HEARTLAND INITIATIVE

WHITE PAPER | NOVEMBER 2025

Surveillance Risks in Conflict-Affected & High-Risk Areas: A Salient & Material Concern for Investors

Introduction

The global development, deployment, and spread of surveillance technologies have profound impacts on both individuals and society at large. While the surveillance industry has enhanced efficiency in fields like law enforcement, counter-terrorism, health care, and education, these same technologies have been used in ways that violate human rights. Such violations range from spyware-enabled privacy breaches against individuals—leading to their arrest and in some cases death—to the use of biometric surveillance to detain and persecute vulnerable communities.

Exposure to salient human rights impacts is increasingly leading to material risks—regulatory, legal, operational, and reputational—for surveillance companies and their shareholders. Growing sanctions regimes and export controls, strategic litigation by both companies and impacted individuals, the loss of access to American technology, and brand damage from advocacy campaigns and divestment decisions are all creating substantial financial losses for companies involved in surveillance-related harms.

The deployment of these products in conflict-affected and high-risk areas (CAHRA), settings with widespread human rights abuses and violations of national or international law, increases the frequency and severity of both human rights and material impacts. As authoritarian regimes, non-state armed groups, and private sector offensive actors use surveillance tools in CAHRA, investors must prioritize identifying, assessing, and addressing these risks within their portfolios. While investors have a responsibility to respect human rights, as outlined in the United Nations Guiding Principles on Business and Human Rights (UNGPs), their exposure to surveillance-related harms also creates material risks that they must address to fulfill their fiduciary duties to clients and fund mandates.

The pressure on investors to mitigate these risks is growing as the number, intensity, and duration of global conflicts and fragility increases, along with the use of targeted and mass surveillance. The World Bank estimates that by 2030 two-thirds of the world's poor will live in settings characterized by fragility, conflict, and violence. Relatedly, the Armed Conflict Location and Event Data (ACLED) monitor reports that global conflicts have doubled in the past five years, noting that instances of political violence in 2024 increased by 25 percent over the previous year, leaving one in eight people exposed to conflict.

The purpose of this paper is to provide a framework for investors and civil society organizations (CSOs) to better understand how surveillance technologies pose salient risks to rights holders in CAHRA and material risks to shareholders in these companies. Part one of the paper will outline relevant materiality concepts—traditional, impact, and double—and discuss how the "saliency-materiality nexus" connects these concepts to identify the most severe and systemic risks in a portfolio. Part two will detail the human rights harms associated with the deployment of targeted and mass surveillance technologies in CAHRA. Finally, part three will provide examples of how surveillance-related harms are translating into legal, regulatory, operational, and reputational risks for companies and shareholders.

HEARTLAND INITIATIVE

Surveillance Risks in Conflict-Affected & High-Risk Areas: A Salient & Material Concern for Investors

The Evolution of Materiality

"Materiality" is an accounting concept used to identify information that a reasonable investor would consider important when buying, selling, or exercising rights over securities. Even the most responsible institutional investment firms must frame their human rights, climate, or other sustainability efforts through a materiality lens. This is because institutional investors are bound by fiduciary duties to protect their clients' interests. Regulatory and voluntary frameworks for company reporting to investors also use materiality as the standard for what information must be disclosed to investors.

Financial Materiality

Traditionally, materiality has been limited to financial information about a company's performance that could affect shareholder value. This narrow understanding led investors and companies to focus on and disclose information that impacted the bottom line. However, with the rise of ESG (environmental, social, and governance) investing and greater consideration of sustainability-related risks, financial institutions are increasingly recognizing "impact materiality." This concept expands on the traditional definition to include information about a company's activities that could positively or negatively affect the environment, the economy, or stakeholders both inside and outside the company. For example, impact materiality would include information about how a technology company contributes to global greenhouse gas emissions, labor rights violations within its supply chain, or human rights abuses facilitated by its technology.

