Business & Human Rights Resource Centre

Scrutinising migration surveillance

HUMAN RIGHTS RESPONSIBILITIES OF TECH COMPANIES OPERATING IN MENA

SEPTEMBER 2022

Contents

Executive summary . . . 3

Introduction . . . 5

Analysis of company responses . . . 7

- Transparency . . . 8
- Human rights policies . . . 9
- Human rights due diligence . . . 10
- Stakeholder engagement . . . 11
- Grievance mechanisms . . . 11

Human rights concerns and implications for migrants, refugees and asylum seekers . . . 12

- Racial profiling and discrimination at West Bank checkpoints . . . 12
- Biometric systems entrenching inequalities at Jordan refugee camps . . . 13
- Monitoring and deportation of migrants and refugees crossing the Mediterranean . . . 14

Recommendations . . . 15

Annex:
List of tech companies approached to answer survey questions . . . 16

Executive summary

Personal security is a human right, and the protection of national security is a legitimate concern of governments. Digital technology, including surveillance technology, can play a useful role in advancing human security if it is well-managed and follows the principles of legality, necessity and proportionality. However, without robust regulation it can rapidly facilitate human rights abuse. In this context, the opaque global surveillance technology industry, and the human rights implications of its products and services for migrants, asylum-seekers and refugees, are increasingly cause for alarm. At the hands of repressive regimes, such as many in the Middle East and North Africa (MENA), the consequences of these technologies can be even more extreme – resulting in fundamental losses of privacy, dignity and autonomy, and entrenching inequality between citizens and those forced to flee their home states. There is an urgent need for governments, surveillance technology companies and the investors who fund them to halt this trajectory through improved transparency, robust human rights due diligence and support for regulation of a lucrative industry whose profits can be linked to human rights violations of vulnerable groups.

This briefing analyses responses to a survey conducted by the Business & Human Rights Resource Centre (the Resource Centre) on corporate transparency and the human rights due diligence processes of 24 companies which have allegedly produced or provided surveillance technologies to governments in the MENA region. We further sought responses from 24 companies regarding specific allegations of human rights infringements in the context of border management and migration in the region.

Strikingly, only five of the companies approached – Airbus, G4S, Cellebrite, IrisGuard, and Thales Group – provided any form of survey response. An additional two companies (Nexa Technologies and VideoTec) responded to abuse allegations, together with Airbus, Cellebrite and G4S. This reflection of the sector's limited commitment to transparency – a fundamental requirement for human rights compliance for any company – is profoundly concerning.

Our analysis also found:

- Surveillance technology companies lack **human rights policies** to guide commercial decisions and approaches.
- A lack of **adequate and effective due diligence** by companies to identify human rights risks, including the undertaking of heightened human rights due diligence recognising the higher risks involved.
- A lack of **engagement with stakeholders**, especially with civil society and those likely to be placed at risk by surveillance software deployment.
- Underperformance on ensuring **grievance and remedy mechanisms** are accessible to key stakeholders, including impacted communities and individuals, for when things go wrong.

The implications of these findings for migrants, asylum-seekers and refugees in the MENA region are grave, particularly given the lack of regulation of the sector. While migration control is a legitimate state action, evidence increasingly points to surveillance and monitoring technology, including iris recognition, facial scanning and unmanned drones, being used in ways which threaten the fundamental freedoms and rights of these communities and broader society. Case studies from Palestine, Jordan and Libya included in this briefing highlight how this technology can embed bias and discrimination, resulting in violations of autonomy and interception and return of asylum-seekers fleeing torture, among other rights infringements.

While the human rights policies and practices of the companies responding to the Resource Centre's survey and queries are thin, they nevertheless indicate better practice in comparison with those companies which ignored the survey.

Clear opportunities for improvement exist. The former UN Special Rapporteur on the Promotion and Protection of the Rights to Freedom of Opinion and Expression, David Kaye, has called for a moratorium on the global sale and transfer of private surveillance tools until robust safeguards are put in place to regulate such practices and ensure that states use these tools appropriately. Modest amendments to the European Commission's draft Corporate Sustainability and Due Diligence Directive could demand greater human rights responsibility from European tech companies – including those allegedly exporting surveillance technologies to MENA states – whose products have the potential to cause harm. Some of the more responsible investors in surveillance tech, such as Goldman Sachs, are demanding more due diligence from investee companies – a practice that needs to spread rapidly. Investors and companies already have human rights risk management frameworks in the form of the international standards of the UN Guiding Principles on Business and Human Rights (UNGPs) and OECD Guidelines, and guidance manuals.

