Hidden risk is the most expensive

High-risk surveillance tech thrives in the shadows

Introduction

Everyone pays the price when surveillance technology is abused. The disproportionate extraction, exploitation and weaponisation of data can corrode civic space, degrade democracy and destabilise markets. Surveillance technology companies are, as a result, under mounting scrutiny from policymakers, regulators, and the public because of the immense and often irreparable harm their products can cause to individuals and communities. But misuse of these technologies is often obscured by claims that they enhance public safety. In reality, responsible investors seeking to align portfolios with long-term value creation, stability, and international law must be able to recognise these technologies, commit to undertaking continuous, heightened human rights due diligence on investee firms or companies linked to these technologies, and refuse to fund business models that facilitate human rights harms.

Proper scrutiny of these firms brings a key reality into sharp relief: surveillance technology companies that are unable to meaningfully answer heightened human rights due diligence questions have no place in responsible investor portfolios. Any company selling high-risk technologies must have robust risk mitigation efforts built into their business models and operations.

This guide seeks to better equip investors to avoid unnecessary risks and help push technological innovation in a more rights-respecting direction – which is particularly urgent given the growing allure of funding a rapidly growing sector at the intersection of security, innovation and rising government demand. It provides guidance on identifying and preventing exposure to high-risk surveillance technologies and related products that increase legal, operational and reputational risks linked to the abuses these tools enable or perpetrate. These range from harming civilians in conflict zones to tracking and targeting activists, journalists, political dissidents, lawyers, and judges exercising free speech or seeking to uphold the rule of law, amongst other violations. The frequent absence of meaningful human rights safeguards, policies, or oversight mechanisms within these types of companies heightens the danger of investor complicity and associated consequences for these harms, which have been found to be serious, widespread, and irremediable.

These risks are growing.

Such companies are the focus of sustained media investigations, civil society campaigns and legal challenges across multiple jurisdictions. And with good reason: witness the tens of thousands of people listed as potential targets of NSO Group's Pegasus spyware; the weaponisation by governments around the world of Predator software, and the many other other spyware companies operating out of the spotlight, skirting export controls and selling to authoritarian regimes. Spyware, for example, has also allegedly been used against business leaders providing a glimpse into how it can impact business operations, intellectual property and trade secrets. Companies producing technology marketed for "lawful interception" are of particular concern. These include firms that develop spyware technology, but also "spyware-adjacent" tech – digital forensics, cell site simulators (CSS) and deep packet inspection (DPI) tools – that are rapidly proliferating.

Allegations of abuse associated with the misuse of these technologies is increasing. Companies producing the following types of surveillance tech have been identified as contributing to human rights abuses related to the extraction of personal information through these tools:

- **Spyware:** covert malware installed on a device to secretly monitor, collect, and transmit information about individuals or organisations in real time, often without their knowledge or consent.
- **Digital forensics:** tools are designed to access, copy, and analyse data from devices, enabling both one-time and ongoing monitoring, sometimes supplemented with external data sources via open source investigation techniques.
- **Cell site simulators:** devices that mimic legitimate cell towers to trick nearby mobile phones into connecting, allowing interception of communications, identification of device owners, and tracking of their location.
- **DPI:** a network monitoring technology that inspects the contents of data packets passing through a network, allowing filtering, analysis, surveillance, traffic shaping, and identification of applications or content beyond basic header information.

Many companies that sell these high-risk technologies assert that they are "not surveillance firms" or "data brokers", or that they have no access to user data or control over their clients. In practice, these are often revealed to be simply public relations defences designed to obscure accountability for products that are, in fact, dangerous by design. This guide provides detail on each of these tools to aid investors in risk identification and mitigation but also in fulfilling a critical role in disrupting these patterns of harm, in fulfilment of their responsibilities under the UN Guiding Principles on Business and Human Rights. As this guide will explain:

- **These high-risk technologies carry unquantifiable legal and reputational liabilities that can rapidly destroy value.** Surveillance tools marketed for "lawful interception" are increasingly linked to human rights abuses, creating exposure to sanctions, litigation, export restrictions, criminal investigations, and global media scrutiny. Because the underlying risks stem from how the products enable harm, not just who the client is, investors cannot reliably model the downside. The result is tail-risk exposure that cannot be diversified away, and societal consequences that are largely irremediable.
- **Business models built on opaque contracts lack transparency and defensibility.** Investors that have limited visibility into who the end-users are, how products are being deployed, or whether the activity complies with international human rights standards are ultimately investing in black boxes. Risk may be acceptable, but uncertainty without information is not suitable for securing financial returns or for democratic societies.
- **Weak oversight and accountability structures create systemic risk that investors will be expected to absorb.** Firms routinely claim they "only sell to democracies," "comply with local laws," or "lack access to user data," yet documented evidence shows these assurances do not prevent or mitigate harm. These claims are reputational cover, not risk controls. Without enforced human rights due diligence, investors inherit responsibility for abuses facilitated by the products.

Responsible investors have a unique opportunity to contribute to the emancipatory potential of a tech sector designed to support the public good. Investment in surveillance technology – without proper safeguards and a clear understanding of the risk of misuse of these products – may do just the opposite.

How to use this guide

This guide is designed to aid investors in:

- **Understanding** the capabilities of high-risk surveillance technologies and identify exposure within their portfolios that include vendors of these tools;
- **Identifying** reasonably foreseeable or actual human rights harms linked to these high-risk surveillance technologies, using real case studies; and
- **Effectively engaging** with potential or actual portfolio companies to better ensure compliance with responsible investment policies and commitments.

Current practices of high-risk surveillance tech companies

In March 2025, the Business and Human Rights Centre (BHRC) conducted an analysis of 41 surveillance tech companies and found that **80% lack publicly available human rights policies**, offering no clear commitments to prevent misuse of their products. Furthermore, **61%** of the companies reviewed **do not have a business code of conduct**, raising concerns about ethical governance.

High-risk surveillance technology types

This guide contains overview of four categories of surveillance technology: **spyware**, **digital forensics**, **cell site simulators (CSS)** and **deep packet inspection (DPI)** tools. Each are high risk and merit heightened human rights due diligence by investors and companies. For each technology type, this guide contains:

- An infographic demonstrating how the tool works
- A brief description of the tool's capabilities
- Red flag keywords for how companies typically market these technologies
- A brief overview of the level of control technology companies could have over the product/service once sold to the client
- Basic human rights impact assessment, including salient human rights risks, organised through the categories of: scale, scope, and remediability
- An explanation of who can be directly or indirectly impacted by the abuse of the technology
- Examples of which other actors in the business ecosystem may act against these high-risk surveillance technologies
- Case studies demonstrating legal, operational, regulatory and reputation risk

Available resources for conducting due diligence on high-risk surveillance tech companies

Beyond UN, EU, OFAC and other sanctions lists, as well as the United States BIS Entity List, there are a number of civil society resources that can be referenced during due diligence exercises:

- Business and Human Rights Centre Database of human rights harms linked to surveillance technology companies
- Surveillance Watch Database of surveillance companies and their investors
- The Atlantic Council's Mythical Beasts Mapping of spyware companies and their investors
- Mapping the location of manufacturers of spyware and other cyber-surveillance tools, SIPRI
- Litigation and other formal complaints related to mercenary spyware, Citizen Lab
- Surveillance risks in conflict-affected & high-risk areas: a salient & material concern for investors, Heartland Initiative
- Navigating the surveillance technology ecosystem: A human rights due diligence guide for investors, Heartland Initiative, the Business and Human Rights Centre, Access Now, Gulf Centre for Human Rights, Agentur.ru, Paradigm Initiative, and R3D.

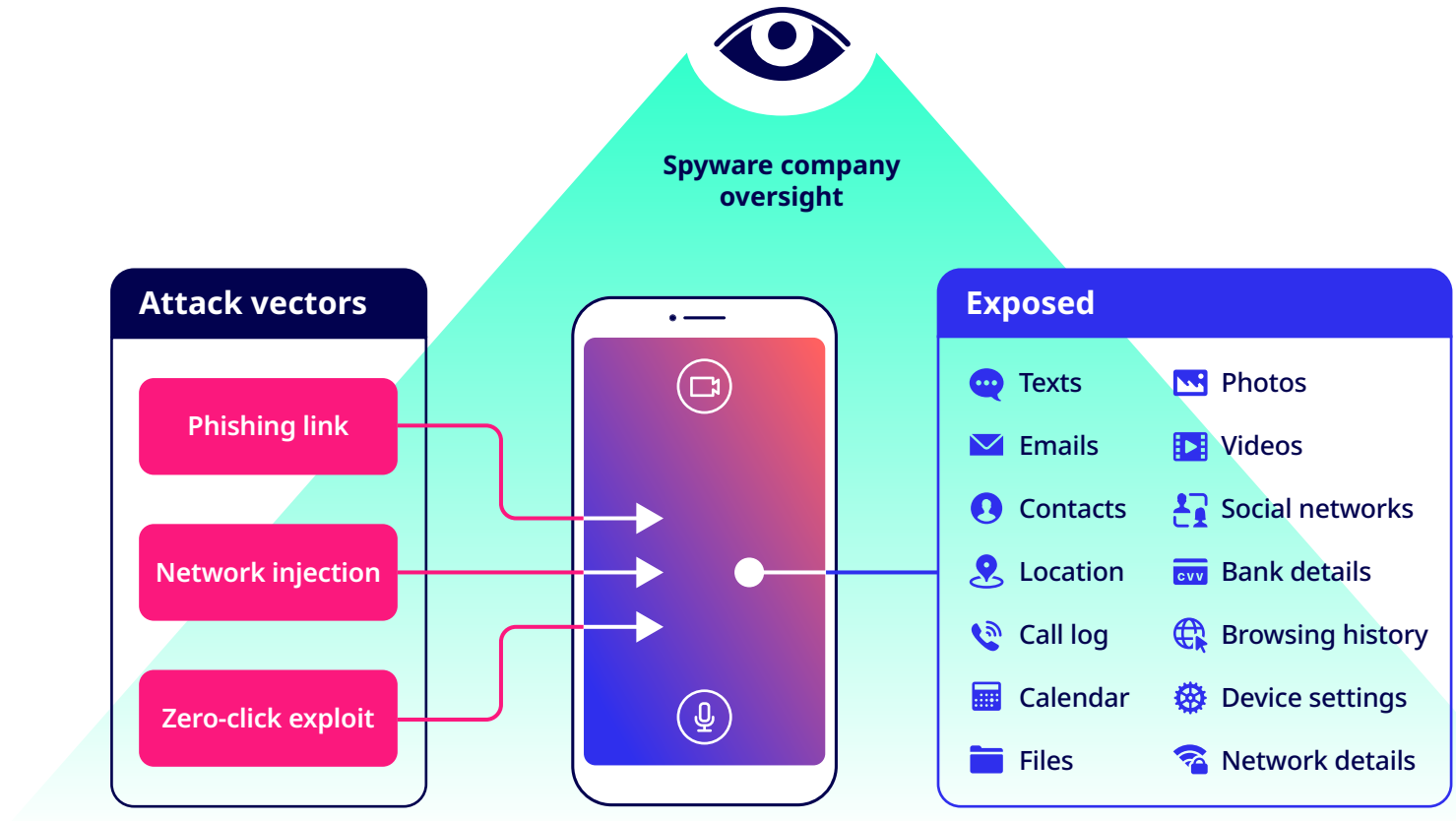
Are you looking to identify companies commercialising these technologies linked to your portfolio?

Contact us to learn more about how to effectively leverage the BHRC database to support your due diligence processes: **techaccountability@business-humanrights.org**

Spyware

Spyware is a hidden malware that enables covert monitoring of individuals or organisations. It continuously extracts data from the targeted device without the owner's knowledge or consent and enables a third party/perpetrator to activate the device's capabilities. These capabilities may include decrypting communications, accessing passwords, geolocation data, calendar records, photos, videos, phone calls, contact lists and browsing history, as well as changing device settings and activating the microphone and camera, for the purpose of surveillance.