Impact & Double Materiality

As impact materiality has gained traction, investors have also recognized the concept of "double materiality." This holds that a company's external impacts can be material to both financial returns (financial materiality) and the economy, environment, and people (impact materiality). Double materiality encourages investors, companies, and regulators to simultaneously consider human rights and material risks when evaluating an investment. In essence, it is the primary accounting concept for identifying how a company's involvement in human rights harms could lead to financial losses.

International accounting standards and regulatory bodies are increasingly incorporating both impact and double materiality into their frameworks. For example, in their sustainability-related financial disclosure framework, the "Big Five" accounting standard organizations focus on "how sustainability matters create or erode enterprise value." They state that rights holders and the company's external environment can "positively or negatively affect the company's business model and therefore create or erode its enterprise value and financial returns to providers of financial capital."

Similarly, the European Union (EU) and some of its member states have passed laws, directives, and regulations that require companies and investors to disclose double materiality information, such as the French Duty of Vigilance Law. The EU Corporate Sustainability Reporting Directive (CSRD) requires a company to report on its impact on "environmental, social and employee matters, respect for human rights, anti-corruption and bribery matters." Additionally, the EU Corporate Sustainability Due Diligence Directive (CSDDD) requires covered companies to conduct human rights due diligence, which involves identifying and addressing how their operations, subsidiaries, and value chain partnerships contribute to human rights harms. Finally, under the EU Sustainable Finance Disclosures Regulation (SFDR), investors and other financial market participants offering ESG financial products must assess and report how their investment decisions affect sustainability factors, including human rights.

HEARTLAND INITIATIVE

Surveillance Risks in Conflict-Affected & High-Risk Areas: A Salient & Material Concern for Investors

The Saliency-Materiality Nexus

Heartland Initiative developed the "saliency-materiality nexus" as a context-specific version of double materiality. This concept posits that in CAHRA, salient human rights risks to people most often translate into material risks for companies and their shareholders.

Salient Human Rights Risks in CAHRA

"Salient human rights" are those rights most at risk of being negatively impacted by a company's activities and are identified through a process of assessing irremediability, scale, and scope. These risks are necessarily more acute and prevalent in CAHRA, where rights holders are more vulnerable to human rights harms from state or non-state actors, lack basic necessities of life, are more susceptible to exploitation, and have limited avenues for corporate accountability or government redress.

These contexts are further characterized by weak governance, as regimes are often unwilling or unable to protect democratic norms and individual rights. CAHRA feature widespread corruption and the absence of a state monopoly on the use of violence.

Due to the heightened risks endemic to CAHRA, the typical human rights and conflict risks associated with industries operating there are amplified, including those in the surveillance technology sector. There is a growing record—from government, civil society, and media reports—of authoritarian regimes in CAHRA using targeted and mass surveillance technologies, as well as technologies not originally designed for surveillance purposes (e.g., cloud-based platforms, telecommunications), to harass, detain, compel to work, and sometimes kill human rights defenders (HRDs), political dissidents, and/or vulnerable populations. These authorities either intentionally avoid or rarely have the necessary regulatory oversight and legal structures to ensure that surveillance technologies are deployed lawfully under international humanitarian, human rights, and criminal law and that impacted rights holders have access to justice.

Amplified Salient & Material Risks

What is less often reported is that the characteristics of CAHRA also increase material risks for companies and shareholders. As recent conflicts and crises demonstrate (e.g., Israel-Palestine, Russia-Ukraine, Myanmar, Sudan, Xinjiang Uygur Autonomous Region), companies in CAHRA face greater exposure to:

- An increasing number of regulatory regimes, including sanctions, trade controls, and anti-corruption laws.
- Strategic litigation on behalf of rights holders, especially with the advent of mandatory due diligence legislation in the EU and its member states.
- Disruption of company operations due to conflict, expropriation of assets by state or non-state actors, or loss of social or regulatory license to operate.
- Advocacy campaigns against companies operating in CAHRA and/or divestment decisions by ESG-aligned investors.