In the face of the growing climate crisis, global conflict and increasing economic instability, migration will continue to rise. People on the move, particularly asylum seekers and refugees, are highly vulnerable to the rights abuses irresponsible deployment of surveillance and monitoring technology may facilitate. Governments, companies and investors should act now to ensure migration management through technology does not become shorthand for violation of the rights of some of the world's most marginalised people.

We are calling on governments in these countries to end their trade in and use of invasive surveillance technologies and services until regulations guaranteeing their use complies with international human rights standards are in place.

Companies should halt the sale, transfer and use of invasive surveillance technologies until they have implemented robust human rights due diligence, remedy and reporting policies, which includes effective consultation with local CSOs and those affected. They should be able identify and mitigate human rights risks, and provide remedy when things go wrong for rightsholders.

Investors should strengthen their human rights policies and ensure they are in line with the UNGPs. Additionally, they should review portfolio companies that provide authoritarian governments in the MENA region with surveillance tools and products, and ensure they have evidence the company's human rights compliance system is sufficient to address human rights risks.

Introduction

Increasingly, governments in the MENA region are purchasing and using powerful digital tools, ranging from spyware and wiretapping tools to facial recognition technology for targeted and mass surveillance. These tools are often used to silence activists and journalists, and repress organised opposition, as invasive laws on national security and anti-terrorism facilitate state practices which infringe on people's rights and fundamental freedoms. This empowers companies which have little fear of being held accountable.

A similar trend can be seen in the context of border management and migration in recent years, with increasingly authoritarian governments in MENA introducing policies or participating in programmes with European countries aimed at curbing migration in ways that increase the vulnerability of migrants and refugees. Conflict, climate change and economic instability continue to drive the increasing number of forcibly displaced people. The enhanced use of autonomous border security systems, such as drones, facial recognition and biometric systems, poses new threats to human rights. There is already evidence such systems push migrants to take more dangerous routes, and concerns have been raised that a gradual trend toward weaponised migration will endanger migrants' lives further.

Surveillance technology companies are deeply implicated in these trends. Private companies around the world – including European and Israeli firms – create, transfer and service surveillance technologies for authoritarian governments in the MENA region in opaque and unaccountable ways. As highlighted by the MENA Surveillance Coalition, *"the MENA region has become a breeding ground for invasive surveillance, allowing for private tech companies to reap profits off egregious human rights violations."*

In the context of border management and migration, companies with operations in the MENA region have allegedly been involved in perpetuating human rights abuse against migrants, refugees and asylum seekers. They have been accused of operating drones on migrants crossing the Mediterranean to monitor their movement without rescuing them; preventing migrants arriving by boat and leading to their detention in abusive conditions in Libya; forcing millions of Syrian refugees in Jordan to exchange their iris scans and biometric data for assistance without meaningful consent; and deploying facial recognition and predictive policing for racial profiling and targeting of Palestinians crossing checkpoints in the West Bank. These cases have demonstrated how data-driven or algorithmic decision-making can increasingly lead to discrimination against already marginalised communities and strengthen authoritarian governments, while creating sizeable profits for software companies.

Because the companies in the private surveillance industry operate under a cloak of secrecy, the public lacks any information about the way in which they may – if at all – consider the human rights harms caused by their products to migrants, refugees and asylum seekers.

The UNGPs provide a framework for assessing whether surveillance companies respect the rights of those affected by their products and services. In particular, the UNGPs place emphasis on business commitments to respect human rights by undertaking due diligence processes to identify, prevent, mitigate and account for human rights impacts. However, the lack of mechanisms in place to ensure compliance with the principles remains a major barrier to greater corporate transparency and accountability – particularly in industries known for their secrecy, such as surveillance companies.

A decade after the adoption of the UNGPs, voluntary due diligence measures undertaken by companies are weak, leaving glaring gaps in human rights safeguards. Encouragingly, there is growing appetite for mandatory human rights and environmental due diligence regulations across a number of jurisdictions, including at the European Union (EU) level with the development of the draft Corporate Sustainability Due Diligence Directive. However, key areas must be strengthened if the Directive is to effectively curb the harmful practices of the tech sector and, more specifically, the surveillance industry.