Red flag terms for portfolio managers to trigger additional due diligence: Spyware vendors sell these highly intrusive software apps or programs to customer operators, often marketing the technology as "zero-click access", "real-time intelligence", "silent infection", "lawful interception" or "offensive cyber" solutions. Vendors will typically offer operator training, installation support and "operational guidance", including how to navigate related control dashboards.



Human rights assessment

Scale: *How grave is the impact when the tool is abused?*

Severe. Targeted individuals (often journalists, activists, lawyers or political dissidents) may self-censor or disengage from activism due to the fear of being surveilled, tracked, followed, physically attacked or even killed. Their sense of safety and privacy is compromised and their ability to speak freely or participate in civil society is deterred.

Given the ongoing and persistent nature of surveillance, it is significantly worse than other forms of technology that perpetrate privacy violations. In repressive regimes, spyware infections have led to imprisonment, forced disappearances, torture or other reprisals against the individual or their network.

Spyware can constitute a form of tech-facilitated gender-based violence (TfGBV). Women and LGBTQIA+ individuals face aggravated impacts of surveillance as the personal information extracted is often weaponised to intimidate, harass and isolate the victims.

Beyond immediate threats, spyware can lead to social isolation, reputational damage, job loss and persistent fear. Its effects are often cumulative and enduring, impacting mental health, trust and the ability to participate safely in public or private life.

Scope: *How widespread is the impact when the tool is abused?*

Broad. Spyware rarely affects only its initial target. One infected device can expose entire contact networks, revealing messages, files and location data of hundreds or thousands of people. Continuous monitoring expands that circle of exposure over time, while most victims remain unaware due to the absence of effective notification systems.

If there is continuous monitoring enabled, a progressively longer list of impacted persons continues to grow while the spyware remains undetected.

Due to lack of proper and consistent notification protocols, victims and those in contact with them may never know they were once a target of continuous monitoring.

Remediability: *Is it possible to counteract or rectify the resulting harm?*

Irremediable. Replacing the device cannot fully restore privacy or safety. Once deployed, spyware perpetrates other violations linked to the right to privacy that may be impossible for a company to rectify.

The effects on the individual, including intimidation, imprisonment, physical harm, death or, for example, the exposure of journalists' networks of trusted contacts, cannot be undone. Rebuilding trust and repairing personal, professional or community harm is extraordinarily difficult, making remediation nearly impossible.

Key considerations for human rights due diligence

Based on previous cases, which are the most salient human rights risks?

- Right to life
- Right to privacy
- Freedom of expression
- Freedom of the press
- Freedom of assembly
- Due process and right to a fair trial
- Right to be free from arbitrary detention
- Freedom from torture

Right to privacy: *What kind of data is exposed?*

Spyware can extract data such as contacts, messages, call logs, browsing history, and live geolocation, along with usernames, passwords and financial details. More advanced spyware may also record calls, activate the microphone or camera, and capture encrypted chats before they're secured. Massive amounts of personally identifying information (PII) are exposed when a single device is infected with spyware, including PII about people within the periphery of an infected device or persons who have sent images, messages or other forms of multimedia to the device – a key consideration for companies operating in jurisdictions with strong data protection laws where regulators may take action against companies improperly managing PII.

Rightsholders: *Who can be directly or indirectly impacted by the abuse of the technology?*

- **Directly impacted:** Individuals specifically targeted with the software that is installed on their devices.
- **Indirectly impacted:** Anyone who communicates with or is associated with the directly impacted individual or organisation, as their private data or communications could also be compromised. Anyone within their physical vicinity, such as during in-person conversations, may be recorded. Friends, loved ones and family members may then also be targeted with spyware based on the information that is collected, expanding the list of those directly impacted.

Corporate control: *What level of control can a company have over the product/service once sold to the client?*

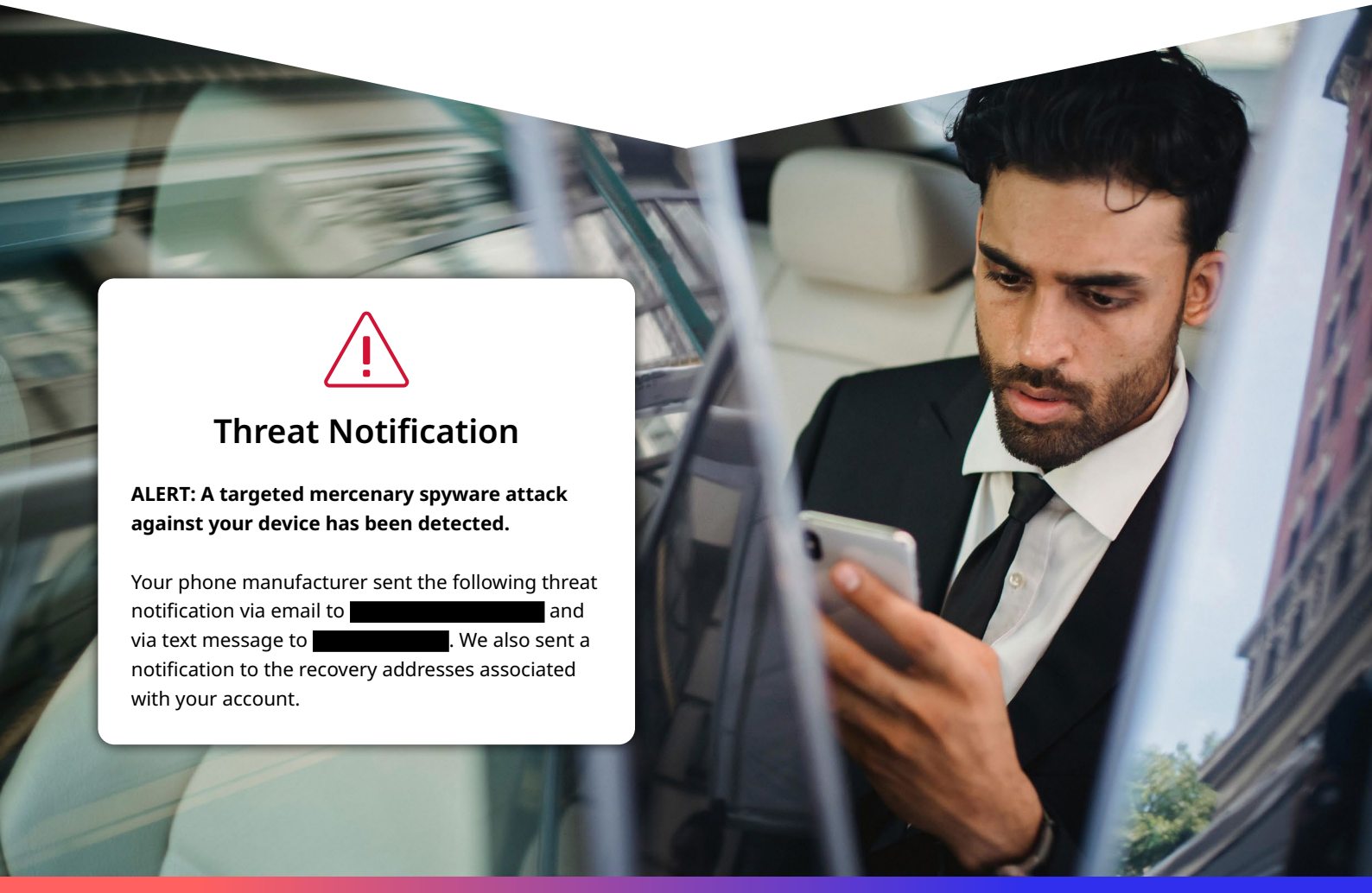
High. Spyware often requires continuous updates to bypass security patches. Vendors usually keep the customer dependent on them for product functionality and new exploits. Vendors also offer ongoing services such as subscriptions for updates, exploit packs, or cloud-based control dashboards. In some cases, as seen later in the WhatsApp vs. NSO case, the company may allegedly be directly involved in installing and extracting data from targeted phones using their spyware.

Corporate ecosystem: *Which other corporate actors have an incentive to take (legal, regulatory, operational) action against spyware companies?*

Mobile phone manufacturers, application and operating systems developers and cloud service providers whose platforms and products are directly exploited to deliver spyware infections (e.g. Apple, Google, WhatsApp/Meta) may initiate lawsuits, shut down operational infrastructure, or participate in the generation of regulatory risk for spyware companies through push notifications citing company names. The security and integrity of their operating systems and apps are essential to their business models and user trust. These stakeholders can substantially influence the operating environment for spyware products by terminating services, banning companies from their platforms and taking legal action.

Accountability considerations: *Will the target know that they have been impacted?*

Unlikely. Spyware is specifically designed to deceive the targeted individual and avoid detection. Whether the individual becomes aware depends on the complexity of the spyware targeting. A device can be infected without the target interacting with the malicious content (a "zero click" attack/exploit). In other examples, a target clicks on a piece of malicious content, which facilitates the infection (a "one-click" attack/exploit). It requires highly specialised technical skills to detect spyware on a device. Tech companies such as Meta and Apple have begun sending notifications to warn users when their devices may be infected with spyware, although it is not immediate nor guaranteed that they will be notified due to a lack of standardised notification protocols.



Case studies

NSO Group Technologies Ltd. (NSO Group) – developer of "Pegasus"

Human rights incidents/allegations

- **2016-2021:** In July 2021, the French nonprofit Forbidden Stories launched the Pegasus Project, which exposed more than 50,000 leaked phone numbers identified as likely targets of NSO customers. Notably, the data revealed numerous states with well-documented rights-violating behaviour, including Bahrain, Morocco, Saudi Arabia, India, Mexico, Hungary, Azerbaijan, Togo, Kazakhstan and Rwanda, that used Pegasus to surveil human rights defenders, political dissidents, businesspeople and journalists. NSO denied the allegations, calling them "uncorroborated theories."

Additional reporting on Pegasus alleges:

- **2019-2023 – Jordan:** NSO Group technology used against 35 journalists, lawyers and activists. Forensic analysis confirmed most of the infections. NSO Group says that it vets customers and investigates any reports that its spyware has been abused. A 2022 report on a smaller group of Pegasus victims in Jordan identified two operators of the spyware that may have been agents of the Jordanian government.
- **2020-2023 – EU:** NSO Group technology reportedly used against Russian, Belarusian, Latvian and Israeli journalists and activists based in the EU, with forensic analysis identifying most of the infections.
- **2021 – Bahrain:** A Bahraini human rights activist was targeted with Pegasus technology, as identified by forensic analysis. NSO Group did not answer specific questions.
- **2022 – Lebanon:** NSO Group technology allegedly targeted a senior Human Rights Watch (HRW) employee. The company told HRW that it was *"not aware of any active customer using [its] technology against a Human Rights Watch staff member"* and that it would open an initial assessment into allegations.
- **2020-2021 – El Salvador:** 35 journalists targeted by Pegasus, as identified by forensic analysis. 23 journalists were associated with independent investigative outlets in El Salvador, which have often published reporting critical of the Salvadoran government.
- **2021 – Morocco/Western Sahara:** NSO Group technology used to target a human rights activist, as identified by forensic investigation. The Moroccan authorities deny using Pegasus on activists.
- **2021 – Togo:** Phones of at least two journalists were infected with Pegasus.
- **2021:** According to Amnesty International, the phone numbers for 14 heads of state, including *"French President Emmanuel Macron, Pakistan's Imran Khan and South Africa's Cyril Ramaphosa, as well as hundreds of government officials, were selected as people of interest by clients of spyware company NSO Group."* NSO denied that Macron or Mohammed VI were ever targeted by clients and insists that its spyware is meant only for terrorists and serious criminals, pledging to "investigate all credible claims of misuse" and act if they are confirmed.

