This guide is a product of the Surveillance Technologies Accountability Project, a joint initiative of **Access Now**, **Business & Human Rights Resource Centre**, and **Heartland Initiative**

Navigating the surveillance technology ecosystem:

A human rights due diligence guide for investors

MARCH 2022

Summary

Why now?

As the information and communication technology (ICT) industry rapidly expands, it has the power to support democratic, accountable institutions and the exercise of civic freedoms or perpetuate violations of individual and collective rights. As described by the UN Human Rights Council's 2020 report, new technologies can enable individuals in exercising their rights and in recent years have been used to organize social movements, document abuses, and ensure access to education during the COVID-19 pandemic. However, as UN representatives,[1] digital rights organizations, and state governments attest, certain new technologies - particularly those with surveillance capabilities - are being used to violate an array of human rights.

Navigating the surveillance technology ecosystem: A human rights due diligence guide for investors (the Guide) focuses specifically on the surveillance technologies industry because it represents the most intrusive and pervasive means for systemic invasion of privacy, leads to direct violence against individuals, and perpetuates discrimination against marginalized communities. The purpose of the Guide is to assist investors in conducting human rights due diligence (HRDD)[2] of cyber-security and surveillance technology companies in order to protect their investments, fulfill their responsibilities under the UN Guiding Principles on Business and Human Rights (UNGPs), and ensure emerging technologies are used to support human rights and democratic freedoms around the world.

What is this guide?

"Navigating the surveillance technology ecosystem: A human rights due diligence guide for investors" is a comprehensive resource designed for institutional investors of all sizes, types, and geographies. It is intended to be used by asset owners and asset managers to evaluate purchasing or holding shares in companies with activities or investments in the surveillance technology ecosystem.

Grounded in the perspectives of digital rights advocates, due diligence modeling experts, and investors, this Guide draws on learnings from a series of virtual workshops as well as individual interviews and desk research. The Guide seeks to assist investors to navigate the surveillance technology ecosystem by providing definitions, examples of current and evolving risks, and guideposts to be used in fulfilling their human rights and fiduciary responsibilities. Specifically, it provides: (a) an examination of how surveillance technologies create human rights risks for individuals and communities; (b) an explanation of material risks for investors; (c) questions to identify severity of risk; and (d) a framework for investment decision-making. While developed for institutional investors, the Guide will also be useful for other stakeholders, including civil society organizations, companies, and policymakers.

The key HRDD steps are organized in three areas for investors to consider through the use of targeted questions:

- **Governance, Policy & Practice** refers to the role, composition, culture, and special units (e.g., human rights committee) of the company's board of directors and senior staff as well as the preventative and mitigatory policies and practices the company has in place to identify, assess, and address human rights harms.
- **Product Life Cycle** considers the ways in which a company's "design & development," "promotion, deployment & sale," and "licensing & use" either make its products or services vulnerable to rights-violating behavior by end users or enable the company to prevent and/or mitigate human rights harms in its value chain.
- **Remedy** examines the policies and practices the company has in place to provide access to remedy for individual(s) adversely impacted by the use of its product or service.

The final section of the Guide assists investors in applying the findings from their evaluative process through a tiered risk management framework. While decisions ultimately rest with investors, the evaluative criteria provided can help them identify the varying levels of risk associated with each company based on answers to the Guide's questions.

The Guide is a product of the Surveillance Technologies Accountability Project, a joint initiative of Access Now, Business & Human Rights Resource Centre (the Resource Centre), and Heartland Initiative. Over the last two years, project partners worked with Agentura.ru, Gulf Centre for Human Rights, Paradigm Initiative, and R3D to deliver three virtual workshops and support the development of the Guide. The workshops brought investors and civil society stakeholders together for frank sharing of perspectives, challenges, and ways forward on ensuring business respect for human rights within the surveillance technology ecosystem.