Such material risks have plagued the surveillance industry in these contexts. Egregious examples of mass surveillance (e.g., persecution of the Uyghur minority in Xinjiang Uygur Autonomous Region) and targeted surveillance (e.g., the kidnapping and murder of *Washington Post* journalist Jamal Khashoggi) have resulted in lawsuits, sanctions, travel bans, export controls, advocacy campaigns, and divestments against the developers and deployers of these technologies. Parts three and four below will provide additional details regarding the salient and material risks associated with the surveillance industry in CAHRA.

HEARTLAND INITIATIVE

Surveillance Risks in Conflict-Affected & High-Risk Areas: A Salient & Material Concern for Investors

Salient Risks of Surveillance Technologies

Surveillance technology typically falls within two categories based on its intended use: targeted surveillance and mass surveillance.

- Targeted surveillance uses overt or covert technology to discretely gather information from particular individuals. This can include remote intrusion software (commonly known as spyware) and digital forensic tools.
- Mass surveillance is indiscriminate, using systems or technologies to collect, analyze, store, and/or generate data on indefinite or large numbers of people. Common types include biometrics, IMSI Catchers, deep packet inspection (DPI) systems, and data retention systems.

While many mass surveillance systems access and process the data from a large group, they can also be used to support targeted surveillance of individuals by accessing individuals' locations, intercepting text messages or calls, and reviewing a device's data. For example, both DPI and IMSI Catchers can be used for either mass or targeted surveillance.

Moreover, mass surveillance systems can be instrumental tools in supporting broader international crimes against particular religious or ethnic groups. For example, mass surveillance technologies have been identified as a critical pillar of the Chinese government's oppression of Uyghur and other Turkic minorities in and beyond the Xinjiang Uyghur Autonomous Region, conduct that has been classified as crimes against humanity and genocide.

Surveillance Technology Value Chain

The nature of a company's exposure to surveillance-related harms depends on the type of technology being deployed and where the company sits in the value chain, which is the entire suite of companies necessary to deliver goods or services. Some companies, known as "pure players," focus solely on the development and sale of surveillance technologies. For example, NSO Group (NSO) and Dark Matter Group develop products designed to remotely access a person's electronic devices to extract personal information or location data.

Information and communication technology (ICT) companies are crucial in enabling both targeted and mass surveillance, often by providing the underlying infrastructure. This involvement can be seen in various ways, from direct collaboration to being an essential part of the value chain.

For example, some multinational ICT companies like Nokia and Cisco Systems were involved in developing Russian internet infrastructure. Their products were used to support the state's mass surveillance system (SORM), which has contributed to human rights abuses against Russian dissidents and is used to control internet traffic in occupied Ukraine. In other cases, surveillance platforms themselves rely on Artificial Intelligence (AI) systems and cloud computing software developed by technology companies.

Enabling Surveillance Infrastructure

Relatedly, telecommunications companies in CAHRA are often required to integrate surveillance tools, such as DPI devices, into their hardware to comply with government requests for individuals' data, including content of texts, calls, and internet traffic. In some contexts, governments may exploit these systems to surveil and ultimately persecute rights holders. For example, there is documented evidence that the Kenyan National Intelligence Services required local telecommunications operators to install IMSI Catchers and exploited this technology, without proper warrants, to track and detain HRDs prior to scheduled protests.

Other companies are key value chain partners that provide necessary inputs that support the development of surveillance technologies. For example, electronics companies may supply hardware such as video cameras that are ultimately used in facial recognition systems. Furthermore, AI, mass data analytics, or cloud computing companies are often critical to storing, processing, and interpreting data taken from mass surveillance systems in order to achieve targeted surveillance goals. Finally, companies producing and selling surveillance systems rely on brand name companies' products for their surveillance capabilities. For example, Salesforce's sales management program and Zoom's video conferencing platforms were found to have been providing services to Sandvine Incorporated, a company that provides DPI technology to authoritarian regimes.