Allegations involving conflict zones

- **2020-2022 – Azerbaijan-Armenia:** NSO Group technology was allegedly used to hack Armenian media, civil society and human rights representatives, as confirmed by forensic analysis: *"Circumstantial evidence suggests that the targeting is related to the military conflict in Nagorno-Karabakh (also referred to as the Republic of Artsakh in Armenia) between Armenia and Azerbaijan. This is the first documented evidence of the use of Pegasus spyware in an international war context."* NSO Group stated that it could not comment on the report because it had not been shared with the company.

- **2023 – Israel-Palestine:** NSO Group reportedly enlisted by Israeli security services to track hostages in Gaza. NSO Group declined to comment. In 2021, forensic analysis identified Pegasus on phones belonging to Palestinian human rights activists.

Legal risk (lawsuits)

Punitive damages:

- **2025 – California, USA:** The District Court ordered NSO Group to pay $167 million to Meta in damages for hacking WhatsApp accounts in 51 different countries including those belonging to journalists, activists and government officials. NSO Group has challenged the ruling.

Criminal investigations and lawsuits:

- **2024 – UK:** Criminal complaint filed by activists against NSO Group, parent company Q Cyber Technologies and owner Novalpina Capital.

Public prosecutor action: Public prosecutors have opened investigations into NSO Group in Spain, Hungary, Poland, France and Mexico.

Civil lawsuits: Activists, journalists and individuals targeted by spyware have filed ongoing civil lawsuits against NSO Group in five jurisdictions.

Operator lawsuits: Public investigations and civil lawsuits have also been brought in relation to NSO Group's government customers in Saudi Arabia, UAE, Bahrain, Thailand, Spain, Colombia, Israel, the EU, Hungary, Poland, India and Mexico.

Compliance and operational risk

Sanctions and export controls:

- **2021 – USA:** Department of Commerce placed NSO Group on the Entity List. The White House stated that the company had *"enabled foreign governments to conduct transnational repression."*

Bans by intermediary service providers and app ecosystems:

- **2021:** Amazon Web Services shut down infrastructure and accounts linked to NSO Group following publication of the Pegasus Project. AWS's infrastructure was allegedly used to deliver spyware to targets.

Investor action, divestment pressure and asset devaluation:

- **2025:** NSO Group was acquired by US investors for "several tens of millions of dollars." The transaction is "expected to include the divestment of NSO's roughly $500 million debt." According to Techcrunch, an NSO spokesperson confirmed these details and then later declared that they were "off the record."

- **2022:** NSO Group was deemed "valueless" according to BRG, the consultancy brought in to manage Novalpina Capital (owner of NSO Group). The allegation was made in a UK High Court case BRG filed against two founders of the fund. NSO Group commented that this information was "baseless." (In July 2021, EY reportedly valued NSO Group at $2.3 billion. NSO declined to comment.)
- **2022:** The Oregon Education Association, AFL-CIO and AFSCME unions approved a resolution calling for Oregon's pension fund to complete an "immediate and complete" divestment from the fund that owns NSO Group. NSO did not respond to requests for comment.

Intellexa Consortium (Intellexa) – developer of "Predator"

The Intellexa Consortium is a joint venture between Nexa Technologies, Passitora (formerly known as WiSpear), Cytrox and Senpai Technologies. Cytrox develops Predator.

- **October 2023:** The "Predator Files" reveals extensive sales of Intellexa consortium's technology to countries with poor human rights records including Oman, Qatar, Congo, Kenya, UAE, Pakistan, Jordan and Vietnam. None of the Intellexa Consortium responded to requests for comment, except from the main shareholders and some former Nexa group executives, who claimed that the Intellexa alliance "has ceased to exist."
- **2022 – Sudan:** Intellexa technology was reportedly imported into Sudan for use by the RSF militia. Intellexa and its executives did not respond to requests for comment.

Legal risk (lawsuits)

Criminal prosecution of executives:

- **2025 – Greece:** Criminal prosecution of three former executives of Intellexa, which marketed the technology Predator. This was allegedly used against journalists in Greece, and ten victims have filed civil lawsuits.

Criminal investigations and lawsuits: Public prosecutors in the EU have opened investigations into Cytrox/Intellexa.

Operator lawsuits: Public investigations and civil lawsuits have also been brought in relation to government customers of Cytrox/Intellexa in Greece.

Compliance and operational risk

Sanctions and export controls:

- **2024 – USA:** Imposes sanctions against executives of Intellexa consortium.
- **2023 – USA:** Department of Commerce places four companies in the Intellexa consortium on export Entity List, including Cytrox, which makes Predator.

Bans by intermediary service providers and app ecosystems:

- **2021:** Meta bans Cytrox and other surveillance companies acting on findings from Citizen Lab report.

Other spyware companies

- **Paragon, 2025 – Italy:** Paragon technology (Graphite) allegedly found on Italian journalists' devices, as identified by forensic research. The Italian government denies that it deployed the technology against journalists. In response to reporting, Paragon and the Italian government reportedly ended their contract.

- **Saito Tech (formerly Candiru), July 2021:** Candiru technology was used to hack at least 100 victims including human rights activists, dissidents and journalists in Palestine, Israel, Iran, Lebanon, Yemen, Spain, UK, Turkey, Armenia and Singapore, according to forensic analysis. Researchers also found 750 fake websites that contained spyware, posing as groups including Amnesty International and the Black Lives Matter movement. Candiru did not respond to requests for comment.

- **Memento Labs (formerly Hacking Team), 2015:** A hacker leaked internal Hacking Team documents revealing sales contracts with repressive regimes, including Ethiopia, Myanmar, Qatar, Russia, Sudan,and Syria (Hacking Team maintained that it had always sold within the law).

- **FlexiSPY, May 2025:** FlexiSPY spyware was allegedly installed on two filmmakers' phones while the devices were in Kenyan police custody. FlexiSPY did not reply to outreach from the Committee to Protect Journalists.

Allegations involving conflict zones

- **Saito Tech (formerly Candiru), 2023 – Israel-Palestine:** Candiru and Paragon were reportedly enlisted by Israeli security services to track hostages in Gaza.

Legal risk (lawsuits)

Criminal prosecution of executives:

- **FinFisher, 2023 – Germany:** Prosecutor criminally indicted former executives of FinFisher for unlawfully supplying the Turkish secret services.

Criminal investigations and lawsuits: Public prosecutors have opened investigations into FinFisher in Germany.

Operator lawsuits: Public investigations and civil lawsuits have also been brought in relation to government customers of Gamma Group/FinFisher in Bahrain and Ethiopia, and Paragon in Italy.

Compliance and operational risk

Sanctions and export controls:

- **2021 – USA:** The Department of Commerce placed Candiru, Positive Technologies, Computer Security Initiative Consultancy (COSEINC) on the Entity List.

Investor action, divestment pressure and asset devaluation

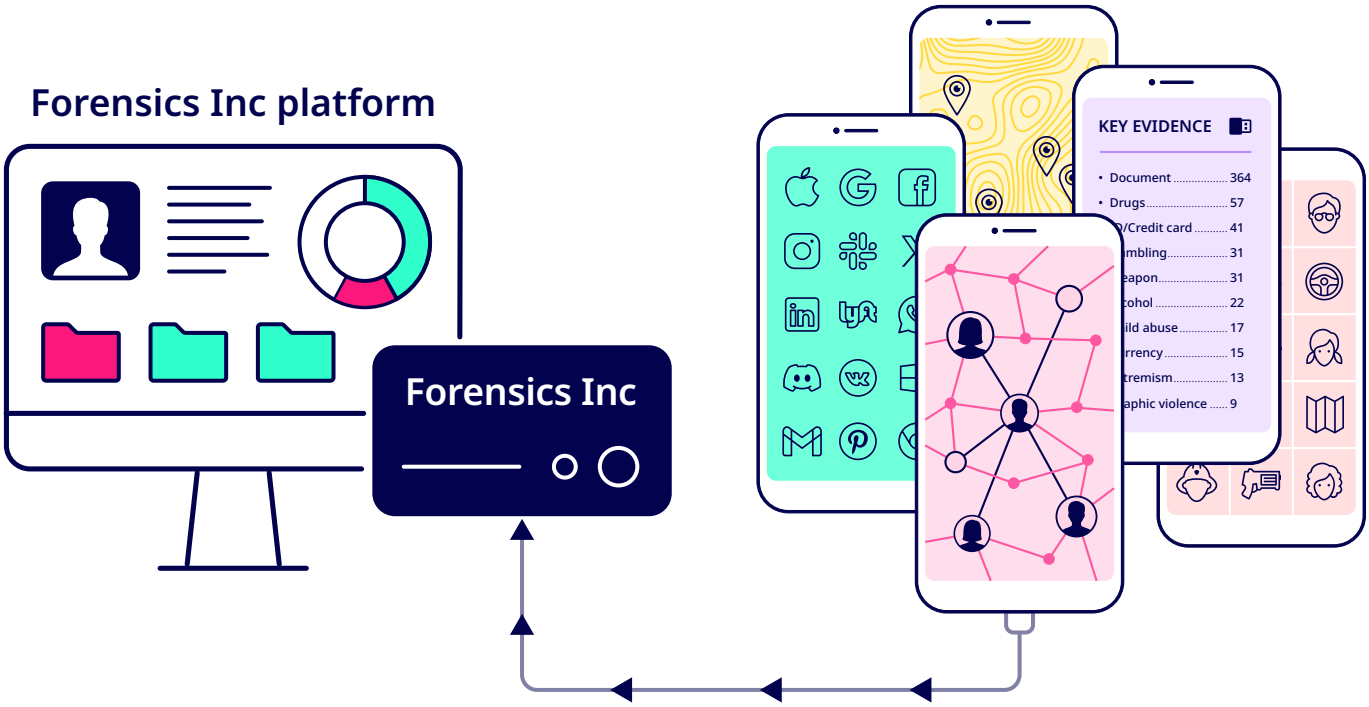
- **Variston, 2025:** Variston reportedly liquidated. Its closure follows a 2022 Google report revealing the company's spyware products.
- **QuaDream, 2023:** QuaDream reportedly shuts down after it was revealed that it was used against journalists, opposition politicians and NGOs.
- **FinFisher, 2022:** FinFisher files for insolvency after the Public Prosecutor's Office seizes the company's accounts following a criminal complaint filed by civil society.
- **eSurv, 2021:** eSurv declares bankruptcy. In 2019, Naples prosecutor's office opened an investigation into eSurv for uploading spyware apps to Google PlayStore.
- **Memento Labs (formerly Hacking Team):** Following its 2015 hack, Hacking Team reportedly struggled to maintain contracts and retain staff due to its links to human rights abuse and reputational damage. In 2019, it was acquired by InTheCyber to become Memento Labs. As recently as 2020, media articles reported that Memento Labs is struggling to maintain staff and secure clients. According to Paolo Lezzi, Chairman of Memento Labs, the company ended its affiliation with InTheCyber two years ago.

  Memento Labs' chairman Paulo Lezzi told CPJ in a November 2020 email that customers were all government or law enforcement agencies and that the company limited the time period for installing their technology to a period of months. Licences for their products would not be renewed if "there is a violation of human and/or political rights by the country or, more specifically, the exact customer" during that period. Reputational risk continues to build for Memento Labs, given recent allegations linked to spyware use in Russia and Belarus.

Digital forensics – extraction and Open Source Intelligence Tools (OSINT)

Forensic extraction tools are sold as specialised hardware kits with extraction software and analytic capabilities. They enable one-time data extraction (creating a metaphorical "screenshot image" of all data within a device) that typically requires physical access to the target's device. The tools may not require any involvement from the device owner, may be able to bypass device passwords, and may extract passwords for cloud services and other apps, which can facilitate longer term continuous monitoring. Other digital forensics tools collect and integrate data from multiple sources, including open source intelligence (OSINT) datasets that are enriched by third parties. Vendors typically offer the core product and support services (e.g. how to operate extraction devices and platforms, interpret reports and use evidence in court testimony). They may offer renewable certification programmes.