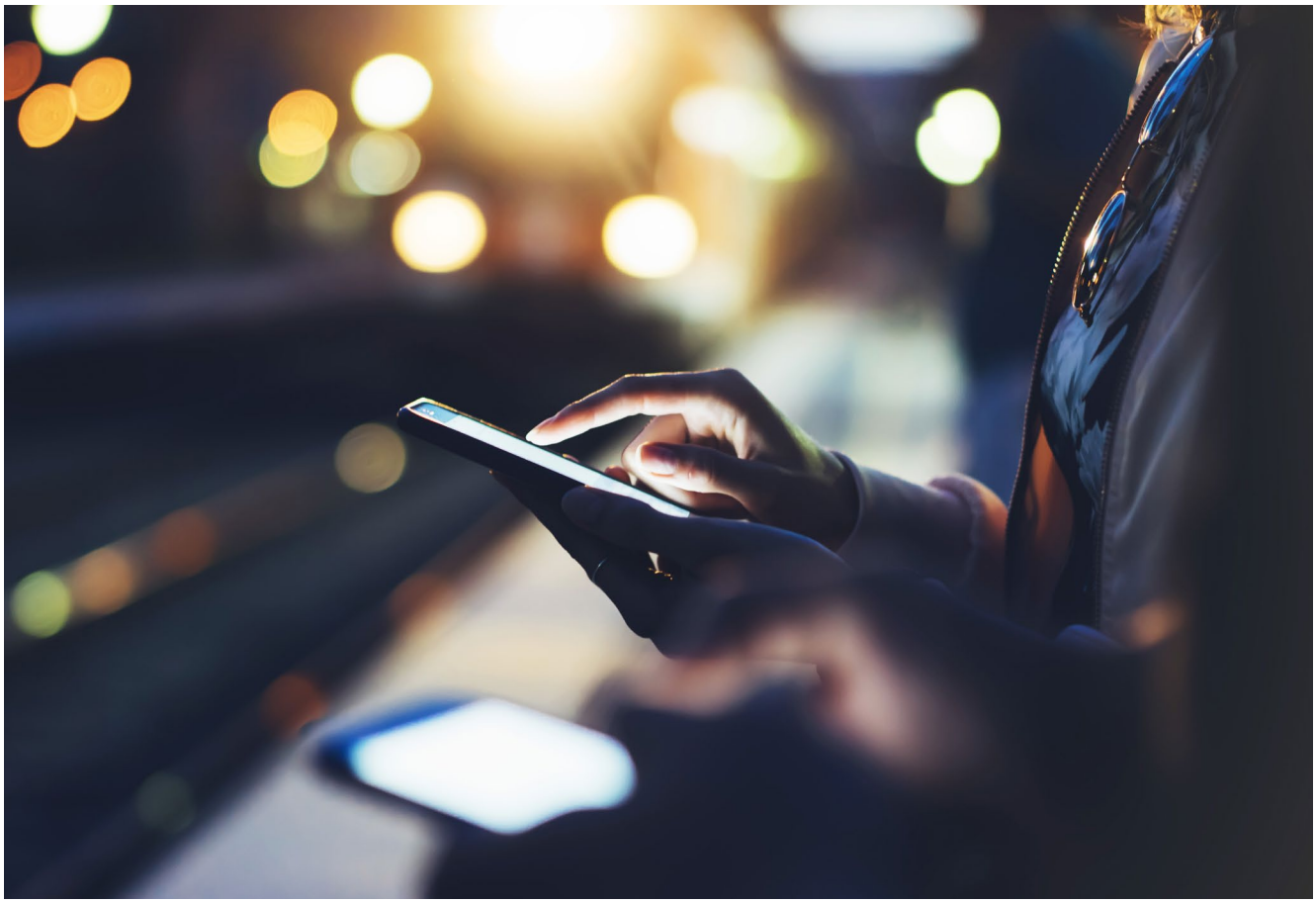
Contents

Introduction

Cyber-surveillance (surveillance) technologies are fundamentally reshaping our societies. New revelations of how these products and services impact our individual and collective lives appear daily, from spyware targeting journalists, lawyers, human rights defenders, diplomats, and world leaders to facial recognition software being inherently biased against communities of color. While certain technologies within the surveillance sector may serve legitimate national security and public safety purposes, the global surveillance industry is affecting peoples' fundamental rights in unprecedented ways.

These technologies have proliferated thanks to their relatively low cost, broad accessibility, and limited regulation. In turn, this has created challenges for both public and private stakeholders in holding accountable rights-violators and the companies that enable them. Such challenges have been amplified as states and companies raced to adapt surveillance technologies to stop the spread of COVID-19 without policies and guardrails to ensure sufficient consideration of human rights.

Digital rights organizations, journalists, and policymakers are sounding the alarm concerning the ways in which surveillance technologies are used to violate an array of human rights, from privacy to life itself. Investors increasingly recognize that the human rights risks to individuals and communities associated with these technologies represent a material risk to their portfolios and they have an ethical, normative, and fiduciary responsibility to address them. This Guide is designed to help investors better identify, assess, prevent, and mitigate risks throughout the surveillance technology ecosystem.



What are surveillance technologies and how do they impact human rights?

The absence of a universal or even generally accepted definition of the term "surveillance technologies" among stakeholders is a central challenge to effective regulation and accountability. Governments, companies, and civil society are perpetually trying to catch up to these technologies, as well as the companies that produce them, given their ever-evolving technological sophistication and accessibility to state and non-state actors. In the absence of a universal definition for surveillance technologies, the Guide adopts the European Commission's widely-accepted version, which describes them as ICT goods, services, and technologies that are, "specifically designed, in whole or in part, for surveillance purposes."

These technologies can either be used for targeted (e.g., spyware) or mass surveillance (e.g., biometric recognition software, deep packet inspection, IMSI Capture Devices). As with the overarching definition of surveillance technologies, a global consensus for differentiating between mass and targeted surveillance remains elusive and often depends on how a particular technology is used and the type of information that is gathered. Drawing from current legislation and leading digital rights organizations, the Guide uses the following definitions:

- **Targeted surveillance** is directed at particular individuals. It can be carried out overtly or covertly. Targeting methods include the interception of communications (e.g., spyware), the use of communications "traffic" data, visual surveillance devices, and devices that sense movement, objects, or persons.[3]

- **Mass surveillance** is indiscriminate and uses systems or technologies to collect, analyze, store, and/or generate data on indefinite or large numbers of people instead of limiting surveillance to individuals about which there is reasonable suspicion of wrongdoing. Governments can capture virtually all aspects of our lives with existing forms of mass surveillance.[4]

The Guide is intended to be used by investors who are considering purchasing shares in companies that fall into one or more of the following categories:

- Companies exclusively engaging in the production and/or sale of one or more surveillance technologies or services (e.g., NSO Group, Gamma).

- Companies providing a range of goods, services, and technologies that include, but are not limited to, surveillance technologies (e.g., Alphabet, Amazon).

- Companies producing goods, services, and technologies that can be used for both surveillance and non-surveillance purposes (e.g., Sandvine).

Surveillance technologies have both subtle and profound impacts on human rights. They are being used to gradually erode norms around individual privacy and trust between citizens and their governments; enable the growing illiberalism and autocratization of certain states; promote censorship of media outlets and human rights defenders; facilitate the surveillance, detention, and forced labor of hundreds of thousands of members of an ethnic minority; reinforce discrimination; and have led to the kidnapping and killing of political dissidents by repressive regimes.

The former UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, David Kaye, highlighted that targeted surveillance has been shown to lead to arbitrary detention, torture, and/or extrajudicial killings. In 2019, he called for an **immediate moratorium** on the global sale and transfer of surveillance technologies until human rights safeguards are in place to regulate their sale and use.[5] Relatedly, in September 2021, the UN High Commissioner for Human Rights, Michelle Bachelet, urged states to impose a moratorium on the use of remote biometric recognition technologies in public spaces until sufficient privacy and data protection regulations are enforced.

Though not exhaustive, the Guide provides users with a list of salient human rights issues associated with certain targeted and mass surveillance technologies, which must be identified, assessed, and addressed. (See Annex 1: Table of Salient Human Rights Issues.)

Why should investors care about surveillance technologies?