Material Risks of Surveillance Technologies

Companies with direct or indirect connections to the human rights harms from targeted and mass surveillance systems deployed in CAHRA are at increased risk of exposure to material legal, regulatory, operational, and reputational risks. As described above, CAHRA are inherently high-risk markets, often already under heightened international scrutiny. They are subject to more restrictive regulatory regimes, experience more operational disruptions, and are frequently the focus of advocacy campaigns. Additionally, lawmakers, regulators, and administrative agencies are increasingly interested in curbing the impacts of surveillance technologies due to corresponding national security risks.

This trend is reflected in executive orders and joint statements issued by the Biden administration. In March 2023, President Biden signed Executive Order 14093 (EO 14093), which prohibited U.S. federal departments and agencies from using commercial spyware that poses counterintelligence or national security risks to the U.S. Government, or that foreign governments or persons may misuse. The executive order required federal entities to review their existing commercial spyware deployments and discontinue their use as soon as reasonably possible if risks were identified. Additionally, in September 2024, the U.S. and partner governments released a Joint Statement on Efforts to Counter the Proliferation and Misuse of Commercial Spyware. The statement emphasized information sharing and coordination, export and trade controls, regulatory cooperation, sanctions, and visa restrictions. It lent diplomatic weight and normative legitimacy to domestic measures like EO 14093, reflecting a broader U.S.-led diplomatic effort to build a coalition of states committed to restraining spyware abuses and to pressuring vendors and actors to adopt responsible practices.

Other countries have engaged in similar efforts, including the UK and France's Pall Mall process, which aims to address commercial cyber intrusion capabilities, and the EU's denial of 67 export license applications for cyber surveillance tools. Consequently, surveillance technology companies face a convergence of human rights, national security, and material risks that can significantly impact their financial performance. It should be noted that such administrative and diplomatic tools are subject to changes in political administrations and will fluctuate with differing priorities, as demonstrated by the Biden and Trump presidencies.

The next section includes an overview of the material risks associated with surveillance-related harms. While risks can generally be categorized as legal, regulatory, operational, and reputational, these types of financial impacts are often interconnected and can be experienced simultaneously. The following case studies should not be considered as identifying causal relationships between impact and cost, but rather as examples of how companies with proximity to human rights harms from the deployment of targeted surveillance technology can also suffer corollary financial impacts. Additionally, the case studies include examples of companies connected to both targeted and mass surveillance systems to demonstrate how these types of risk could apply across the entire surveillance technology ecosystem.

HEARTLAND INITIATIVE

Surveillance Risks in Conflict-Affected & High-Risk Areas: A Salient & Material Concern for Investors

Legal Risks

Companies engaging in or facilitating human rights harms in CAHRA through the use of surveillance technologies face increased criminal and civil liability. Civil claims are based on violations of civil statute, tort theories, and international law. These claims have been brought by a variety of stakeholders, including rights holders, CSOs, and multinational ICT companies whose products and services have been compromised by intrusive targeted surveillance. In the United States, the majority of these lawsuits have included violations of federal and state computer fraud statutes, as well as tort theories like trespass to chattel, negligence, infliction of emotional distress, and breach of contract.

Additionally, targeted and mass surveillance technologies have been used by both state and non-state actors to violate international law, leading to further criminal and civil legal risks. For example, some advocates argue that certain types of targeted surveillance tools, such as spyware, are fundamentally incompatible with human rights and can only be deployed in a rights-violating manner. Even when used for a legal and legitimate purpose under international law, the deployment of spyware violates the "essence of the right to privacy" because the technology's scope cannot be limited to meet the requirements of the principles of necessity and proportionality. Other types of mass and targeted surveillance tools can also facilitate egregious violations of international law, such as crimes against humanity, torture, or genocide. Finally, there is increasing documentation of state actors using mass and targeted surveillance in military operations during international and non-international armed conflicts, which includes violations of IHL.