Red flag terms for portfolio managers to trigger additional due diligence: The tools can be described or marketed as "data recovery platforms", "digital forensics investigation" and "investigative analytics software."



Human rights assessment

Scale: *How grave is the impact when the tool is abused?*

High. Individuals lose full control over their personal information, often without consent or awareness. Targeted use against journalists, activists, political dissidents or marginalized groups can stifle communication and reporting, chilling public participation. Extracted data can facilitate targeted arrests, interrogations or other forms of coercion. In authoritarian contexts, digital forensic and extraction tools have been used in combination with detention or intimidation, increasing the risk of torture, imprisonment or reprisals. Unlike a typical data breach, forensic extraction devices enable comprehensive and precise access to private and often encrypted data, allowing authorities or malicious actors to bypass protections that are supposed to safeguard personal information. Beyond immediate risks, data collected can be used for ongoing surveillance, social profiling, blackmail or harassment. Targets may experience lasting psychological distress, professional and social harm.

Scope: *How widespread is the impact? (How many people are impacted directly and indirectly?)*

Broad. While forensic extraction typically requires physical access to specific devices, impacts are not limited to the individual. One seized device may expose hundreds or thousands of contacts and sensitive messages and networks. The impacts are linked to all individuals that may have some link to the device (contacts, photographs, messages) at that point in time.

Remediability: *Is it possible to counteract or rectify the resulting harm?*

Irremediable. Once data has been copied, the privacy violation is permanent. Sensitive contacts, communications and networks are already exposed. Harassment, intimidation, legal persecution or arbitrary detention based on extracted data cannot be undone. To return to the pre-abuse state would require recalling or destroying all copied data, something over which victims have no control. Restoration requires rebuilding trust, repairing personal and professional networks, and in many cases addressing physical or psychological harm, which may not be possible.

Key considerations for human rights due diligence

Based on previous cases, which are the most salient human rights risks?

- Right to life
- Right to privacy
- Freedom of expression
- Freedom of the press
- Freedom of assembly
- Due process and right to a fair trial
- Right to be free from arbitrary detention
- Freedom from torture

Right to privacy: *What kind of data is exposed?*

Forensic extraction tools can collect system details, contacts, call logs, texts, emails, photos, videos and app data from messaging or social platforms. They can also recover deleted files, access location history and extract browser activity, giving a deep view into a device's previous usage.

Rightsholders: *Who can be directly or indirectly impacted by the abuse of the technology?*

- **Directly impacted:** Targeted individuals whose phones are confiscated for digital forensic extraction. In the case of OSINT, it is easier to target individuals with an expansive online presence, less awareness about digital hygiene best practices, or whose data has been leaked in data breaches.
- **Indirectly impacted:** Anyone who communicates with or is associated with the directly impacted individual or organisation, as their private data or communications could also be exposed via forensic extraction. In the case of OSINT, relationship data graphs could point to and correlate with other individuals who are not the initial target, which might violate their privacy.

Corporate control: *What level of control can a company have over the product/service once sold to the client?*

Medium to high. The core hardware/software works offline, but licences, updates and new device support (new iOS/Android versions, new exploits, updates to the software) are usually locked to vendor subscriptions. Access to the extracted data is typically available to the client and potentially the company that has developed the tool. Based on terms of service, the developer may set up cloud services needed for storing and analysing the data, or conduct data analysis as an added service.

Corporate ecosystem: *Which other corporate actors have an incentive to take (legal, regulatory, operational) action against digital forensics and extraction companies?*

Device manufacturers, application developers and cloud service providers have the greatest stake (Google, Apple, Whatsapp/Meta etc.). Their reputation relies on the security of the data stored on their devices and in their cloud services.

Accountability considerations: *Will the target know that they have been impacted?*

Potentially. Targets will likely know when a physical device has been seized (especially if they are forced to disclose passwords), but they may not know that forensic extraction technology has been deployed on their device. In the case of cloud extraction, device data may be continuously extracted without the target's knowledge. It requires highly specialised technical skills to detect evidence of forensic extraction use on a device.

Associated risks: *Has this technology been linked to spyware injections?*

Yes. Spyware injection and forensic extraction tools serve different purposes: spyware provides ongoing remote monitoring, while forensics tools typically perform one-time data extraction when a device is accessed. However, some advanced forensic platforms may use exploit-like techniques to unlock devices, blurring the line between spyware and forensic access methods. In 2024, forensic analysis reported that the Serbian police and intelligence authorities had used Cellebrite forensic technology to unlock journalists and activists' devices. Once unlocked, the authorities infected the devices with NoviSpy spyware. In response, Cellebrite stated that its products are "licensed strictly for lawful use."

Case studies

Cognyte Software Ltd. (Cognyte)

On 1 February 2021, Verint announced that it had completed its split of the company's intelligence and cyber activities into a new company named Cognyte Software Ltd.

Human rights incidents/allegations

- **2020 – Myanmar:** Cognyte reportedly won a 2020 tender to supply extraction technology to Myanmar state telecoms firm one month before the 2021 military coup.
- **2015-2017 – South Sudan:** Verint reportedly provided communications interception equipment to the South Sudanese authorities, who are alleged to target political critics.
- **2018 – Azerbaijan:** Verint reportedly provided training to Azerbaijan authorities on its products, with the government asking for specific training on how to target LGBTQIA+ minorities, according to whistleblower allegations.

Legal action

- **2023 – Israel:** Human rights activists filed a criminal complaint with the Attorney General in relation to Cogynte's sale to Myanmar state-backed telecoms company a month prior to the military coup. The deal was made despite Israel's claims to stop defence technology transfers to Myanmar following a 2017 ruling by Israel's Supreme Court. In 2024, the Attorney General found that it did not have a licence for the sale, but did not open an investigation.

Operational risk

- **2021:** Meta blocked OSINT tool providers Cognyte and CobWeb's access to its platform after Meta threat teams identified that it was using the platform to target politicians and journalists. Cognyte reported that it made modifications to certain features in response to Meta's allegations.

Investor backlash, divestment pressure and asset devaluation

- **2023:** Storebrand ASA, and by extension Equinor Asset Management, excluded Cognyte due to the risk of human rights violations in several high-risk countries, among them Myanmar.
- **2022:** Norges Bank excluded Cognyte due to an unacceptable risk of contributing to serious human rights abuses.

Cellebrite DI Ltd. (Cellebrite)

Human rights incidents/allegations

- **2025 – Georgia:** Human rights advocates called on Cellebrite to review its contracts with Georgia, raising concerns that the technology is used against protestors.
- **2024 – Serbia:** Serbian security services reportedly used Cellebrite technology to extract data from journalists and activists, including for spyware installation, based on forensic analysis by Amnesty International's Security Lab. In response, Cellebrite suspended the Serbian authorities' use of the tools.
- **2022:** Russia's main investigative arm reportedly used Cellebrite technology after Cellebrite officially halted sales to the country in 2021. Cellebrite has described these allegations as "completely false."
- **2022:** Human rights advocates raised concerns of Cellebrite's sales to Ugandan authorities, and led a campaign for Israel Defense Export Control Agency intervention. Two publications quote Cellebrite stating that it always ensures that its tools are only used for legal and ethical purposes.
- **2019 and 2020 – Botswana:** In at least two separate cases, Cellebrite technology reportedly used by Botswana police to search journalists' devices.
- **2020 – Hong Kong:** Hong Kong police reportedly used Cellebrite technology to extract data from pro-democracy activists' phones. Cellebrite later reported that it had stopped sales to China and Hong Kong following civil society advocacy. The company stated that it does not sell to sanctioned countries.
- **2017 – Myanmar:** Cellebrite technology was reportedly used to arrest two Reuters journalists investigating a military massacre of Rohingya Muslims in Rakhine state.

Compliance

- **August 2020 – Israel:** 61 petitioners, including human rights activists, filed legal petitions against the Ministry of Defence and Cellebrite to prevent exports to Hong Kong, Russia and Bangladesh in relation to reported misuse against human rights activists. Cellebrite later stopped business in China and Hong Kong, and proactively stopped selling to Russia but reported that it may be impacted by reputational damage.

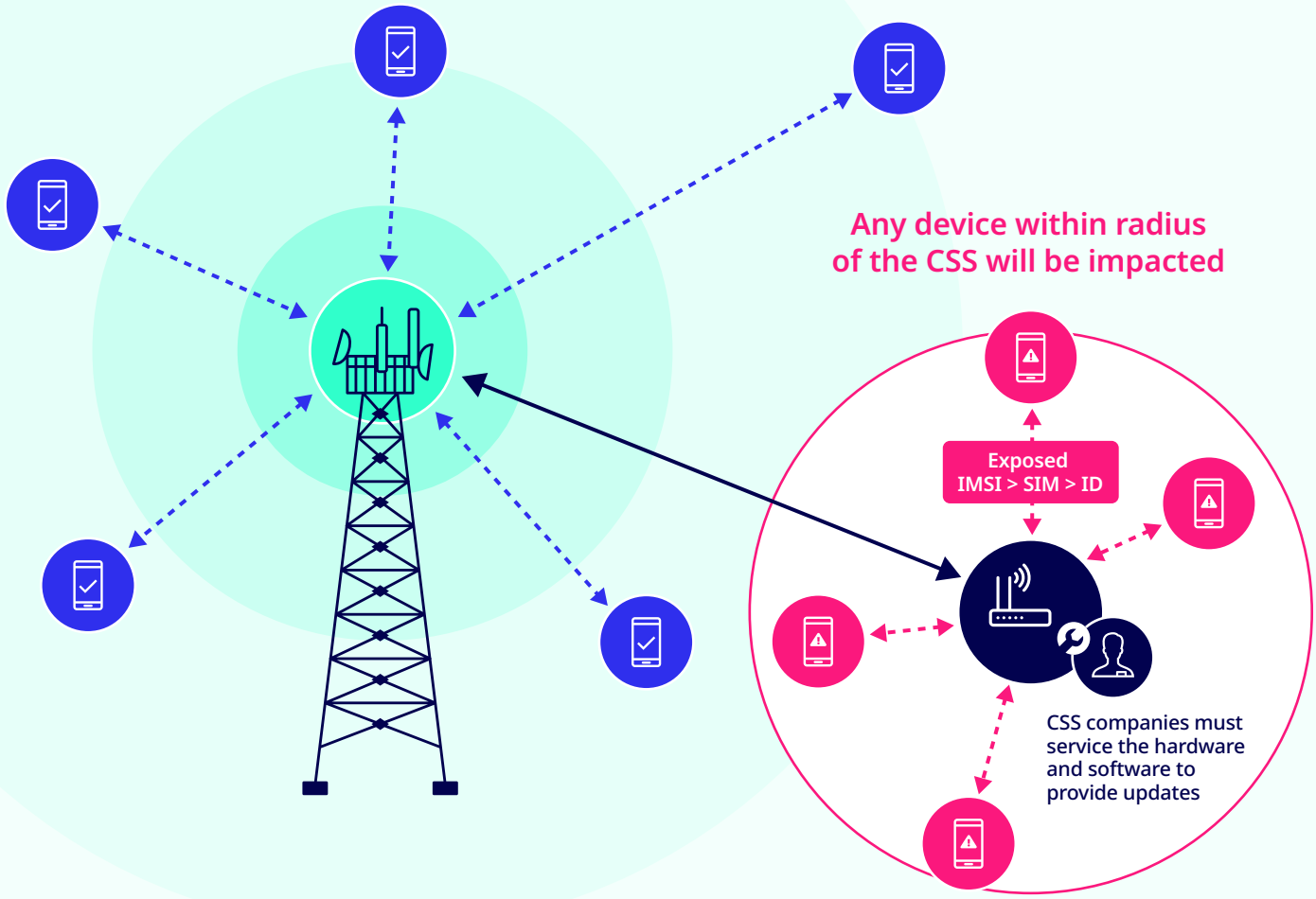
Micro Systemation AB (MSAB)

- **2020 – Hong Kong:** Hong Kong police reportedly used MSAB products to extract data from pro-democracy activist Joshua Wong's phones. MSAB allegedly withdrew from China and Hong Kong in 2020, following changes in US policy including the Hong Kong Autonomy Act (which sanctions individuals and entities that contribute to the erosion of Hong Kong's autonomy).
- **2019 – Myanmar:** MSAB reportedly sold tools to the Myanmar police in 2019, two years after the country's security forces began a crackdown on the minority Rohingya population. MSAB revoked product licenses following the 2021 coup and reportedly prevents further technology updates.