As shareholders in companies with activities or investments in the surveillance technology ecosystem, investors have a critical role to play in promoting human rights and helping to uphold the UN Guiding Principles on Business and Human Rights (UNGPs). Under this framework, and as described by the Investor Alliance for Human Rights, investors have a responsibility to respect human rights as adverse impacts may be "caused by, contributed to, or linked to portfolio companies."[6] In order to fulfill their responsibility, investors must publish a policy commitment, have due diligence processes, and enable or provide access to remedy to impacted rights holders.[7]

In addition to their responsibilities under the UNGPs, investors have a fiduciary duty to their clients, which has evolved to include environmental, social, and governance (ESG) criteria as key indicators of a company's long-term value and performance.[8] The concept of "double" or "dynamic" materiality holds that adverse ESG impacts (including human rights) present material legal, operational, and financial risks that can undermine portfolio companies' profitability.[9]

There is perhaps no better example of the ways in which human rights risks translate into material risks (or create double materiality) than the surveillance technology industry, specifically the business activities and global impact of the NSO Group (NSO). (See Annex 2: NSO Group Case Study.)

There are numerous other examples of material risks associated with the human rights harms enabled by the surveillance technology ecosystem, including but not limited to:

- **Litigation** presents legal and financial risks as lawsuits can impose burdensome awards of financial damages, limitations on company operations, and/or excessive legal fees. Surveillance technology companies may see claims from affected rights-holders and other technology companies implicated in rights-violating conduct. For example, rights-holders around the United States have brought a consolidated lawsuit against facial recognition software company Clearview AI for its extraction of faceprints from people without their consent in violation of Illinois state law. Similarly, WhatsApp filed suit in October 2019 against NSO alleging it used WhatsApp's servers to hack 1,400 user devices. In November 2021, NSO was also sued by Apple for similar conduct and to "curb the abuse of state sponsored spyware."

- **Regulatory enforcement** creates legal, reputational, and financial risks, as highlighted by U.S. Presidential executive orders banning investment in certain Chinese surveillance technology companies and the inclusion of NSO, Candiru, and Nexa on the U.S. Department of Commerce's Entity List for Malicious Cyber Activities, Germany's criminal investigation into FinFisher's illegal exports of spyware products, and France's indictment of Amesys and Nexa Technology executives for complicity in torture in Libya and Egypt.

- **Export regimes** present legal and operational risks to investors as they limit when and to whom surveillance companies can sell their products and impose significant financial penalties for violations. Under the new EU Dual-Use regulation, government authorities are required to consider human rights and the history of the end user in granting licenses. Similarly, the U.S. Department of Commerce adopted a new rule that applies comparable license requirements on hacking tools destined for countries of concern for misuse. In December 2021, the Biden Administration announced the Export Controls and Human Rights Initiative in partnership with Australia, Denmark, Norway, Canada, France, the Netherlands, and the United Kingdom, calling for harmonized policies on the export of "key technologies" and including a voluntary code of human rights criteria applied to export licenses. In addition, over the past year more than 3,600 export licenses were revoked by Israel's Defense Ministry over concerns about human rights abuses and political instability.[10]

- **Public pressure** creates reputational and core business risks as experts, advocates, and companies are calling for and/or imposing moratoriums on the sale of these technologies until adequate legal and regulatory safeguards can be implemented. These calls are coming from a range of industry actors and stakeholders, including UN-appointed experts, Amazon self-imposing a moratorium on police use of its facial "Rekognition" software, Microsoft divesting from AnyVision and ending its role in facial recognition, and Facebook shutting down its Face Recognition system.

Investors can be directly and indirectly exposed to these risks throughout their investment portfolios. They face direct human rights and other material risks through investments in companies whose entire or partial product and service line includes surveillance technologies. Investors may also be exposed to risks when their asset managers invest in surveillance technology companies. For example, asset management firm The Blackstone Group has indirect investments (via American private equity firm Francisco Partners) in Sandvine, which has a history of allegations of human rights harms. When invited to respond to allegations that the deep packet inspection technology it produced has been used to facilitate human rights violations by repressive governments, Sandvine shared that its "end user license agreement explicitly prohibits actions that support or enable the commission of individual human rights violations" and that the firm is "deeply committed to ethical business practices."

Key Questions

The questions below are intended to prioritize the key areas on which investors may focus during the HRDD process. They provide a menu of options investors may use based on institutional priorities and the particular company/product in question.

These questions are not intended to be, nor should they be treated as, exhaustive. Further, examples of company policies and practices are included for illustrative purposes only and do not necessarily reflect best practice. Some company examples are taken from other industries as surveillance technology companies' human rights policies and practices generally lag behind other sectors. Finally, due to the complexity of surveillance technologies and their human rights impacts, investors may find it necessary to enlist the support of external subject matter experts.

Governance, Policy & Practice

- Does the company have a **public human rights policy** consistent with the International Bill of Human Rights, UNGPs, UN Declaration on the Rights of Indigenous Peoples, UN Declaration on Human Rights Defenders, and other human rights treaties?
  - Does the policy **identify** all salient upstream and downstream human rights risks (i.e., workplace, supply chain, and end use) associated with its business model and/or the broader industry?
  - Is the policy **widely communicated** among internal and external stakeholders (e.g., via employee manuals, training, publications, grievance mechanisms)?
- Does the board **monitor, enforce, and/or report** on the company's human rights policies and in particular ensure that the company:
  - embeds the **responsibility** to respect human rights into its knowledge and practices?
  - addresses and reports on its salient human rights **risks** and provides for **remedies**?
- Does the board and senior management:
  - proactively **participate** in industry-wide efforts and/or multistakeholder initiatives to address salient human rights issues?
  - internally discuss and **speak or write** publicly about human rights issues associated with the surveillance industry?