The most notable example of legal liability for exposure to surveillance technology that led to adverse financial impact for the targeted company is the lawsuit brought by Meta Platforms, Inc. (Meta) against NSO. Meta sued NSO for unlawfully hacking its WhatsApp platform and extracting users' personal information through the deployment of spyware. Meta's lawsuit against NSO has overcome many of the typical legal challenges that often bar rights holders' claims against companies for human rights abuses, such as personal jurisdiction, *forum non conveniens*, and a lack of sufficient financial resources to litigate against large, well-funded companies.

In December 2024, a California federal court granted Meta summary judgment on all of its claims and imposed sanctions on NSO for failing to turn over its code during the discovery process. Subsequently, the jury ruled in May 2025 that NSO must pay more than $167 million in punitive damages to WhatsApp. However, in October, the court lowered the punitive damages owed to $4 million but issued a permanent injunction preventing NSO from targeting Meta's platforms—a move NSO claims could put the company out of business. This litigation contributed to NSO's two-year fall from a $2 billion valuation to "worthlessness," in addition to a myriad of legal, regulatory, operational, and reputational impacts described in more detail below.

Additionally, in 2011, advocates brought a lawsuit under the U.S. Alien Tort Statute against Cisco Systems for developing a mass surveillance system, the "Golden Shield," on behalf of the Chinese government. The surveillance software was allegedly customized to target minority groups for detainment, and Cisco staff reportedly provided training on how to conduct the targeted surveillance. While the original lawsuit was dismissed in 2023, a California district court revived the claims and the appellate court affirmed that the case could proceed. As of the date of this paper, Cisco Systems had appealed the decision to the U.S. Supreme Court.

HEARTLAND INITIATIVE

Surveillance Risks in Conflict-Affected & High-Risk Areas: A Salient & Material Concern for Investors

Case Studies: Legal Risks, Civil Liability

NSO Group	In 2022, journalists from El Salvador sued NSO in California, alleging the firm facilitated the unlawful access to and extraction of data from their devices. Though the district court initially dismissed the complaint on procedural grounds, the Ninth Circuit Court of Appeals overturned that ruling in July 2025, finding an abuse of discretion. The case has been remanded and remains active, marking a significant development in the application of U.S. law to international spyware allegations.
IDEMIA	In 2023, IDEMIA faced a lawsuit brought by CSOs under the French Duty of Vigilance Law. The action was based on the company's contract to provide biometric technology, which was alleged to have caused human rights harms, posed risks for unlawful surveillance, and contributed to discrimination against marginalized communities in Kenya. While the financial impact of the case is unclear, the parties reached a settlement requiring the integration of human rights safeguards into the technology.
ViaQuatro	In 2018, the São Paulo subway operator, ViaQuatro, was hit with a public civil lawsuit by a CSO for unlawfully deploying a facial recognition system that violated Brazilian data protection regulations. The 2021 court ruling awarded plaintiffs damages and issued an injunction to stop the system's use. Following an appeal, the fine against the company was increased to BRL $500,000, highlighting the escalating legal consequences for data protection violations.

Moreover, impacted rights holders, including high-ranking politicians, have filed criminal complaints in their respective jurisdictions against targeted surveillance companies. These legal actions have been based on violations of data protection regulations, export controls, and professional confidentiality requirements. Criminal liability for violating these laws can also result in charges against individual executives who facilitate the harms. Similarly, in 2017, the International Federation for Human Rights (FIDH) filed a criminal complaint against Amesys for selling a targeted surveillance system to the Al Sissi regime in Egypt. The complaint alleged that the Egyptian government used Amesys technology to unlawfully surveil, track, detain, and torture HRDs and dissidents. In 2022, the Investigative Chamber of the Paris Court of Appeals upheld indictments against the company and its executives for crimes against humanity and war crimes.