Cell site simulators

Cell site simulators (CSS) mimic cell towers, trick nearby mobile devices into connecting with them, and collect unique device identifiers such as the International Mobile Subscriber Identity (IMSI) – the 15-digit number that identifies a mobile phone user on a cellular network. With this data, CSS operators can uniquely identify device owners, and locate a device in a given location at a specific time. They may include functionality to intercept calls or texts. CSS include hardware – including portable physical interception devices that can be carried in backpacks or briefcases – and management software.

Red flag terms for portfolio managers to trigger additional due diligence: They are also known as IMSI catchers or Stingrays. Stingray is a popular CSS technology manufactured by the Harris Corporation (now the L3Harris corporation, following the 2018 merger with L3 Technologies Inc.), and has since become a generic term for the technology type. CSS are also marketed as "tactical interception" devices or "passive/active GSM interception" devices.



Human rights assessment

Scale: *How grave is the impact when the tool is abused?*

High. CSS indiscriminately capture identifiers, metadata and sometimes content from all mobile devices within range. CSS erode privacy and anonymity in public spaces. They are particularly harmful when deployed against protesters or vulnerable groups, enabling tracking, intimidation and mass arrests. There is a chilling effect on freedom of expression, assembly and association.

Scope: *How widespread is the impact? (How many people are impacted directly and indirectly?)*

Broad. CSS impact all internet-enabled devices and affiliated persons within a geographic area (range) of the CSS during its use. They impact targeted individuals and bystanders indiscriminately.

Remediability: *Is it possible to counteract or rectify the resulting harm?*

Irremediable. The physical and psychological impacts of hyper-surveillance, intimidation, arbitrary detention and overall social control cannot be easily undone, if at all. One would need to eliminate all copies of intercepted data, release anyone arrested or "ensure the security of anyone" targeted based on the "data" capture, and re-establish safe conditions for freedom of expression/assembly/association, which is an exhaustive long term and sociopolitical process.

Key considerations for human rights due diligence

Based on previous cases, which are the most salient human rights risks?

- Right to life
- Right to privacy
- Freedom of expression
- Freedom of the press
- Freedom of assembly
- Due process and right to a fair trial
- Right to be free from arbitrary detention
- Freedom from torture

Right to privacy: *What kind of data is exposed?*

CSS collect device and subscriber identifiers such as IMSIs, along with metadata about calls, texts and location. They can map which phones are nearby, track movement and intercept or block communications.

Rightsholders: *Who can be directly or indirectly impacted by the abuse of the technology?*

- **Directly impacted:** Any owner of an internet-enabled device within the radius of the active CSS – any device that connects with the CSS will "have its data captured" by the technology.
- **Indirectly impacted:** Anyone who communicates with the targeted individuals, as their conversations may be intercepted.

Corporate control: *What level of control can a company have over the product/service once sold to the client?*

Medium. The hardware is physically owned by the operator, but vendors may restrict software updates and frequency bands (which can be remotely managed).

Corporate ecosystem: *Which other corporate actors have an incentive to take (legal, regulatory, operational) action against CSS companies?*

Mobile network operators (e.g. Verizon, AT&T, T-Mobile) have the greatest stake. CSS interfere with their cellular networks, potentially causing service disruptions and creating security risks for their customers, which directly impacts their core business.

Accountability considerations: *Will the target know they have been impacted?*

Unlikely. Most people cannot tell if their phone is connected to a CSS, since these devices impersonate cell towers and operate silently. Possible clues include sudden drops to 2G (where surveillance is easier), unusual call failures or battery drain, but reliable detection usually requires special apps or dedicated hardware. In practice, the best protection is using end-to-end encrypted apps for calls and messages, since CSS mainly expose metadata. It is difficult to prove that a specific device was hit by a specific CSS without corroborating evidence, such as independent network monitoring or data from the cellular provider.

Associated risks: *Has the technology been linked to spyware injections?*

Yes. CSS mainly collect device identifiers and metadata, but some advanced models can also push malicious configuration messages, downgrade connections or inject traffic. CSS has been marketed specifically as an “infection vector” for spyware solutions. In practice, this would mean attempted spyware installation, although this requires more sophisticated capabilities than basic IMSI collection.

Case studies

Human rights incidents/allegations

While there are substantial human rights concerns, allegations and litigation focused on CSS, such activities focus primarily on transparency around CSS operators and technology deployment. As described, CSS operate for a brief period, and are not well-suited for retroactive forensic assessment to determine which brands are associated with the use or abuse of the technology. The lack of transparency is further compounded by reported manufacturer and vendor practices. For example, in 2014, media reporting revealed that Harris Corp, the major CSS manufacturer, had non-disclosure agreements with US police departments that explicitly prohibited disclosure about their use of Harris Corp's CSS equipment. Harris Corp said that it could not comment.

- **2025 – USA:** Public records revealed that Immigration and Customs Enforcement (ICE) procured CSS in May 2025 (the documents did not specify the CSS manufacturer). ICE has a long history of reported use of CSS.
- **2020:** American Civil Liberties Union (ACLU) analysis of ICE public records disclosure revealed that ICE had upgraded from Harris Corp's Stingray II technology to "Crossbow". As of January 2020, this was still in use.
- **2025 – Iran:** Miaan, the Iranian human rights organisation, reported that Iranian authorities use a surveillance apparatus that includes CSS to systematically identify, track and intimidate women who defy the mandatory hijab law.
- **2024 – Russia-Ukraine:** Russia reportedly used CSS to gather personal details on mobiles used by Ukrainian soldiers and locate military targets.
- **2021 – Bangladesh:** The Bangladesh army reportedly purchased CSS which can monitor hundreds of devices at once through PicSix linked company Sovereign Systems in 2018. Sovereign Systems denies the reported allegations and states that it did not sell IMSI catchers. PicSix did not respond.
- **2018 – Guatemala:** Guatemalan authorities reportedly conducted a large-scale operation to target "activists, entrepreneurs, politicians, journalists, diplomats and social leaders" with CSS.
- **2017 – Kenya:** Kenyan state actors reportedly employed CSS as part of a broader, largely unregulated communications surveillance programme, leading to gross human rights abuses such as arbitrary arrests, torture, and enforced disappearances.

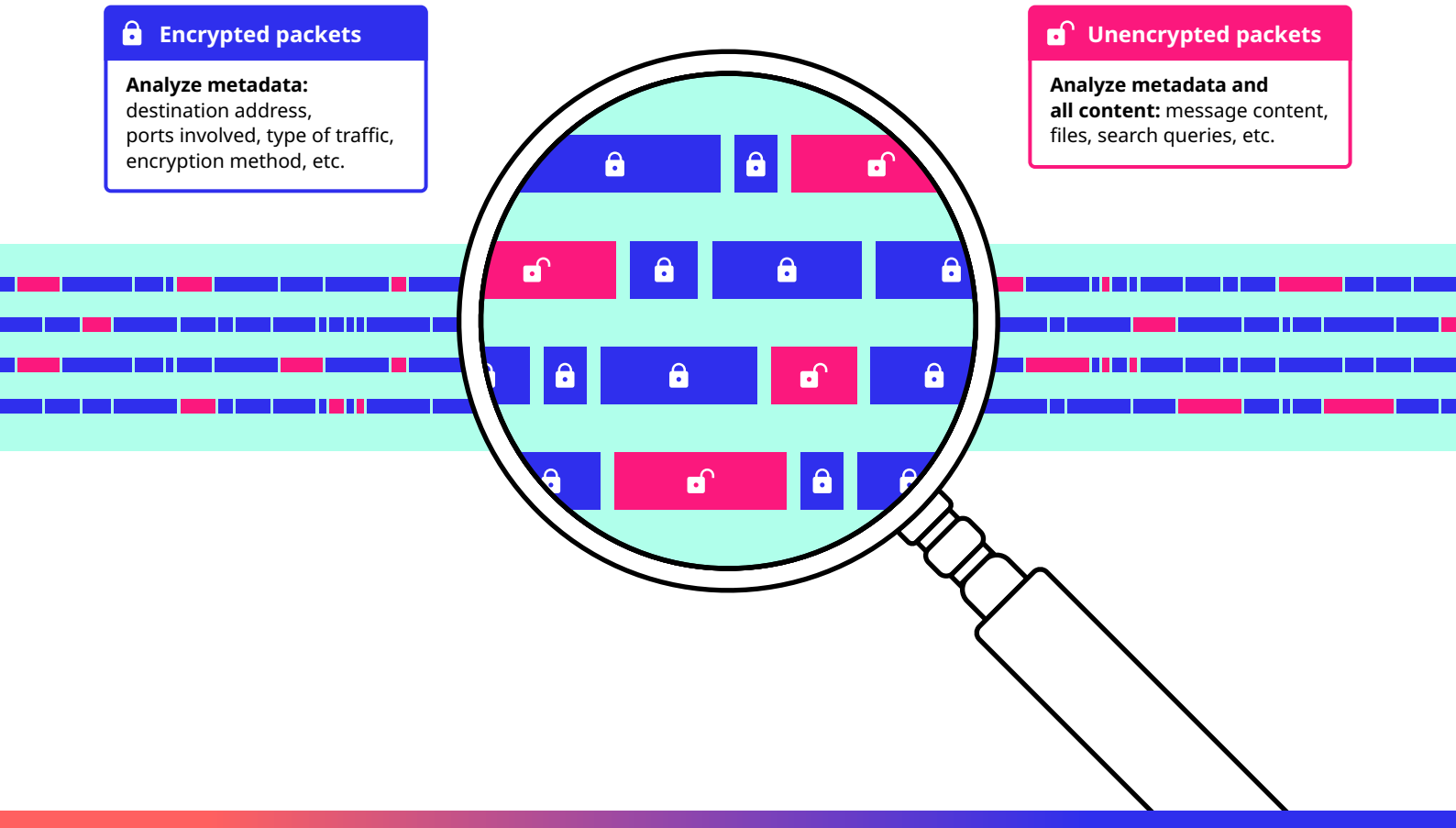
Notable legal action focuses primarily on disclosure of operators' use of the technology:

- **2021 – USA:** The City of Tacoma agreed to pay $311,607 to resolve a case in which the Tacoma Police Department improperly withheld information related to its use of a CSS. The case was filed by the ACLU of Washington.
- **2019 – USA:** The American Civil Liberties Union (ACLU) sued the US Customs and Border Patrol (CBP) and ICE for failing to promptly respond to a public records request on the agencies' use of CSS. The request followed reports on the use of the tool to locate, arrest and prosecute an individual on immigration charges. In response to ACLU legal action, the agencies shared records, which revealed that ICE had used CSS at least 466 times from 2017-2019.
- **2019 – UK:** Privacy International (PI) filed public records requests to various police forces, the Home Office and National Police Chiefs' Council seeking records related to UK police purchase and use of CSS. PI submitted the requests following an October 2016 article by The Bristol Cable citing evidence that – from the available information – was understood to be a reference to police use of CSS. The requests were denied.

Deep packet inspection

Deep packet inspection (DPI) technology lets telecommunications network operators look inside internet traffic to block, redirect or monitor it.