- Does the company:
  - have a **commitment to zero tolerance** of intimidation, violence, and criminalization of human rights defenders[11] in its operations and value chain, either in its human rights policy or in a standalone human rights defenders policy, and procedures for implementing this commitment?
  - conduct **human rights impact assessments** (HRIAs) at key stages (e.g., development, deployment, response to harms) that ensure safe, regular, and meaningful stakeholder engagement, including local rights holders and defenders, are grounded in the UNGPs, and publish and discuss the findings regularly?
  - have a reputation for **engaging investors** and taking **risk prevention** and/or **mitigation** measures regarding ESG issues based on stakeholder grievances, investor feedback, and other external findings?
  - have a **human rights unit** or other cross-departmental entity tasked with monitoring, enforcing, and/or reporting on policy and practice implementation?
  - consult with **local rights holders and defenders** to understand the human rights and other impacts of the technology in question in a manner that ensures broad community representation, regular exchange, and protection for consulted rights holders?

Product Life Cycle • Design & Development

- What is the **intended use** of the technology? Specifically, is there a documented history that the type of technology being produced by the company has been used in human rights violations?
- What are the potential **salient human rights issues** associated with the use that the technology is designed for?[12]
- Does the design of the company's technology:
  - incorporate a standard set of **human rights safeguards**, such as flagging systems that detect misuse?
  - include the ability to **disable/shut down** (e.g., via a "kill switch") the technology in the event of misuse or known human rights violations?
  - require an **ongoing relationship** with the end user (e.g., via the provision of updates and tech support)?
  - consider the possible impact of **interconnected products** being misused together?
- Is the technology designed in such a way that its use is intended to go **undetected** by the target(s) of the surveillance?
- How has the technology been **tested** for efficacy and accuracy of intended use, vulnerabilities to modification, and/or risk of unauthorized access to and theft of data?
- Could the technology be used or readily **adapted** for unintended, severely harmful purposes?
- Does the company build in **end-user attribution** to the technology to advance transparency and accountability?

Product Life Cycle • Promotion, Deployment & Sale

- What **percentage** of the company's total revenue or product suite is represented by surveillance technology products and services?
- Does the use of the technology take place in a:
  - state or territory experiencing international armed **conflict**, non-international (internal) armed conflict, and/or a military occupation?
  - state or territory with country-, entity-, or individual-based **sanctions** by the United States, European Union, United Kingdom, Canada, and/or United Nations?
  - state with laws, regulations, policies that contribute to or a documented history of, **restricting civil liberties**, violating the rule of law, and not providing access to justice as detailed by leading international indices?[13,14,15]
  - state or state agency with a documented history of **targeting protected and/or vulnerable populations**, including women and children, LGBTQI+ individuals, ethnic/racial/religious/other minorities, immigrants, asylum seekers, and refugees, human rights defenders, journalists, political dissidents, and civilians in conflict?[16]
- What percentage of the company's **customers** are governments (e.g., law enforcement, immigration enforcement, military) and/or defense contractors?
- Does the structure or duration of the company's relationships, or its role in the surveillance technology value chain, limit the company's **control over the use** of its technology?
- Does the company **prohibit sales to end users** who have a track record of misusing surveillance technologies?

Product Life Cycle • Licensing & Use

- Does the company:
  - have in place a set of **human rights criteria** it uses to evaluate tender processes and requests for proposals in which it participates?
  - ensure the inclusion of **contractual provisions** in the sales contract that renders the contract and any related operational support void if the technology is misused and enables the company to **revoke** its license and/or disable the system?
  - ensure that end users and all members of its value chain **sign commitments** to respect human rights?
  - publicly **disclose its client list** or provide data about the types of clients?
  - vet, monitor, and, if necessary, end contracts with intermediary companies that resell the product/service to **rights-violating end users**?
  - contractually **prevent end users from customizing the product** in a way that increases the risk of human rights harm?
  - contractually require its customers to **provide ongoing reporting** on the use and impacts of the technology?
  - **monitor the use of its technology**, including using internal and external experts?
- Are end users **vetted** by relevant state authorities?
- Are there examples of the technology being **misused** by customers and/or examples of unintended users (e.g., non-state armed actors, private sector offensive actors, criminal organizations) obtaining and using the technology?

Remedy

- Does the company:
  - have a **publicly available policy** describing its approach to identifying, assessing, and, if necessary, administering remedy to impacted individuals or communities?
  - have a process in place for determining instances in which remedy for human rights harms is required for an individual or community and then **delivering remedy** to the impacted party? Are there examples of the company administering such a remedy?
  - have an UNGP-aligned **grievance mechanism** that is safe, effective, and accessible?
  - retain external, **independent experts** for investigating whether rights have been violated through the use of its technology?
  - have processes in place to ensure that it can provide **evidence of harm** and attribution for any harm that is caused?
  - have a track record of **cooperating** with independent investigations by relevant authorities?

Applying Findings

While applying the findings of the HRDD model ultimately rests with each investor, the criteria below that correspond to three levels of risk provide some guidance when making the decision to invest in, engage, or exclude a company in the surveillance technology industry

Governance, Policy & Practice

LOW RISK

Senior leaders/managers and/or board:

- use internal staff and external experts to identify, assess, prevent, and mitigate human rights risks.
- regularly train management and employees to identify/ mitigate human rights risks.
- participate in industry/multi-stakeholder efforts to develop and implement voluntary and/or regulatory standards for surveillance technologies.

The company:

- has a regularly updated policy and corresponding practices that address upstream and downstream salient human rights issues, which has been documented through leading digital rights indices (e.g., Ranking Digital Rights) and public reporting.
- has a human rights unit or other relevant entity that: (a) is organizationally independent from sales or operational teams, (b) monitors, enforces, and reports on policy implementation, (c) is authorized to suspend or terminate contracts based on its findings, and (d) has a direct reporting line to senior management and the board.
- hires credible external experts to regularly conduct HRIAs, publishes the findings, and uses those findings to take preventative/mitigatory action.
- has a whistleblower system allowing anonymous reporting from internal and external stakeholders and relevant policies on who will and how to handle reports.
- consults internal and external stakeholders, including local rights holders, in a way that fosters regular exchange, responsive action, and security for those consulted.
- does not exhibit a history or pattern of malicious or misleading statements made to internal and external stakeholders, including media.
- does not engage in retaliatory statements or actions against actors who critique the company or its staff, products, and services.