The EU's new export control rules on surveillance technology, which entered into force in September 2021, are another step towards preventing the abuse of surveillance technology. If implemented consistently and robustly, this new regulation can enhance transparency of export licensing decisions that is key to ensuring respect for human rights by the surveillance industry; an industry currently operating with opacity and impunity.

Given the absence of a robust international framework that would establish binding rules for the sale and transfer of surveillance technology, in August 2021, UN special rapporteur mandate holders, including the UN Working on Business and Human Rights, called for a moratorium on the sale of surveillance tools until regulations are implemented to safeguard human rights.

In July 2022, the Resource Centre invited 24 companies to respond to questions about their provision or deployment of surveillance technology for purposes of migration and border control in the MENA region, as well as about their human rights due diligence processes more generally, and any steps they are taking to mitigate human rights risks related to the use of these technologies on the following at-risk groups: migrants, refugees and asylum seekers. In addition, we invited the same 24 companies to respond to specific allegations of human rights abuse in the context of border management and migration in the region.

Analysis of company responses

This briefing covers a high-risk sector for human rights violations, in a high-risk region where situations of armed conflict, violent extremism, shrinking civic space and repression of civil society are common challenges. While news articles and reports published by peer human rights organisations point to widespread surveillance, limited responses from companies to our survey and allegations of human rights abuse underscore the significant lack of transparency, safeguarding policies and accountability of companies selling surveillance software and services. Migrants, asylum seekers and refugees are particularly vulnerable in the face of this opacity.

The 24 companies profiled in this report had two weeks to respond to the survey, with an extension of one week – giving them a total of three weeks to provide a response. In this time we received responses from five companies: **Airbus**, **G4S**, **Cellebrite**, **IrisGuard**, and **Thales Group**.

We identified six key concerns:

- A broad lack of **transparency** regarding clients, contracts and licensing in relation to human rights protections and impacts, with confidentiality clauses frequently cited as the reason for this secrecy.
- A lack of clear **human rights policies** to guide commercial decisions and approaches.
- A lack of **adequate and effective due diligence** to identify human rights risks, including the undertaking of heightened human rights due diligence.
- Inadequate **consultation** and lack of **engagement with stakeholders**, especially with civil society and those likely to be placed at risk by surveillance software deployment.
- Underperformance on ensuring **grievance and remedy mechanisms** are accessible to a wide variety of stakeholders, including impacted communities and individuals, for when things go wrong.
- A range of human rights concerns and implications for migrants, refugees and asylum seekers, including issues of **civil liberties, privacy and discrimination**.

Transparency

Companies demonstrate a broad lack of transparency on client, contracts and licensing with regard to human rights protections and impacts, often hiding behind confidentiality clauses.

None of the companies approached stated explicitly which countries in MENA they operate in or to which they provide surveillance solutions, services, goods, or equipment, or the type of surveillance technology they provide to governments in the region.

Three companies (**G4S**, **Thales Group** and **Airbus**) stated they cannot disclose the contracts or any details about their contracts with government clients or the number of surveillance solutions, products, services or equipment that have been distributed. **G4S** asserted it was restricted from doing so due to laws and regulations, while **Thales Group** stated the information is subject to confidential agreements and contractual relationships with their clients, as well as citing security reasons. In 2019, Amnesty International reported that *"national security considerations"* or *"confidentiality clauses"* have been exploited by companies to *"keep information on their activities out of the public domain."* The latter also noted the sensitivity of the issue of border control, particularly in unstable countries and conflict zone areas.

While unable to disclose detailed information about government clients, **Airbus** confirmed the company provided surveillance "solutions" to customers in the MENA region for the purpose of border control, but stated it does not produce surveillance equipment (cameras, radars, etc.). The company did not offer further information on the nature of "solutions" provided. **Cellebrite** said it does not offer technology solutions that support surveillance or monitoring efforts and that its solutions are used lawfully to help government agencies and law enforcement investigate an event *after* it has occurred – not *prior* to it. **IrisGuard** altogether denied the provision of any surveillance products or services to governments in MENA.

None of the companies provided an updated list of the surveillance solutions, products, services or equipment they supply to governments in MENA.

The low response rate from the companies surveyed highlights a lack of commitment to transparency by companies operating in the surveillance industry. Further, responses we did receive indicate much more needs to be done by surveillance tech companies to understand and mitigate their human rights impacts.