Red flag terms for portfolio managers to trigger additional due diligence: Network equipment vendors supply these large-scale hardware appliances alongside analytics software, often marketing it as "content policy enforcement", "website filtering solutions", "network security and traffic management", or "Lawful Interception Management Systems (LIMS)". Large vendors may bundle the equipment with professional services, deployment consulting and training for network operators or government staff.



Human rights assessment

Scale: *How grave is the impact when the tool is abused?*

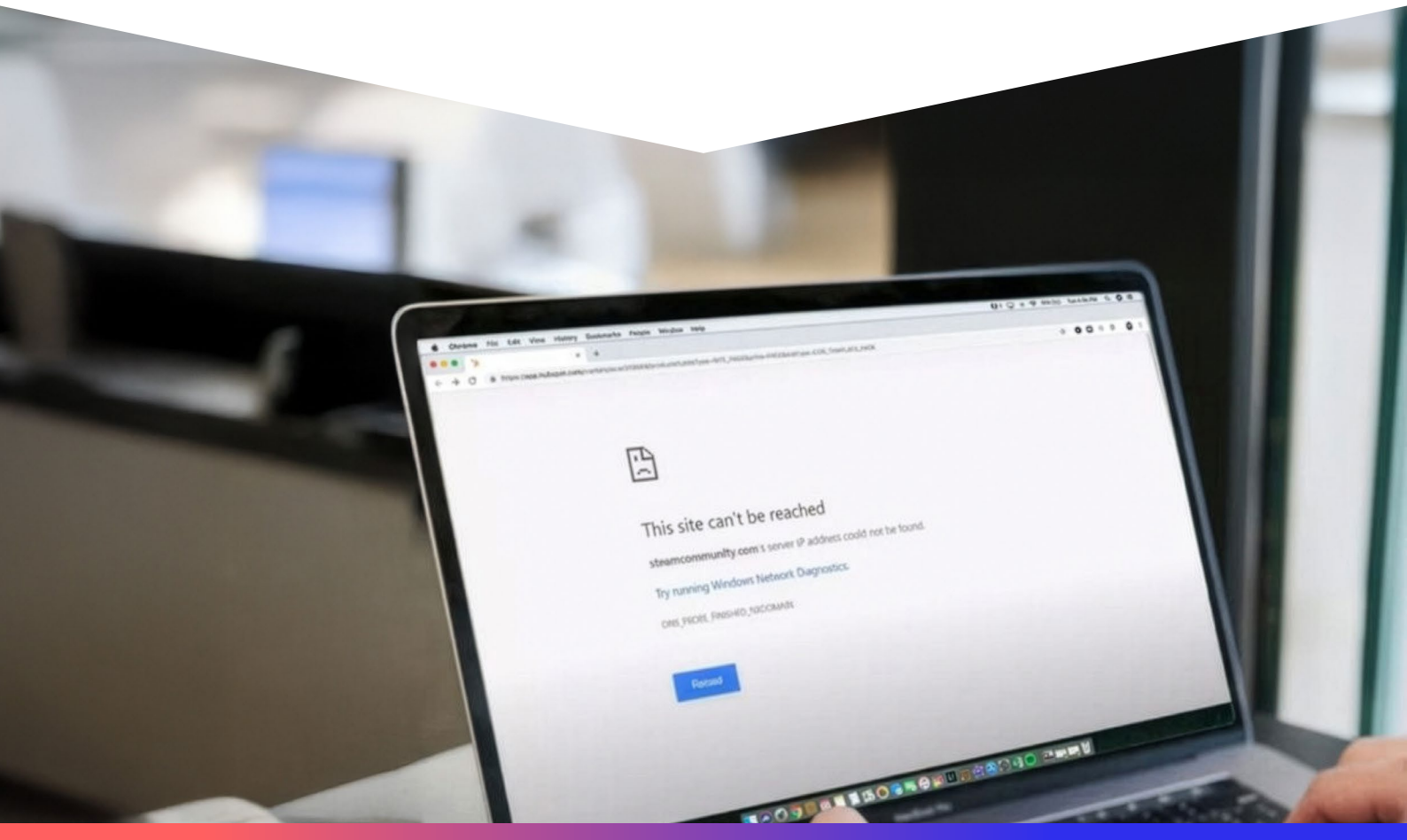
High. Abuse of DPI technologies allows states or powerful actors to intrusively monitor, censor and profile "unencrypted" digital activity at the content level – emails, messages, downloads and searches. DPI abuse has been linked to systemic violations affecting entire populations, undermining freedom of expression, access to information and the right to privacy on a massive scale.

Scope: *How widespread is the impact? (How many people are impacted directly and indirectly?)*

Systemic. DPI impacts all users on the network. This has led to mass surveillance of broad swathes of populations, crippling civil society and increasing the probability of attacks against human rights defenders.

Remediability: *Is it possible to counteract or rectify the resulting harm?*

Irremediable. The psychological impacts of mass surveillance last across generations. Chilling effects on speech, lost opportunities and repression of civil society often persist even if monitoring stops. Returning to a pre-abuse state would require dismantling DPI infrastructure, ending censorship, deleting surveillance records and re-establishing an environment of trust and safety for civic life, which is a systemic and sociopolitical, not just technical, challenge.



Key considerations for human rights due diligence

Based on previous cases, which are the most salient human rights risks?

- Right to life
- Right to privacy
- Freedom of expression
- Freedom of the press
- Freedom of assembly
- Due process and right to a fair trial
- Right to be free from arbitrary detention
- Freedom from torture

Right to privacy: *What kind of data is exposed?*

DPI collects and analyses the contents of network traffic including websites visited, search queries, and unencrypted messages or files. It can log metadata such as IP addresses, device details and communication patterns, and can also block, throttle or alter specific traffic. In effect, it provides detailed visibility into both what users are accessing and how they're using the network.

Rightsholders: *Who can be directly or indirectly impacted by the abuse of the technology?*

- **Directly impacted:** Any user of the network. Unlike the other technologies listed in this guide, DPI is implemented on network infrastructure, not end user devices.
- **Indirectly impacted:** Websites, services, and applications that have their traffic manipulated, potentially affecting their performance or accessibility for users.

Corporate control: *What level of control can a company have over the product/service once sold to the client?*

High. DPI systems need frequent vendor updates (signatures, analytics models). Licensing models are often subscription-based, meaning that the vendor maintains strong leverage.

Corporate ecosystem: *Which other corporate actors have an incentive to take (legal, regulatory, operational) action against DPI companies?*

DPI allows Internet Service Providers (ISPs) to identify and slow down traffic from specific services. DPI can be used to favour certain corporate-affiliated content or services over those of competitors. It has previously been abused to censor specific media outlets, but any business model that relies on a consistent, high-quality and real-time internet connection to deliver its service can be financially impacted by the abuse of DPI.

Accountability considerations: *Will the target know they have been impacted?*

Unlikely. People generally can't tell if their traffic is being intercepted with deep packet inspection, since it happens invisibly within the network. At most they might notice slower connections, blocked content or VPN disruptions, but reliable detection requires technical analysis tools.

To confirm DPI abuse, you would need to run sophisticated network tests, often from multiple locations and with different ISPs, to compare performance. This is something that only network experts, researchers or regulatory bodies can do, not the average citizen.

Associated risks: *Has this technology been linked to spyware injections?*

Yes. DPI gives a network operator or attacker the ability to inspect and manipulate traffic flows, which can be used to inject malicious payloads, fake updates or altered downloads that install spyware on a device. In this way, DPI can serve not just for monitoring but also as a delivery channel for targeted spyware attacks. A 2018 CitizenLab report revealed that Sandvine technology was used to redirect users in Turkey and Egypt to a platform containing state-sponsored spyware. Sandvine did not comment on the existence of business dealings in these countries, citing contractual confidentiality clauses.

Case studies

AppLogic Networks (formerly Sandvine)

Human rights incidents/allegations

- **2018-2020 – Egypt and Turkey:** In 2020, forensic analysis indicated that Egyptian telecommunications operators allegedly used deep packet inspection technology to block more than 600 websites, including the independent news website Al-Manassa. Sandvine did not respond to a request for comment. In 2018, forensic analysis indicated the technology had been used to block dozens of human rights, political and news websites in Egypt and Turkey.

- **2020:** Internal documents and employees reportedly allege that deep packet inspection technology was used in a number of countries with human rights concerns. This included blocking livestream social media video content in Azerbaijan; enabling internet shutdowns of Facebook, WhatsApp and websites in Jordan; blocking various websites in Eritrea and Thailand; blocking independent news websites in Egypt and Uzbekistan; enabling Egypt, Uzbekistan, Russia and Afghanistan to log user's web browsing history; and agreeing to provide tools to the Algerian government to log the online activity data for up to 10 million internet users. Sandvine declined to comment on specific deals, but stated that its technology was used to protect "from billions of malicious internet transactions linked to illicit and illegal activities".

- **2020 – Belarus:** Sandvine DPI technology was reportedly used to shut down internet access and repress protests following the Belarusian presidential election. An internal investigation by Sandvine revealed that custom code had been inserted into the company's product to thwart the free flow of information. As a result, Sandvine stated that it will no longer provide the Belarus government with software updates and technical assistance, although its technology is still usable in the short term.

Compliance and operational risk

- **2024 – USA:** The Department of Commerce placed Sandvine (now AppLogic) on the Entity list from February-October 2024, stating that Sandvine's DPI technology was used for mass web monitoring, censorship and to target political actors and human rights activists in Egypt. The blacklist created substantial financial difficulties – Sandvine lost customers and was unable to access its US stockpiles or components manufactured by US companies. It also lost relationships with major technology service providers, including Zoom and Microsoft. Sandvine conducted mass layoffs in 2024. Sandvine was removed from the Entity List in October 2024, following changes in its corporate practices, including exiting Egypt and 55 other countries with poor human rights records. Civil society groups have warned that this delisting was premature.

Other DPI companies

- **Geedge Networks, 2025 – Myanmar, Pakistan, Kazakhstan and Ethiopia:** The Chinese company allegedly exports censorship technologies to Myanmar, Pakistan, Kazakhstan and Ethiopia. In Pakistan, Geedge has reportedly repurposed infrastructure left behind by Sandvine. Geedge Networks did not respond to questions.

- **Cisco, 2024 – China:** US Court of Appeals confirms Cisco Systems can face liability for providing surveillance technology used to facilitate human rights abuses against the Falun Gong community. The case is being appealed to the US Supreme Court.

- **Nexa Technologies (formerly Amesys) – Libya:** In 2021, the French Court of Appeal confirms indictment of Amesys and its executives for complicity of torture in Libya in relation to sales to the Libyan Gaddafi regime.

Heightened human rights due diligence for high-risk surveillance technologies

Outlining minimum standards for companies that sell these technologies

In order to effectively identify and mitigate problematic behaviour, active corporate engagement from investors is essential. This section is designed to strengthen your understanding of what rights-respecting corporate conduct should look like, and how to evaluate whether a company's policies, practices and decision making align with your own responsible investment commitments. It will equip you with:

- Targeted questions to assess how companies that sell high-risk technologies manage human rights risks
- Examples of what companies should have in place in order to mitigate human rights risks

Key questions companies should be able to answer regarding high-risk surveillance technologies

= Priority questions

Policies, commitments and governance

- Does your human rights policy explicitly reference the need to respect both international human rights law (IHRL) and international humanitarian law (IHL), including by implementing safeguards that prevent abuse in conflict zones? Does it explicitly address a commitment to mitigate the risk of misuse for civic repression, civilian harm, political surveillance and targeting journalists or activists?
- Who has final authority to approve or reject a sale based on human rights/IHL risk, and how is this authority operationally independent from commercial incentives?
- How do you publicly report on policy implementation, including metrics on misuse, denied sales or contract terminations?
- How do you engage with key stakeholders (human rights NGOs, academia, potentially affected groups, diaspora communities of conflict affected areas) in designing policies or safeguards? Do you have a rightsholder engagement program that was co-designed with civil society to maximise its impact?
- What internal mechanisms exist for employees and contractors to raise human rights concerns without fear of retaliation? Is there a zero-tolerance policy for threats, intimidation, or retaliation on those raising human rights concerns?