MODERATE RISK

Senior leaders/managers and/or board:

- recognize the importance of the human rights due diligence process but do not allocate sufficient resources for implementation
- train management and employees to identify, assess, and mitigate human rights risks but without sufficient regularity, technical depth, or coverage of employees

The company:

- has a global human rights or related policy but lacks a record which shows it is consistent in its efforts to prevent and mitigate its human rights risks.
- has conducted HRIAs but not on a regular basis or has not publicly communicated the results and/or responsive actions.
- consults with internal/external stakeholders but does not take corrective measures.
- does not engage in retaliatory statements or actions against actors who critique the company or its staff, products, and services.
- does not exhibit a pattern of malicious or misleading statements made to internal and external stakeholders, including media.
- does not meet the specific requirements of a “low risk” investment, but there is the likelihood of successful company engagement based on:
  - the presence of a human rights or related policy;
  - the presence of a human rights officer, human rights committee, and/or board member(s) with human rights expertise;
  - public reporting (e.g., Global Network Initiative, UN Global Compact);
  - whistleblowing system; and/or
  - a history of shareholder engagement and/or taking rights-respecting measures.

SEVERE RISK

Senior leaders/managers and/or board:

- do not train management or employees to identify, assess, and mitigate human rights risks
- do not participate in relevant industry/ multi-stakeholder efforts

The company:

- does not have a human rights or related policy or does have such a policy but its products or services continue to be associated with human rights harms.
- does not have a team dedicated exclusively to human rights risks.
- does not respond transparently or substantively to claims of human rights violations.
- engages in retaliatory statements or actions against actors who critique the company or its staff, products, and services.
- exhibits a pattern of malicious or misleading statements made to internal and external stakeholders, including media.

	LOW RISK	MODERATE RISK	SEVERE RISK
Product Life Cycle	**The company:** → regularly tests and modifies its products/services to prevent/mitigate vulnerabilities to rights-violating behavior (e.g., preventing bias in biometric recognition software). → has a customer due diligence program to prevent the sale of its products/services to state or non-state customers in conflict-affected and high-risk areas (CAHRA) and/or who have a record of misusing surveillance technologies to violate human rights. → builds in contractual and technological safeguards designed to monitor, inspect, and govern the use of its technology by customers, disable the technology when misused, and ensure attribution by rights-violating customers. → regularly gathers information about the misuse of products/services through research and consultation with civil society organizations.	**The company:** → has a customer due diligence program in place but lacks certain key elements (e.g., consideration of CAHRA or evidence-based assessment). → regularly conducts product/service testing for accuracy of software but fails to conduct adequate post-sale measures (e.g., customer due diligence, monitoring use). → uses contractual and/or technological safeguards that are limited in terms of their ability to prevent the technology from being customized for rights-violating purposes or shut down the technology when it is alerted to instances of misuse. → is inconsistent in efforts to gather information about the misuse of products/services through desktop research and consultation with civil society organizations.	**The company:** → a substantial percentage of the company's total revenue or total product suite is represented by surveillance technology products and services. → the type of products in question are defense grade and developed/marketed for high-risk applications under export control rules. → the company's product and/or services are being sold and used in multiple CAHRA. → the company's product(s) has a documented track record of being used in rights-violating behavior by state and/or non-state actors , and the company has failed to meaningfully address such violations (e.g., Pegasus Project/NSO – see Annex 2: NSO Group Case Study, Hacking Team). → the type of surveillance technology sold by the company has been banned or recommended for a ban, moratorium, or restrictions by authoritative global institutions or national bar associations (see Annex 3). → the type of product/service at issue or its equivalent is litigated in a court (e.g., NSO) or subject to administrative enforcement by a data protection authority (e.g., Clearview AI). → the company does not put in place contractual and/or technological safeguards to prevent the technology from being customized for rights-violating purposes or shut down the technology when it is alerted to instances of misuse.
Remedy	**The company:** → has a safe and effective grievance mechanism that is accessible to all internal and external stakeholders. → has a track record of addressing human rights risks in its direct operations and value chain by providing access to remedy to adversely impacted rights holders. → ensures its legal and litigation activities do not adversely impact human rights, and instead advances the rule of law and respect for human rights, online and offline.	**The company:** → has a remedy policy but not a record of providing access to remedy for adversely impacted rights holders. → does not sue its critics or malign them in public forums, but does take overly protective legal actions and public stances or ignores legitimate criticism.	**The company:** → does not have a remedy policy. → pursues its critics in court, such as through defamation litigation, or is involved with other types of attacks, and actively ignores or maliciously derides those lodging legitimate claims or criticism.

Acknowledgements

The primary authors of this publication are Sam Jones of Heartland Initiative and Astrid Perry with support from Christen Dobson, Henry Peck, and Danny Rayman of the Business & Human Rights Resource Centre, Isedua Oribhabor and Natalia Krapiva of Access Now, and Mallory Miller and Rich Stazinski of Heartland Initiative.

The authors wish to thank all those who participated in the project workshops and are particularly grateful to the following individuals for their keen insights and significant contributions to the Guide: Nardine Al-Nemr, Lindsey Andersen (BSR), Siena Anstis (Citizen Lab), Likhita Banerji (Amnesty International), Jake Barnett (Wespath Benefits & Investments), Yashaswini Basu, Lauren Compere (Boston Common Asset Management), Daniëlle Essink (Robeco), Luis Fernando Garcia Muñoz (R3D – Red en Defensa de los Derechos Digitales), Mark Hodge (UN B-Tech), Anushka Jain, Emil Lindblad Kernell (Danish Institute for Human Rights), Rachel Nishimoto (Parnassus Investments), Peter Micek (Access Now), Paloma Munoz Quick (BSR), Gbenga Sesan (Paradigm Initiative), Dr. James Shires (Leiden University), Andrei Soldatov (Agentura.ru), Hinako Sugiyama (Access Now), Ioana Tuta (Danish Institute for Human Rights), Marlena Wisniak (European Center for Not-for-Profit Law), Pat Zerega (Mercy Investment Services), and the Gulf Centre for Human Rights.