Human rights policies

Surveillance technology companies require clear human rights policies to guide commercial decisions and approaches.

Principle 15 of the UNGPs calls on companies to adopt a human rights policy setting out their responsibility to respect human rights, and Principle 16 elaborates further that companies should embed respect for human rights in a publicly available human rights policy statement.

This is critical in high-impact sectors such as surveillance technology, where human rights risks are prevalent. Between 1 July 2017 and 31 July 2022, the Resource Centre recorded 25 allegations of abuse linked to the sector globally, including against some of the companies mentioned in this briefing, ranging from allegations of contributing to state repression in Egypt, limiting digital rights and censoring voices in Palestine and selling products to countries with a history of leveraging digital technology for human rights abuses in China, Russia, Myanmar, Saudi Arabia and around the world, as well as enabling detentions, prosecutions and harassment of journalists, civil rights activists, dissidents and minorities.

Despite this, in response to the question about their human rights policies and internal processes governing the provision of surveillance technologies, **Airbus**, **G4S**, **Thales Group**, and **Cellebrite** stressed their commitments to human rights.

Given the clear human rights impacts of their products and services, adherence to the UNGPs in respect of policy and practice is essential. More is required of the sector to ensure these risks are properly identified and mitigated.

Human rights due diligence

Companies do not show evidence of adequate and effective due diligence to identify human rights risks, including undertaking heightened human rights due diligence where necessary.

When asked about their human rights due diligence and any steps they are taking to mitigate and prevent risks to migrants, refugees and asylum seekers, four companies (**Airbus**, **Thales Group**, **G4S**, and **IrisGuard**) said they undertake human rights impact assessments through processes and tools. **Airbus** said:

> *... Airbus constantly monitors changes to international law to ensure that all sales are in compliance with any applicable legal requirements with regard to transactions with countries under the UN, EU, UK and US sanctions... Impact of products and services on the right to life and liberty is one of the human rights issues that the company is prioritising, where it is currently reviewing how to integrate risk-based human rights due diligence through its products and processes."*

Thales Group, a signatory to the UN Global Compact for nearly 20 years, stated it has developed strong integrity commitments for designing an ethical, socially accountable facial recognition system.

G4S said it carries out regular "heat-map reviews" to identify the countries in which human rights risks are deemed to be high. Further, in its Ethics Code, **G4S** states:

> *Before embarking on any contract, [we] carry out due diligence on customers, suppliers and subcontractors to check for evidence of current or past human rights abuses... We do not want to work with organisations that abuse the rights of others."*

IrisGuard carries out a DDIQ (AI-based automated due diligence solution) using a third-party analytics platform which identifies, classifies and ranks any flagged risks. This process is also mandated by its key shareholders, including Goldman Sachs. **Cellebrite** stated the company has strict licensing policies and restrictions to govern the sale of its products and how customers utilise its solutions.

When operating in conflict-affected or high-risk solutions such as those present in the MENA region, companies are expected to undertake heightened human rights due diligence. Concerningly, only one of the surveyed companies (**G4S**) appeared to consider the MENA region as a high-risk area and accordingly conduct special due diligence processes for these countries. It stated:

> *We conduct human rights due diligence reviews of all new country entries and major business opportunities as part of our executive review process. In addition, human rights controls, due diligence frameworks, and control self-assessments are regularly carried out for **higher risk** businesses and are integrated into the company's risk and compliance systems."*

None of the companies stated clearly if the company or subsidiary is planning to stop engaging in the sale or provision of a range of surveillance solutions, products, services or equipment to MENA countries with a track record of human rights violations.

Although the four companies confirmed they undertake due diligence measures to identify and mitigate human rights risks, they do not publicly disclose their due diligence policies, making it difficult to assess whether they are being implemented in practice and whether they are effective.

Stakeholder engagement

Companies do not show meaningful engagement with stakeholders, including groups at risk of surveillance, on issues such as the human rights implications of company products.

Regular and effective stakeholder engagement, an integral part of human rights due diligence processes, is key to enhancing prevention and remediation of business-related human rights abuse. In this regard, only one company (**IrisGuard**) provided a substantial response, while **Airbus** stated it currently does not hold such consultations with affected communities (such as migrants, refugees and asylum seekers) and human rights defenders.