Case Studies: Legal Risks, Criminal Liability

FinFisher	In 2019, German prosecutors began a high-profile investigation into the surveillance company FinFisher over allegations that the company unlawfully exported its sophisticated spyware to the Turkish government. The investigation escalated when prosecutors raided the company's offices and the private residences of executives to secure evidence. Authorities ultimately indicted four executives on criminal charges related to violations of export laws. Facing insurmountable legal pressure and financial distress, the company filed for bankruptcy and ceased operations in 2023.
NSO Group	Rights holders globally have filed criminal complaints against NSO, its parent company Q Cyber Technologies, and Novalpina Capital (which purchased NSO in 2019). While most complaints are ongoing, the widespread awareness of NSO's wrongdoing prompted formal investigations by the EU. Furthermore, government leaders, legal figures, and rights holders in Spain have filed complaints to initiate national investigations. The scrutiny intensified in March 2025 when a Barcelona court ruled that three former NSO executives would be indicted.
Intellexa	A Greek journalist and politician filed several lawsuits against Intellexa, seeking criminal investigations for the alleged use of its Predator spyware to hack his personal devices. Approximately ten more complainants have since filed civil lawsuits related to Predator. As of the date of this white paper, a trial is underway in Greece in which four executives linked to Intellexa and a related company are facing misdemeanor charges for violating telecommunication privacy and data protection laws.

HEARTLAND INITIATIVE

Surveillance Risks in Conflict-Affected & High-Risk Areas: A Salient & Material Concern for Investors

Regulatory Risks

Companies connected to the deployment of targeted surveillance technology in CAHRA may face significant regulatory risks, including enforcement actions for violating data protection regulations, export controls, or sanctions regimes. Many of the U.S., UK, and EU sanctions regimes have a geographic scope focused on the prevalence of armed conflict (e.g., Mali, Russia), human rights violations (e.g., Myanmar, Venezuela), or national security risks (e.g., Chinese Military Company Sanctions). Relatedly, the U.S. has imposed visa bans on individuals found to be misusing or profiting from the misuse of spyware.

Export controls are designed to prevent the delivery of technology to certain actors identified by the government based on national security, human rights, or military-related risks. These designations have included entities with connections to known surveillance-related harms and companies have faced steep penalties for exporting products in violation of these regimes.

For example, in 2017, the U.S. Bureau of Industry and Security (BIS), the U.S. Department of Justice, and ZTE Corporation (ZTE) entered into a settlement of $661 million. The company was fined for violating U.S. export controls by building, operating, and maintaining telecommunications networks in Iran and North Korea, which have extensive track records of exploiting telecommunications networks to unlawfully surveil and oppress their citizens, dissidents, marginalized groups, and HRDs. ZTE was also alleged to have provided Iran with a massive surveillance system to be incorporated into the country's ICT infrastructure.

In April 2023, BIS imposed its largest standalone settlement of $300 million against Seagate for knowingly exporting hard disk drives to Huawei Technologies Co. Ltd. (Huawei) without a license. Huawei had been added to the BIS Entity List (U.S. Entity List) for providing products and services that facilitate the Chinese government's unlawful surveillance and oppression of the Uyghur minority. Seagate's investors brought a securities fraud claim against the company, alleging it acted deceptively in describing its relationship with Huawei and that the enforcement action decreased the value of shares by at least 8 percent.