- How do you assess and disclose human rights and conflict-related risks to investors and shareholders?
  - When there is the possibility of your products being used in a conflict affected area, does your conflict sensitivity analysis demonstrate that business operations do not violate or contribute to violations of IHL and/or sanctions or trade restrictions regimes and ensure that business operations do not have adverse impacts on the conflict itself?
- Does the company commit to carry out human rights due diligence throughout the product lifecycle – including design, development, deployment, and end-use? Is this commitment coming from the highest level of management?
- Has the company committed to cease, prevent and remediate any human rights impacts the company causes or contributes to?

Identifying, assessing and mitigating human rights risk

- Have you identified and disclosed your most salient human rights risks in specific geographies and highlighting the most at risks rightsholders? What are they?
- Given that selling exclusively to democracies is not a safeguard against abuse, what criteria do you use to pre-screen government and private sector clients to prevent abuse of high-risk technologies? (see Freedom on the Net or Freedom in the World reports)
- What is your approach to continuously screening clients over time, particularly in light of the rising tide of authoritarianism and the fact that current government customers screened in the past no longer abide by the same human rights norms as previous administrations?
- What mechanisms are in place to prevent the resale, diversion or repurposing of hardware or software to illicit actors?
- How do you handle requests from high-risk states, agencies or private sector clients known for repressing civic freedoms? Have you ever refused to sell to a client due to human rights concerns? Do you maintain a list of clients to whom you will not sell?
- Do you include contractual clauses allowing you to suspend service or revoke licences if misuse is identified? Have you ever exercised such a clause, and if so, when?
- How are employees and contractors trained to recognise product misuse?
- Has the company carried out heightened HRDD when their products will be used in a conflict zone or in settings where violence and use of force will be deployed?

Building proportionality into product design

- Do you conduct scenario planning or red teaming to anticipate misuse?
- What technical safeguards (e.g. including privacy-by-design and security-by-design measures, geofencing, audit logs, kill switches) are built into your technology to prevent or limit misuse? Can your company suspend, revoke or deactivate technology if it is misused?
- How does your product design incorporate IHRL and IHL principles, including:
  - How do you ensure that the tool is deployed only when strictly necessary for a legitimate aim for the benefit of society and only when no less intrusive alternative could achieve the same purpose? Does the tool support the user with a proportionality analysis?

- Are there any technical features specifically designed to minimise privacy intrusion (i.e. data minimisation and purpose limitation) so that it is proportionate to the legitimate aims?
- How is the tool designed so that its use respects the principles of distinction and precautions, and avoids indiscriminate effects on civilians in situations of conflict?

- Where is the extracted data stored and for how long? How is it protected from unauthorised access or misuse?
- How is the product designed to explicitly ensure accountability, from a technical perspective, if it is misused?
- Have you performed a human rights impact assessment (HRIA) on each product prior to launch? Have you communicated the findings with relevant stakeholders?
- Have impacted groups, or their legitimate representatives, been consulted in the HRIA exercise? How have their inputs been implemented into product design changes?

Ongoing human rights due diligence

- To what extent do you actively implement projects, provide technical support or upgrade the products or systems on behalf of governments or clients?
- How do you monitor end user compliance (using both technical and non-technical means) with contractual terms prohibiting misuse?
  - For example: What do the terms of service say with regard to control and access of the extracted data? How much oversight does the company have over situations of potential abuse?
  - For example: Do you require government clients to designate an officer responsible for upholding human rights/IHL compliance?
- How do you go beyond compliance with export controls and sanctions (e.g. Wassenaar Arrangement, EU Dual-Use Regulation) to operate with respect to IHRL and IHL regardless of geopolitical alliances?
- Are you open to independent monitoring/assessment of your policies, procedures and grievance mechanisms to ensure their efficacy?
- Do you have a publicly available grievance mechanism for individuals or groups who believe they've been harmed by your technology, providing a feedback loop into your due diligence practices?

Accountability and remediation for actual harms

- How do you ensure that the grievance mechanism is legitimate, accessible, predictable, transparent and rights compatible?
- Does your grievance mechanism include procedures for addressing harms in conflict-affected or high-risk areas?
- What steps do you take to remediate or mitigate harm once you identify misuse of your technology? Can you share examples of when you have taken corrective action after discovering misuse?
- Do you cooperate with independent investigations by UN bodies, NGOs or authorities when credible IHRL or IHL violations are suspected?
- How do you communicate remediation actions to affected stakeholders?

Examples of how companies can demonstrate that they are mitigating human rights risks

Policies, commitments and governance

MODERATE RISK

- The company has a publicly available **human rights policy**, aligned with the UNGPs, explicitly committing to mitigate surveillance-related risks (e.g. misuse for civic repression, political targeting or journalist surveillance). The company recognises that its products may be used in armed conflict and includes general reference to international humanitarian law (IHL) in its human rights policy.
- The company has a **regularly updated and publicly available due diligence framework** that addresses how the company mitigates upstream and downstream salient human rights issues and prevents violations in international human rights and humanitarian law.
- The company has a **dedicated Chief Human Rights Officer** (CHRO) or equivalent, who reports directly to the CEO and has authority over client approvals and contract termination.
- The company has a **dedicated human rights committee** that: is independent from sales and operations; monitors, enforces and reports on policy implementation; is empowered to veto or terminate contracts based on risk findings; comprises senior level officials and IHL experts; reports directly to senior management and the board.
- The company **publicly commits to suspending or withdrawing services** where credible evidence of product misuse is identified.
- The company **co-designs policies and governance frameworks** with civil society and academia.
- Senior leadership and members of the board participate in **industry/multi-stakeholder efforts** to develop and implement voluntary and/or regulatory standards for "lawful interception" technologies.
- The company **does not have a history or pattern of malicious or misleading statements** made to internal and external stakeholders, including the media.

HIGH RISK

- The company has a human rights policy, but it is **not publicly available or lacks specificity** regarding surveillance-related misuse. The company has no explicit mention of IHL in its policies. It relies entirely on clients' claims of "lawful use".
- The company has a due diligence framework, but it is internally focused, not publicly updated or does not address risks across the entire value chain.
- Responsibility for human rights is **spread across legal or compliance teams**, with no single accountable officer; CHRO may exist but **does not have enforcement authority**.
- A human rights committee may exist but it **cannot enforce contract suspension** or veto decisions.
- Suspension or withdrawal is **limited to extreme cases** (e.g. involving war crimes or crimes against humanity) and not publicly committed; decisions may be discretionary.
- Consultation with civil society or academia is **occasional or ad hoc**, not integrated into formal policy design or procedural improvements.
- Participation in multi-stakeholder efforts by senior leadership is criticised as being **perfunctory** and does not inform internal policy or product design.
- The company has **overly defensive statements** that aim to discredit whistleblowers, activists and journalists that raise legitimate concerns rather than disproving the claims themselves.

EXTREME RISK

- The company **has no formal human rights policy**, or any existing statements are vague, aspirational, or limited to "lawful use".
- The company **lacks a structured due diligence framework** and does not systematically identify or address human rights risks.
- No dedicated human rights officer exists; decisions are controlled by **sales or government relations teams**, often with commercial incentives outweighing rights considerations.
- No independent human rights committee exists; human rights risk is **not monitored or acted upon**, and contract approvals ignore rights considerations.
- The company has **no commitment to stop misuse** and there is no policy preventing the continued servicing of clients even if credible reports of abuse exist.
- No meaningful engagement with civil society occurs; policy decisions are made entirely internally without external or expert input.
- Leadership **does not participate in industry or standards-setting efforts**, and may actively resist or dismiss human rights standards.
- The company **has a record of deceptive communications**, denying abuses or misrepresenting product uses publicly, even when there is credible evidence to the contrary.

Identifying, assessing and mitigating human rights risk

MODERATE RISK

- Senior leadership and the board are **regularly trained on how to identify/mitigate human rights risks and understand the core fundamentals of IHL**.
- All employees and contractors receive **mandatory human rights training**, specifically on how to identify misuse of "lawful interception technologies".
- The company has a **customer due diligence programme** to prevent the sale of its products/services to those that: have a documented history of targeting activists, journalists or political opposition; operate in states that lack credible judicial or parliamentary oversight; or are actively sanctioned or on UN human rights sanctions lists. Mitigating risks of IHL violations is a critical element of customer screenings.
- The **human rights unit regularly gathers information** about the potential or actual misuse of the company's products and services through research and consultation with civil society organisations.
- The company hires credible external experts and works with actual or potentially impacted rightsholders to **regularly conduct human rights impact assessments (HRIA)**, publishes the findings, and uses those findings to take preventative/mitigatory action.
- The company includes **contractual clauses** that require the rights-respecting use of technology by customers and outlines legal pathways towards attribution and accountability by rights-violating customers. Contracts include the ability for the company to audit usage logs, revoke software licences and collect hardware.
- The company conducts enhanced pre-sale and post-sale due diligence to **prevent reselling or diversion/repurposing of hardware or software** to illicit or unauthorised actors. The company is aware of when the technology is transferred from private to government clients. It employs traceable serial registration, secure key management and contractual prohibitions on transfer or modification of products without prior approval.
- The company has a **whistleblower portal, available in all languages needed according to where its tools are being deployed**, allows anonymous reporting from internal and external stakeholders and can demonstrate they have adequate policies and procedures for handling reports, including protection from retaliation.

HIGH RISK

- Leadership receives **only occasional or generic compliance training**, with minimal focus on human rights, IHL or surveillance misuse.
- Employees receive **general compliance training** with limited or optional coverage of human rights and misuse scenarios.
- Customer due diligence is **limited to basic checks**, such as sanctions lists or export controls, or "we only sell to democracies", without assessing historical misuse, procedural safeguards for vulnerable groups, or the actual human rights context. The company does not perform conflict or IHL risk assessments when entering or maintaining contracts with clients in or near armed conflict zones.
- Monitoring of misuse occurs **internally only**, with limited or reactive consultation with civil society or NGOs.
- HRIAs are **occasional, internal or confidential**; findings are rarely published, and follow-up action is inconsistent.
- Contracts contain **standard compliance or export control clauses**, but language around enforcement mechanisms (audits, revocation, hardware retrieval) is weak or non-existent.
- The company performs **basic customer due diligence** before sale but lacks systematic post-sale monitoring to detect or prevent resale or diversion. Traceability measures are partial or inconsistently applied. Contractual restrictions exist but are not routinely enforced or audited.
- Whistleblower channels exist **internally only**, are not multilingual, or have limited visibility to external stakeholders. Handling procedures are unclear or inconsistent, and there is disparate evidence that the mechanism has effectively resolved cases.

EXTREME RISK

- Leadership receives **no training** on human rights risk or misuse of surveillance technologies and they are unaware of IHL and conflict-related risks linked to their business operations.
- No employee or contractor training exists on human rights or misuse; staff are only trained on technical or commercial aspects.
- The company **sells to any government or client** without assessing human rights risks, including abusive regimes or sanctioned entities. The company only withdraws clients from the list after continued civil society pressure. The company knowingly provides tools to parties engaged in armed conflict without regard for IHL compliance.
- No monitoring or consultation with relevant rightsholders occurs; the company **ignores or dismisses evidence** of misuse.
- No HRIAs are conducted; the company does **not adequately consider the impact** of its products on affected groups.
- Contracts **lack restrictions** on misuse; there is no ability to audit, suspend, or terminate usage even if abuse is detected.
- The company **does not conduct due diligence to verify end users or detect diversion or repurposing**. Hardware or software can be freely resold, transferred, or modified without oversight. No tracking or approval mechanisms exist, and the company lacks visibility or control over where or how its products are ultimately used.
- **No whistleblower mechanism exists** or there is no evidence that the mechanism has effectively resolved any cases.