With the UN and humanitarian agencies as its main clients, **IrisGuard** emphasised the company's role is to provide iris biometric verification systems to clients, who themselves have direct contact with affected communities, such as refugees, and beneficiaries. The company said it is therefore not authorised to conduct direct liaisons with them. However, it noted it receives feedback from clients through extensive research projects, which includes direct feedback from refugees on a range of issues.

Grievance mechanisms

Companies lack adequate grievance mechanisms that enable individuals to submit complaints concerning human rights abuses facilitated by company products and services.

When companies were asked about grievance mechanisms in place for people to raise concerns or complaints, only **Airbus** and **G4S** confirmed that employees, suppliers or other third parties can raise concerns or complaints through anonymous channels. **IrisGuard** said it monitors its communications channels regularly to respond to any concerns about its products, as well as ensure its clients, such as UNHCR, have grievance mechanisms to lodge any complaints and feedback about its systems or equipment. **Cellebrite** and **Thales Group** did not respond to this question.

Human rights concerns and implications for migrants, refugees and asylum seekers

Over the last decade, private companies have increasingly played a central role in facilitating human rights violations and reinforcing discriminatory policing practices through the deployment of AI-based authentication systems and tools. Several studies have shown that algorithmic decision-making tends to discriminate against already marginalised or excluded communities, such as migrants, refugees and asylum seekers. Emerging technologies, such as drones, have also been used to facilitate deportation and pushback against these communities, leading to arbitrary detention and abuse. Below, we explore three case studies illustrating the human rights consequences of border externalisation and deployment of surveillance technologies in the context of migration on migrants, refugees and asylum seekers in the MENA region.

Racial profiling and discrimination at West Bank checkpoints

Microsoft came under fire in 2019 for funding Israeli facial recognition company **AnyVision**, which reportedly carries out surveillance on Palestinians crossing checkpoints in the West Bank. According to reports, AnyVision provided the Israeli military with a technology known as Google Ayosh, where "Ayosh" refers to occupied Palestinian territories and "Google" refers to the technology's ability to search for people. This technology is based on cameras spread across the West Bank with the purpose of identifying individuals through facial recognition technology.

In response to **Microsoft**'s investment, human rights advocates voiced concerns about the dangers of mass facial recognition, which could lead to bias and discrimination against thousands of Palestinians who pass through checkpoints every day to visit friends and family in the West Bank. In addition, they argued the use of facial recognition technology developed by **AnyVision** was incompatible with **Microsoft**'s public statements about ethical standards for facial recognition technology. Human Rights Watch also called on **Microsoft** to reconsider its investment due to the *"human rights risk associated with the investment in a company that's providing [facial recognition] technology to an occupying power."*

Following widespread criticism of the company and coordinated global efforts by civil society organisations, Microsoft decided to halt its investment in **AnyVision** and released a joint statement stating, *"After careful consideration, Microsoft and AnyVision have agreed that it is in the best interest of both enterprises for Microsoft to divest its shareholding in AnyVision,"* adding that, *"For Microsoft, the audit process reinforced the challenges of being a minority investor in a company that sells sensitive technology, since such investments do not generally allow for the level of oversight or control that Microsoft exercises over the use of its own technology."*

The Resource Centre invited **AnyVision** to respond to allegations the company provides military forces with facial recognition technology used for discrimination and surveillance of Palestinians at border crossings. The company did not respond.

Biometric systems entrenching inequalities at Jordan refugee camps

Increasing use of biometric technology by governments and aid agencies in the MENA region has profound impacts for business, governance and society. While some humanitarian agencies have noted the potential for such tools to provide food and financial security for refugees, a growing chorus of voices has expressed concerns about the potential for biometric tools to facilitate human rights violations, particularly those of the region's most vulnerable communities such as migrants, refugees and asylum seekers.