Case Studies: Regulatory Risks

Clearview	The use of Clearview AI's facial recognition software by law enforcement has triggered a strong regulatory response across Europe. Following complaints about privacy and human rights harms, data protection regulators in France, Italy, Greece, and the Netherlands levied fines against the company, ranging from €20 to €30.5 million under the EU General Data Protection Regulation (GDPR). Separately, the UK Information Commissioner's Office (ICO) imposed a £7.5 million fine in 2022 for UK GDPR violations. Though Clearview initially succeeded in having the fine overturned jurisdictionally, the ICO successfully appealed, and the legal challenge continues.
Intellexa	In 2023, the Hellenic Data Protection Authority (HDPA) fined Intellexa €50,000 for violating the GDPR by failing to cooperate with an official investigation. The HDPA's probe, often referred to as "Greek Watergate," was launched following press reports of the alleged use of Intellexa's Predator spyware for illegal surveillance. This spyware was reportedly used to target prominent public figures, including opposition leaders, high-ranking Greek ministers, military officials, and journalists, highlighting the scope of the national surveillance scandal.
WS WiSpear Systems	Intelligence company WiSpear was fined €925,000 by the Cypriot Commissioner for Personal Data Protection in 2021. The fine stemmed from the company's collection of mobile data from individuals without their consent while testing and developing its technology—an act linked to the highly-publicized "spy van" scandal in Cyprus. Crucially, even after police found no illegal communication interception, the data protection commissioner determined that WiSpear's data collection still constituted a clear violation of GDPR privacy principles.

HEARTLAND INITIATIVE

Surveillance Risks in Conflict-Affected & High-Risk Areas: A Salient & Material Concern for Investors

Operational Risks

Companies connected to surveillance-related harms in CAHRA may also suffer operational impacts resulting in financial losses. These disruptions include losing access to value chain partners, markets, or skilled personnel. Operational issues can stem from regulatory restrictions, legal action, and administrative decrees.

Regulatory restrictions, such as export controls or sanctions, can limit other companies' ability to engage in specific transactions or otherwise do business with designated entities. Similarly, governments can issue administrative decrees that prevent specific actors, often government-funded agencies, from purchasing products from a particular market.

For example in 2024, Sandvine was added to the U.S. Entity List for providing DPI technology to the Egyptian government. This technology was reportedly used to facilitate targeted surveillance and censorship to suppress dissidents and HRDs. As a result of these regulatory restrictions, Sandvine was reportedly unable to secure contracts with major U.S. companies such as T-Mobile, Verizon, and Comcast. Additionally, the company was prevented from exporting or installing a stockpile of equipment and could not manufacture new products.

Although Sandvine was removed from the U.S. Entity List in October 2024 after committing to implement reforms, the company had already experienced significant financial losses. While the total cost is unknown, the company suffered hundreds of company layoffs, the exit of its most significant investor, Francisco Partners, and the initiation of bankruptcy proceedings to restructure at least $75 million of debt.

Case Studies: Operational Risks

Huawei	Huawei was added to the U.S. Entity List amid allegations of strong ties to the Chinese government, and its role in facilitating unlawful surveillance of HRDs and marginalized groups. Notably, in October 2022, the British government announced that, following guidance citing U.S. sanctions, all Huawei technology must be removed from the UK's 5G public networks by the end of 2027. These regulatory restrictions contributed to a 70% decrease in Huawei's annual profit in 2022 and significantly impacted its operations globally.
Qualcomm	Qualcomm, a leading American semiconductor and wireless technology company, saw its stock price decline by 4% after Huawei, one of its largest customers, was added to the U.S. Entity List for facilitating Chinese state surveillance, a drop that occurred despite a positive market trend. The pressure increased in 2024 when Qualcomm's license to sell 4G chips to Huawei was revoked, contributing to a 23% decrease in Qualcomm's share price from June 2024 to February 2025.
ZTE	ZTE faced U.S. sanctions after an investigation found the company not only provided surveillance equipment and ICT infrastructure to Iran and North Korea but also supplied false information to investigators. The company's deceptive conduct led to its addition to the U.S. Entity List. The action restricted 25-30% of ZTE's supply chain, reportedly halted operations, and effectively crippled the $17 billion company resulting in a $7 billion loss in market capitalization.

