security companies (IGWG), established by HRC resolution 15/26 (2010). PI supports the conclusion of a binding treaty.

- Highlight that the deployment of surveillance technologies by or through PMSCs and mercenary actors impacts the enjoyment of human rights, including in particular the right to privacy;
- ensure that regulatory and oversight bodies responsible for licensing and monitoring PMSCs have the technical expertise, adequate resources, and institutional independence necessary to effectively oversee the use of surveillance technologies, including in extraterritorial operations;
- ensure that comprehensive national data protection law apply to the activities of PMSCs and surveillance providers and that data protection authorities are empowered to enforce those frameworks in respect of private surveillance services provided for security or intelligence purposes;
- to guarantee that victims of surveillance-enabled harm by PMSCs and mercenary actors have access to effective remedies; and
- advance negotiations towards a binding international instrument on PMSCs that explicitly covers the provision of surveillance technologies and data services, consistent with existing international human rights and humanitarian law obligations.