accessnow

Business & Human Rights Resource Centre

HEARTLAND INITIATIVE

GCHR مركز الخليج لحقوق الإنسان

agentura.ru

PARADIGM INITIATIVE

R3D Red en Defensa de los Derechos Digitales

Annex 1: Table of Salient Human Rights Issues

Category	Salient Human Rights Issues	Examples
Mobile Telecommunications Interception Equipment	Right to Privacy Freedom of Expression Freedom of Association Freedom from Arbitrary Arrest and Detention	Use of IMSI-catchers by police in England and Wales to conduct mass surveillance at protests and large sporting events.
Intrusion Software	Right to Privacy Freedom of Expression Freedom of Association Right to Life Freedom from Arbitrary Arrest and Detention Freedom from Torture, Inhuman Treatment, and Degrading Treatment	The phone of a Canada-based Saudi dissident, Omar Abdulaziz, was infected with NSO's Pegasus in 2018. At the time his phone was infected, Mr. Abdulaziz was in frequent contact with Jamal Khashoggi, the journalist murdered at the Saudi embassy in Istanbul. The two discussed human rights issues in Saudi Arabia, and it is thought that the Saudi Government could have tracked Mr. Khashoggi through the use of the spyware. It led the UN Special Rapporteur on extrajudicial killings to conclude in her report that, "the execution of Mr. Khashoggi has also raised serious concerns about domestic and extraterritorial surveillance of the private communication of individuals whose only 'crime' has been the peaceful expression of their views." NSO Group said its "technology was not associated in any way with the heinous murder of Jamal Khashoggi."
Monitoring Centers	Right to Privacy Freedom of Expression Freedom of Association Right to Life Freedom from Arbitrary Arrest and Detention Freedom from Torture, Inhuman Treatment, and Degrading Treatment	In 2021, four French executives of Amesys and Nexa Technology were indicted for "complicity in acts of torture and forced disappearances and aiding authoritarian regimes in Libya and Egypt in suppressing political opposition." Amesys's Eagle monitoring system was used by the Libyan intelligence service during the Arab Spring to monitor phones, email, and chat conservations of government opponents in Libya and abroad on a massive scale Opponents of Gaddafi's regime experienced multiple forms of harassment by the authorities, including arbitrary arrests and detention as well as torture. In certain cases, victims were shown transcripts of emails and text messages while being tortured Trovicor established and maintained monitoring centers in Bahrain that were allegedly used by the authorities to monitor democratic activists. According to media reports, almost two-dozen political prisoners were beaten, and subsequently interrogated, while being shown transcripts of emails and text messages. Trovicor denied the allegations.

Category	Salient Human Rights Issues	Examples
Lawful Interception and Data Retention Systems	Right to Privacy Freedom of Expression Freedom of Association Right to Life Freedom from Arbitrary Arrest and Detention Freedom from Torture, Inhuman Treatment, and Degrading Treatment	TeliaSonera was criticized for allowing Belarus, Uzbekistan, Azerbaijan, Tajikistan, Georgia, and Kazakhstan to install black boxes in their communications networks. In Georgia, lawyers alleged that the use of a black box violated Georgia's national laws on surveillance powers. TeliaSonera responded by issuing a "freedom of expression policy," which states that it, "advocates that governments should not have direct access to a company's networks and systems."
Biometrics	Right to Privacy Freedom of Expression Freedom from Arbitrary Arrest and Detention Freedom from Torture, Inhuman Treatment, and Degrading Treatment Freedom from Discrimination	A pilot surveillance program, Project Green Light (PGL), was deployed in 2016 through the installation of high-definition cameras throughout the city of Detroit. PGL stations are not distributed equally, with surveillance systems being disproportionately used in majority-Black areas, avoiding White and Asian communities. A further problem is that a growing body of research exposes divergent error rates across demographic groups, with the poorest accuracy consistently found in subjects who are female, Black, and 18-30 years old. In the landmark 2018 "Gender Shades" project, an intersectional approach was applied to assess three gender classification algorithms, including those developed by IBM and Microsoft. Subjects were grouped into four categories: darker-skinned females, darker-skinned males, lighter skinned females, and lighter-skinned males. All three algorithms performed the worst on darker-skinned females, with error rates up to 34 percent higher than for lighter-skinned males. Not only are cameras and facial recognition technology distributed unevenly in Detroit, but the chance of a miscarriage of justice occurring is higher for black communities given the inaccuracies in the recognition software.
Digital Forensics[17]	Right to Privacy Freedom of Expression Freedom of Association Right to Life Freedom from Arbitrary Arrest and Detention	MSAB, a digital forensics company, sold its phone hacking technology to Myanmar police in 2019, two years after the country's security services had been accused of engaging in genocide against the Rohingya minority. While the company cancelled a deal to sell its extraction devices to the Bureau of Special Investigations following the military coup in February 2021, the earlier products remain in the hands of Myanmar's security services and enable the extraction of call, contact, GPS, text messaging, and password records from individual's mobile phones. When asked about the 2019 sale, MSAB said that limited technology was sold to police working for a civilian government and that the licenses were canceled after the 2021 coup.

Category	Salient Human Rights Issues	Examples
Location Tracking Devices	Right to Privacy Freedom of Expression Freedom of Association Right to Life Freedom from Arbitrary Arrest and Detention Freedom from Torture, Inhuman Treatment, and Degrading Treatment	An array of businesses use location tracking devices to monitor employees' movements, which can violate workers' privacy and be used to limit union organizing, including Amazon. Amazon has said that it uses such technology to help keep employees, buildings, and inventory safe and that the technology allows employees to be more efficient in their jobs.
Probes[18]	Right to Privacy Freedom of Expression Freedom of Association Right to Life Freedom from Arbitrary Arrest and Detention	Europe's top rights body has said mass surveillance practices, including the use of probes, are a fundamental threat to human rights and violate the right to privacy enshrined in European law. The parliamentary assembly of the Council of Europe says in a report that it is "deeply concerned" by the "far-reaching, technologically advanced systems" used by the United States and United Kingdom to collect, store, and analyze the data of private citizens. It describes the scale of spying by the U.S. National Security Agency, revealed by Edward Snowden, as "stunning."
Deep Packet Inspection (DPI) Systems	Right to Privacy Freedom of Expression Freedom of Association Right to Life Freedom from Arbitrary Arrest and Detention Freedom from Torture, Inhuman Treatment, and Degrading Treatment Censorship	In 2018, Citizen Lab performed internet scanning and found DPI middleboxes on a Turkish network, which they matched to Sandvine PacketLogic devices. The research found that middleboxes were being used to redirect hundreds of users in Turkey and Syria to nation-state spyware when those users attempted to download certain legitimate Windows applications. Sandvine said that these allegations were "technically inaccurate and not feasible" and statements were "intentionally misleading". DPI systems can also enable censorship as they can be mis-used to impose internet shutdowns, prevent individuals from communicating their whereabouts, and limit access to journalist reporting.