Building proportionality into product design

MODERATE RISK

- **The product has not been accused** by leading human rights bodies and experts, such as UN Special Rapporteurs, **of being fundamentally incompatible with international human rights law.**
- The **company regularly tests and modifies its products/ services** to prevent/mitigate vulnerabilities to rights-violating behaviour, and can provide evidence of having done so in consultation with a diversity of rightsholders. For example, there is documentation showing that a substantive amount of HRIA recommendations were implemented.
- There is a **clear requirement to distinguish between military and civilian data** and there are technical safeguards to prevent use of systems for indiscriminate surveillance in conflict areas.
- **Legal authorisation for each specific use of the tool must be documented and verified** before technical access to the system is granted, with documentation retained for audit purposes.
- The product requires that **operators must demonstrate that all other lawful and less intrusive means of achieving the intended democratic objective were exhausted** before seeking technical access to the system.
- The company ensures that its products **only collect data directly relevant and strictly necessary** to the investigation of the specific crime in question.
- The company **builds in technical safeguards** (such as kill switches, audit logs, digital footprints, role-based access controls, data minimisation, retention limits) designed to monitor, inspect and govern the use of its technology by customers, disable the technology when misused and ensure that attribution by rights-violating customers is possible.
- **Technical staff regularly participate in multi-stakeholder initiatives** that prioritise human rights by design.

HIGH RISK

- The company performs internal technical testing for functionality and security, but not specifically for human rights or misuse risks. **Rights holder consultations are overly selective or ad hoc.**
- There is **no requirement to distinguish between military and civilian data** or to prevent use of systems for indiscriminate surveillance in conflict areas. Products lack design features that restrict use in conflict or occupation zones. No geofencing, access control, or context-based triggers exist to prevent targeting of civilians or humanitarian actors. The company provides system customisation for security forces operating in hostilities without rights-based limitations.
- Legal authorisation is **verified by the client**, but there is no safeguarding of the documentation (for transparency and accountability) by design.
- Operators are required to **justify access in general terms**, but proportionality and necessity assessments are not documented or reviewed.
- Products are designed with some data limitation features, but in practice they **may collect more data than necessary**, without automatic filtering or deletion.
- Some safeguards exist (e.g. audit logs or access controls), but they are not comprehensive, cannot be externally verified, lack enforcement (e.g. kill switch rarely used), or can be easily bypassed/disabled by clients.
- **Technical staff rarely participate in multi-stakeholder initiatives or engage with civil society directly** on human rights-centred design.

EXTREME RISK

- **There is no evidence that product design accounts for misuse scenarios or rights-based vulnerabilities.**
- The company **designs or modifies its technology specifically to enhance indiscriminate surveillance or targeting capabilities** in armed conflict. The company knowingly removes safeguards at the client's request. Products may integrate with weapons systems or intelligence platforms used for kinetic strikes. There are no controls to prevent use against civilians, journalists or aid workers.
- No legal authorisation is required for access; the company **leaves legality entirely to the client's discretion**, regardless of due process or oversight.
- No requirement exists for operators to justify access; **no proportionality or necessity checks** are in place before system use.
- Products are designed for **broad or indiscriminate collection**; there are no technical or procedural limits on data scope.
- No technical safeguards are built in; customers have **unrestricted access**, there is **no oversight or audit trail**, and misuse **cannot be detected or reversed**.
- **Technical staff do not participate in multi-stakeholder initiatives or engage with civil society** on human rights-centred design.

Ongoing human rights due diligence

MODERATE RISK

- The company is able to demonstrate **monitoring and auditing procedures** for end user compliance with the human rights policy. Governments must be required to name an individual responsible for upholding the rule of law and human rights in product use.
- The company has a **heightened human rights due diligence programme** that specifically aims to mitigate conflict-related risk, consistent with the OECD Due Diligence Guidance for Responsible Business Conduct and the UNGPs.
- **Technical staff ask tailored questions regarding product use** and the implementation of human rights safeguards when carrying out routine service checks or upgrades.
- The company **distributes informational materials to client employees** to raise awareness about the human rights policy and the grievance mechanism. The company requires that any government officers who will be using the technology must be trained on human rights.
- The company has a **rightsholder engagement programme** that was co-designed with civil society in order to effectively carry out ongoing human rights due diligence within the jurisdictions in which it operates. The programme includes engagement with local rights holders, and is managed in a way that fosters regular exchange, responsive action and security for those consulted. For conflict-affected and high-risk areas, humanitarian organisations and the diaspora community are regularly consulted.
- The company **maintains a log of clients that are no longer able to utilise their products or services** due to human rights concerns.

HIGH RISK

- The company performs **occasional or informal reviews** of client use but lacks structured monitoring. Government clients are **not required** to designate a human rights compliance officer.
- The **company occasionally reviews clients operating in conflict-affected areas** but lacks a systematic conflict-sensitive due diligence process. Monitoring focuses on reputational risk, not IHL compliance.
- Service checks focus on **technical performance only**, with **limited or no reference to human rights safeguards**.
- The company provides **some general compliance materials** to clients but **does not ensure** that deployers receive training on human rights.
- The company engages with civil society **sporadically** or only with organisations operating at the global level, not within specific jurisdictions in which its technology is deployed. Engagement may be **reactive** rather than continuous. Engagement with humanitarian organisations or conflict experts is limited.
- The company has **informal records** of contract terminations but **does not track** them systematically, and there is no mechanism to prevent re-engagement with terminated clients.

EXTREME RISK

- The company conducts **no monitoring or auditing** of client use. There are **no accountability requirements** for government users, and oversight ends after the sale.
- The company conducts **no IHL-specific monitoring or auditing**. There is no mechanism to verify that clients' use of technology in conflict respects distinction, proportionality, or military necessity principles. The company deliberately avoids oversight of clients in conflict zones to maintain plausible deniability.
- Staff are **instructed not to inquire** into client use or implementation practices, actively **ignoring potential misuse** during maintenance or upgrades.
- No training or informational materials are provided; the company **takes no responsibility** for how clients use the technology or understand human rights responsibilities.
- The company **does not engage with civil society or rights holders** at all and operates without external input or consultation in any jurisdiction.
- The company **lacks an internal exclusion list** or centralised register to prevent sales teams from re-engaging with clients or regions previously identified as high risk for human rights abuses.

Accountability and remediation for actual harms

MODERATE RISK	• The **grievance mechanism has been meaningfully audited by an independent third party to determine that it is safe, legitimate, transparent, predictable and accessible** to all those that may have a link to the company's business operations, including impacted rights holders. The mechanism includes escalation channels, protection from retaliation, and feedback loops that inform due diligence practices. • The company has a **specialised investigation and remediation protocol** for grievances arising in conflict-affected or high-risk areas, aligned with the UNGPs and IHL principles. The mechanism includes context-specific procedures for safe and confidential engagement with victims and rights holders, even in insecure environments.	• The company **publishes a disaggregated and anonymised list of cases** received through the grievance mechanism and a clear explanation of changes made to address credible claims raised. • The company **publishes examples of how it has provided access to remedy**, consistent with victims' definition of harm, for those who have had their rights violated as a result of their product/service being abused. • The company **cooperates fully, proactively, and in good faith** with judicial, parliamentary, or regulatory investigations into technology misuse. It provides necessary documentation (e.g. contracts, audit logs) for ensuring access to justice. • The company has a zero tolerance policy for retaliation and **does not engage in retaliatory statements or actions** against actors who critique the company or its staff, products and services.
HIGH RISK	• A grievance channel exists but **has not undergone independent review or validation**. Accessibility is limited (e.g. only in certain languages or regions or scope). Reports are handled with limited transparency or follow-up. • The grievance mechanism **does not explicitly cover harms linked to armed conflict**. There is no clear protocol for cooperating with humanitarian investigations or UN fact-finding missions related to IHL violations. • **Limited or aggregated summaries** of grievances are disclosed, often without detail on outcomes or lessons learned.	• Some remedial actions (e.g. retraining or contractual amendments) occur but are inconsistent or lack transparency. **Remedies are internally defined without rightsholder participation.** • Cooperation with investigations is **limited, selective or delayed**. The company provides partial documentation. It does not proactively share information with credible accountability bodies or humanitarian actors investigating violations involving its technologies. • **No formal non-retaliation policy exists**, but there is no clear evidence of retaliatory behaviour. Responses to criticism are overly defensive.
EXTREME RISK	• The company **lacks a formal or functioning grievance mechanism**. There are no channels for impacted individuals to raise complaints. • The company **fails to recognise any risks linked to conflict affected and high-risk areas** and has no relevant coordination or remediation policies or procedures. • The company **does not disclose any grievance data**. There is no public evidence of tracking, resolution, or systemic learning from complaints. • There are **no examples of where the company has provided remedy** to victims when credible misuse of its technology has been identified.	• The company **refuses to cooperate with judicial, parliamentary and regulatory investigations** or obstructs accountability processes, for example, by providing contradictory statements. It withholds or destroys evidence relevant to potential misuse. The company actively obstructs accountability for IHL violations, including by withholding data relevant to war crimes investigations. • The company **has engaged in retaliatory actions** or statements against civil society, journalists, or internal whistleblowers.It publicly discredits or threatens critics. Examples include threatening or filing defamation suits, monitoring or surveilling civil society organisations.

This table is adapted from "Navigating the surveillance technology ecosystem: A human rights due diligence guide for investors" (March 2022), which was a joint initiative between Heartland Initiative, the Business and Human Rights Centre, Access Now, Gulf Centre for Human Rights, R3D, Agentura.ru and Paradigm Initiative.

Companies that have been mentioned throughout this guide

Below is a non-exhaustive list of companies that have sold these technologies. We include this list in order for investors to conduct any appropriate human rights due diligence. Inclusion on this list is not of itself intended to suggest that a company has committed any human rights abuses. The Centre wrote to each of the companies listed below and includes the responses received here.

The landscape of surveillance technology companies is constantly evolving, with new players emerging and existing ones rapidly adapting. Please feel free to contact us for the most up-to-date information and insights.

Spyware

- FlexiSPY
- Intellexa Consortium (Nexa Technologies, Passitora (formerly WiSpear), Cytrox and Senpai Technologies)
- Memento Labs (formerly Hacking Team)
- NSO Group
- REDLattice (formerly Paragon Solutions)
- Saito Tech (formerly Candiru)

Spyware companies that have reportedly shut down, but whose IP may have been repurposed:

- eSurv
- FinFisher
- QuaDream
- Variston

Digital forensics

- Cellebrite (which acquired BlackBag Technologies)
- Cognyte Software
- Micro Systemation AB (MSAB)

Cell site simulators

- L3 Harris Technologies
- PicSix

Deep packet inspection

- AppLogic Networks (formerly Sandvine)
- Cisco Systems
- Geedge Networks
- Nexa Technologies (formerly Amesys)

For more information, contact: techaccountability@business-humanrights.org

Authors and researchers:

- **Aparna Surendra** and **Esme Harrington**, AWO
- **Meredith Veit**, Business & Human Rights Centre
- **Ragheb Ghandour**, Cyber Security Technologist, SMEX

Thank you to all the contributors whose expertise has made this guide possible:

- **Andrei Romanov**, Secura.Team
- **Jack Parham**, FIND.ngo
- **Jennifer Brody**, Freedom House
- **Esra'a Al Shafei**, Surveillance Watch
- **Jonathan Rozen**, Committee to Protect Journalists (CPJ)
- **Siena Anstis**, The Citizen Lab
- **Mallory Miller**, Heartland Initiative
- **Rand Hammoud**, Access Now
- **Diana Kearney**, **Hana Ivanhoe** and **Caroline Brodeur**, Oxfam

We gratefully acknowledge the **Spyware Accountability Intiative** for making this guide possible. Special thanks to Rand Hammoud for her critical role in sparking the development of this comparative analysis.