HEARTLAND INITIATIVE

Surveillance Risks in Conflict-Affected & High-Risk Areas: A Salient & Material Concern for Investors

Reputational Risks

Companies and investors connected to targeted surveillance can face significant reputational risks that translate into material financial impacts. A company's reputation is an asset that affects its ability to secure funding, maintain customer trust, and attract employees. Companies that are publicly exposed for their role in causing or contributing to surveillance-related harms can experience a loss of capital, boycotts, protests, a loss of revenue from consumer preferences, and an inability to attract or retain skilled employees.

Further, employees are becoming more vocal about their company's involvement in human rights issues. Companies linked to surveillance controversies have experienced employee protests, boycotts, and the departure of skilled staff. For example, Amazon, Alphabet, and Microsoft have faced significant employee protests based on the companies' relationships with the Israeli Defense Forces (IDF), including allegations that their business relationships and technology contributed to war crimes during the conflict in Gaza.

Case Studies: Reputational Risks

Oosto	AnyVision Interactive Technologies Ltd., a developer of AI-powered facial and visual recognition software, was rebranded as Oosto in October 2021. This change followed a controversy over 2019 reports alleging its technology was used for the mass surveillance of Palestinians in the occupied West Bank. The resulting reputational damage ultimately led to Microsoft's investment arm withdrawing its $75 million stake in the company. Following the divestment, Microsoft also announced a policy change, committing to end all minority investments in companies that sell sensitive facial recognition technology.
Cognyte	Since being spun off from Verint in 2022, Cognyte has faced investor backlash. Its surveillance tools have been linked to the tracking and harassment of HRDs and vulnerable groups. Citing the company's sales of these tools to governments involved in military occupation (such as Israel and Morocco), prominent institutional investors—including the Government Pension Fund Global, Storebrand Asset Management, and KLP—have divested from Cognyte.
Microsoft Corporation	Microsoft is facing employee backlash—including resignations, internal protests, and the "No Azure for Apartheid" coalition—over services provided to the IDF. The controversy centers, in part, on the use of Microsoft's Azure cloud services by the elite IDF Intelligence Corps Units 8200 and 81. Responding to the backlash, Microsoft launched internal and external investigations that verified the allegations. Based on a violation of the terms of service, Microsoft terminated some of Unit 8200's cloud storage and AI services. While the financial impact is uncertain, Microsoft acknowledges that the reputational damage could adversely affect its business, operations, and ability to attract qualified employees.

HEARTLAND INITIATIVE

Surveillance Risks in Conflict-Affected & High-Risk Areas: A Salient & Material Concern for Investors

Conclusion

As targeted and mass surveillance technologies proliferate alongside geopolitical conflict and fragility, the risks to rights holders and shareholders will continue to grow. Although this trend is alarming, recognizing how the use of these technologies in CAHRA create distinct but interrelated risks for these actors also presents an opportunity to advance accountability in the surveillance technology industry. By identifying, assessing, and addressing surveillance-related harms across their investment universe and directly with portfolio companies, investors can more effectively fulfill their responsibilities under the UNGPs and as responsible fiduciaries to clients and fund mandates.

Using the saliency-materiality nexus as an analytical framework, this paper summarized how surveillance-related harms in CAHRA can translate into material losses for companies and shareholders. Additionally, to enable investors to identify, assess, and address these risks among portfolio companies, Heartland Initiative, the Business & Human Rights Resource Centre, and Access Now, in partnership with leading Global Majority digital rights organizations and institutional investors, developed the guide Navigating the surveillance technology ecosystem: A human rights due diligence guide for investors. The guide provides a practical set of recommendations for investors to analyze portfolio companies' exposure to surveillance-related harms from the product research and design stage to end-use and make corresponding decisions around investment, engagement, and/or exclusion.

Acknowledgements: This white paper was authored by Mallory Miller, with substantial contributions from Aaron Clements-Hunt, Sam Jones, Hannah Norman, and Rich Stazinski. We extend our thanks to the Business & Human Rights Resource Centre for their critical insights and feedback, which informed the research and findings of this work. We also gratefully acknowledge the generous support of the Ford Foundation, which made this publication possible.