Annex 2: NSO Group Case Study

Introduction

Founded in 2010, NSO Group Technologies Ltd. (NSO) is an Israeli technology company that designs, manufactures, and sells sophisticated cyber intelligence "solutions," including spyware products and "multi-layered cyber defense" services. Currently, NSO is majority-owned by the European private equity fund Novalpina Capital.

NSO's most well-known spyware product, Pegasus, is a targeted surveillance tool that enters an individual's phone or computer to gather data about the target. Pegasus gains control of the device by remotely installing itself through malicious links or "zero-click" attacks. Once installed, the spyware can remotely activate the camera or microphone, intercept communications, receive personal data such as calendar events, passwords, and contact lists, and track the location of the device.

NSO has said it only sells its products to government agencies or law enforcement to "thwart serious criminal acts that threaten life, liberty, safety, and personal security." However, journalists, advocates, and companies have released a large body of research showing that NSO supplies its spyware tools to governments with known surveillance-based human rights abuses and that this software has led to death, torture, arbitrary detention, harassment, and intimidation.

In response to international pressure, NSO published a Transparency and Responsibility Report in June 2021 that acknowledged the misuse of its products and described their salient human rights risks. However, leading digital rights experts found the report to lack crucial information, including disclosure of key legal challenges and remediation for victims. NSO says it has effective human rights mechanisms in place to mitigate these risks and has refused 15 percent of Pegasus business opportunities due to human rights concerns.

The risks inherent in surveillance technology have manifested in this case into material legal, operational, and reputational risks, causing the company to consider selling off the spyware unit.

Salient Human Rights Issues

Research from advocates around the world has connected NSO to countless human rights violations, including attacks on journalists, lawyers, human rights defenders, political dissidents, diplomats, and even heads of state. In July 2021, the French nonprofit Forbidden Stories launched the Pegasus Project, which exposed over 50,000 leaked phone numbers surveilled by NSO customers. Notably, the data revealed numerous states with well-documented rights-violating behavior, 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."

- **Morocco.** Amnesty International revealed that Moroccan authorities used Pegasus to surveil local human rights activist Maati Monjib since 2017, leading to harassment and his arbitrary detention. NSO responded to this allegation here.
- **Kingdom of Saudi Arabia.** In 2018, Citizen's Lab connected Pegasus to journalist Jamal Khashoggi's death, finding Pegasus infected Saudi dissident Omar Abdulaziz's phone, harvested communications between Abdulaziz and Khashoggi, and enabled the Saudi Government to track Khashoggi to Turkey where he was murdered. NSO Group has denied that its products were used to target Mr. Khashoggi.
- **Azerbaijan.** The Pegasus Project revealed that Khadija Ismayilova, an investigative journalist, was subject to a Pegasus attack for nearly three years. During this time, Khadija was harassed, falsely charged, and arbitrarily detained by local authorities. NSO has said that it cannot confirm or deny the identity of its government customers.

The unlawful use of Pegasus against individuals demonstrates a clear violation of several internationally recognized human rights, including the right to privacy, right to life, freedom from torture or degrading treatment, and the security of the person. (See Annex 1.) Additionally, utilizing surveillance to suppress expression and control dissidents perpetuates social contexts that further violate rights inherent to democratic values, including the right to freedom of expression, freedom from discrimination, or rights surrounding equality of life and opportunity. (See Annex 1.)

Double Materiality

The human rights risks associated with NSO's products and services have translated into an array of financially material risks -- legal, regulatory, operational, and reputational. In October 2019, WhatsApp filed suit in California against NSO, claiming Pegasus used WhatsApp servers to hack 1,400 user devices and target activists, journalists, and human rights defenders. The case has survived a motion to dismiss from NSO and is moving forward. Relatedly, in November 2021, Apple filed a lawsuit against NSO, to "curb the abuse of state-sponsored spyware." Beyond litigation, NSO is also under government investigations (e.g., US Department of Justice, Paris Prosecutor's Office, and the Israeli Defense Ministry) and facing potential criminal liability.

NSO has also faced operational disruptions as the result of investigations and regulatory actions, including limited access to key suppliers, resignations by executives, and diverted time, staff, and other resources to comply with information requests and on-site inspections.

In November 2021, the United States Commerce Department's Bureau of Industry and Security (BIS) placed NSO on its Entity List for engaging in conduct that is contrary to US policy or national security. The inclusion on the Entity List requires any US company to obtain a license before exporting products such as software, tangible goods, or technology information to NSO. The new requirement will increase the cost for NSO to apply for and obtain necessary licenses and potentially exclude crucial companies from its value chain. Shortly after NSO was listed by the BIS, the company's CEO-designate quit, citing the US decision as a key factor for his resignation.

Finally, NSO has faced reputational challenges. This impact can be seen through loss of investors, such as Blackstone pulling out of a $400 million bid to purchase 40 percent of NSO's holdings and mounting calls of public pressure against the company. After the Pegasus Project exposed NSO's spyware being used against US diplomats and French cabinet members, the EU Commissioner for Justice called on the EU Parliament to take swift action against NSO, and Congressional Members of the Senate Finance Committee and House Intelligence Committee demanded NSO be sanctioned for its conduct.

Financial Impact

In the wake of advocates' efforts, government action, civil litigation, and the private sector response, NSO has faced financial losses. In January 2021, NSO considered an initial public offering valued at around $2 billion. However, after a year of international scrutiny, NSO is in danger of defaulting on debts. In November, Moody's downgraded the company's credit rating to Caa2, indicating very high risk, and quotes on the company's debt are at just 70 cents on the dollar of $350 million. In response, NSO is considering altering the Pegasus product to only be used defensively or selling off or shutting down the Pegasus unit entirely. The company has spent nearly two-thirds of the Pegasus unit's remaining capital, investing heavily in drone-monitoring capabilities and big data analytics. NSO's rapid decline mirrors the surveillance technology industry generally as FinFisher recently initiated insolvency proceedings to restructure as a new company and the Hacker Team CEO called the company "dead" after a sale to new ownership.

Annex 3: List of Resolutions, Reports, and Statements Recommending Bans or Moratoriums on Surveillance Technologies

- EU Council Regulation 267/2012 of 23 March 2012 (places restrictions on trade in dual-use goods and technology)
- European Parliament Resolution of 11 December 2012 (calls for banning the export of "repressive tech" by EU)
- European Parliament Resolution of 12 March 2014 (examines U.S. National Security Agency's surveillance of EU citizens)
- European Parliament Resolution of 15 January 2015 (calls for EU-wide ban on the export to Egypt of intrusion and surveillance technologies)
- "Surveillance and Human Rights," Report of UN Special Rapporteur, June-July 2019 (recommends moratorium on dual-use technology and goods)
- Report by David Kaye (then UN Special Rapporteur on Freedom of Expression) and Agnes Callamard (then UN Special Rapporteur on Summary Executions) (reports on Saudi Arabia's use of surveillance technology, targeting Jeff Bezos, and Saudi diaspora human rights defenders using Pegasus spyware)
- Statement by UN High Commissioner for Human Rights Michelle Bachelet, 19 July 2021 (comments on use of spyware to surveil journalists and human rights defenders)
- Statement by UN Human Rights Experts in August 2021 (calls for ban on "life threatening" surveillance tech)
- Statement by the Higher Commissioner for Human Rights, Michelle Bachelet in September 2021 (comments on implications of Pegasus spyware)

Endnotes

1 United Nations Human Rights, Office of the High Commissioner, "UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools," June 25, 2019 (accessed December 27, 2021); UN News, "Independent UN rights experts call for 'immediate investigation' into alleged Bezos phone hack by Saudi Arabia," January 22, 2020 (accessed December 27, 2021); United Nations Human Rights Office of the High Commissioner, "New technologies must serve, not hinder, right to peaceful protest, Bachelet tells States," June 20, 2020 (accessed December 27, 2021); United Nations Human Rights Office of the High Commissioner, "UN expert joins call for immediate moratorium on sale, transfer and use of surveillance tech," July 15, 2020 (accessed December 27, 2021).

2 This guide uses the definition of human rights due diligence (HRDD) provided by Shift Project, the leading center of expertise on the UNGPs: "An ongoing risk management process that a reasona ble and prudent company needs to follow in order to identify, prevent, mitigate and account for how it addresses its adverse human rights impacts. It includes four key steps: assessing actual and potential human rights impacts; integrating and acting on the findings; tracking responses; and communicating about how impacts are addressed." Shift Project, "Human Rights Due Diligence," UN Guiding Principles Reporting Framework (accessed December 27, 2021).

3 Parliament of the United Kingdom, "Surveillance: Citizens and the State, Chapter 2: Overview of surveillance and data collection" (accessed on October 22, 2021).

4 Privacy International, "Mass Surveillance" (accessed on October 22, 2021).

5 United Nations Human Rights Council, "Surveillance and human rights: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression," May 28, 2019 (accessed on October 22, 2021).

6 Investor Alliance for Human Rights, "Investor Toolkit on Human Rights," May 2020 (accessed on October 22, 2o21).

7 Principles for Responsible Investment, "Why and How Investors Should Act on Human Rights," 2020 (accessed on October 22, 2021).

8 Principles for Responsible Investment, "The modern interpretation of fiduciary duty," November 6, 2020 (accessed on October 22, 2021).

9 This concept also provides an additional point of analysis and leverage – the potential negative financial impact associated with human rights harms – for digital rights organizations seeking to advance rights-respecting behavior among surveillance technology companies.

10 Anna Ahronheim, The Jerusalem Post, "Amid NSO scandal, over 3,600 export licenses revoked in the past year," January 31, 2022 (accessed on February 2, 2022).

11 In June 2021, the UN Working Group on Business & Human Rights released additional guidance about companies and investors' responsibilities to respect the rights of human rights defenders. The guidance states that, "business enterprises need to ensure, as a minimum, that their activities, actions and omissions, do not lead to retaliation, violence, death, legal harassment or any other form of silencing or stigmatization of human rights defenders, and they need to address adverse impacts on human rights defenders with which they are involved, either through their own activities or as a result of their business relationships." UN Working Group on Business & Human Rights, "The Guiding Principles on Business and Human Rights: Guidance on Ensuring Respect for Human Rights Defenders," June 2021 (accessed on January 13, 2022).

12 See Annex 1: Table of Salient Human Rights Issues

13 U.S. Department of State, "Country Reports on Human Rights Practices" (accessed on October 22, 2021).

14 Human Rights Watch, "World Report 2021" (accessed on October 22, 2021).

15 The Rule of Law Index does not include those countries (e.g., China, Saudi Arabia) that do not elect to participate, a decision that may represent a red flag to investors in terms of that country's level of transparency concerning its citizens' access to justice. World Justice Project, "WJP Rule of Law Index 2020" (accessed on October 22, 2021).

16 Ibid.

17 Digital forensics is the recovery, investigation, examination, and analysis of material found in digital devices, often in relation to mobile devices and computers.

18 Probes are used to collect data as it passes through a communications network. DPI systems are used to examine the content of data as it passes through a communications network. Passive probes collect data indiscriminately as it moves through the communications network. Active probes collect data from specific individuals using their identifiers (e.g., IP address) or based on specific signatures (e.g., specific semantic content). See "Catalyst 6500 Series Switches Lawful Intercept Configuration Guide," CISCO, August 2007 (accessed on November 4, 2021).