In 2013, Jordan became the first country where the UN High Commissioner for Refugees (UNHCR) introduced an iris scanning system for registering Syrian refugees. According to the World Food Program (WFP)'s regional communications officer, the UNHCR has biometrically registered 90 per cent of Syrian refugees in Jordan. In addition to registration, WFP implemented a biometric cash system in partnership with **IrisGuard**, a UK-registered company, to allow Syrian refugees living in camps to purchase food from grocery stores and local shops in exchange for their biometric data. Refugees who want to receive WFP's assistance have no choice but to surrender their eye scan, as this system relies on the UNHCR's database to confirm refugees' identity before allowing them to withdraw money from ATMs or purchase from groceries. As UN Special Rapporteur on racism, racial discrimination, xenophobia and related intolerance E. Tendayi Achiume noted:

> *"Conditioning food access on data collection removes any semblance of choice or autonomy on the part of refugees — consent cannot freely be given where the alternative is starvation."*

According to reports, **IrisGuard** is providing WFP and UNHCR with iris scan technology, which has direct implications and potential risks for the security, privacy and dignity of refugees, reproduces asymmetries between refugees and humanitarian agencies, and ultimately entrenches inequalities. Critics of the iris scan technology, and biometric systems more broadly, argue that refugee camps are profitable markets for companies because they can sell their products as humanitarian aid and test them on a large scale, while the refugees are not in a position to question their biometric coverage.

The Resource Centre invited **IrisGuard** to respond to these allegations. The company did not respond.

Monitoring and deportation of migrants and refugees crossing the Mediterranean

In August 2021, EU border agency Frontex awarded contracts worth €100 million to companies for providing aerial surveillance services and operating unmanned drones to monitor migrants and refugees on the move in Mediterranean and Libyan coastal areas.

Under this agreement, **Airbus** and **Israel Aerospace Industries (IAI)** reportedly received €50 million to operate its Heron drone, and another €50 million contract was signed with Israeli arms company **Elbit Systems** to operate its Hermes 900 drone. Notably, some of these companies have been operating surveillance flights in the Mediterranean for Frontex for years, including in Tunisia and North African countries more broadly.

Although Frontex claims drones are crucial to assisting in the rescue of migrants and refugees by detecting and monitoring their movement, a recent report by Human Rights Watch suggests otherwise, revealing surveillance drones have been used to monitor migrants and refugees without aiding in their rescue, and in some cases have facilitated interceptions and deportation to Libya.

Private companies contracting with Frontex such as **Airbus**, **IAI** and **Elbit Systems** have also been heavily criticised for contributing to a system of increasingly militarised borders, which results in pushbacks and violence against migrants and refugees crossing the borders in Libya and elsewhere in the Mediterranean. In addition, the drones supplied by these companies were reportedly deployed by the Israeli military and tested in a series of attacks on the Gaza Strip in 2014, implying they can be promoted for border surveillance as "combat proven" equipment.

The Resource Centre invited the three companies to respond to these allegations. Only **Airbus** responded to our request; IAI and **Elbit Systems** did not respond.

Airbus stated the company's business activities with the European Border and Frontex are *"very formal and fully transparent."* It also explained the main purpose of surveillance services provided by the company is to *"support search and rescue missions,"* while also performing other services such as *"providing assistance to EU and non-EU countries in border surveillance operations against criminal acts like terrorism, drug smuggling, human trafficking or illegal shipping."*

Recommendations

The following recommendations emerge from findings from both the survey and companies' responses to allegations, as well as conclusions from the UN and other partners on surveillance software and the protection of human rights.

For states and governments:

- End the use of invasive surveillance technologies on migrants, refugees and asylum seekers, and adopt safeguards to protect these vulnerable communities in line with international human rights law.
- Declare an immediate moratorium on trade in surveillance technologies and services in line with calls by the former UN Special Rapporteur on the Promotion and Protection of the Rights to Freedom of Opinion and Expression, until there are robust regulations in place to guarantee their use in compliance with international human rights standards, ensuring accountability and transparency.
- Accelerate efforts to develop a multilateral initiative to create minimum international standards for trade in surveillance software.
- Specifically, the European Commission should add technology, including surveillance, to the high-impact sectors category in the final text of the EU's Corporate Sustainability and Due Diligence Directive and include a default licensing requirement for this high-risk sector.

For companies:

- Strengthen human rights risk management in line with international standards set out by the UNGPs and OECD Guidelines, including robust stakeholder/rightsholder engagement and access to remedy.
- Conduct heightened human rights due diligence and adopt a conflict-sensitive approach when operating in conflict-affected and high-risk areas to avoid becoming involved in severe human rights abuses and violations of international humanitarian law.
- Halt the sale, transfer and use of surveillance technologies until the company has implemented robust human rights due diligence which includes effective consultation with affected rightsholders, particularly migrants, refugees, and asylum seekers and civil society. They should be able identify and mitigate human rights risks, and provide effective remedy when things go wrong for rightsholders.
- Develop and publish transparency reports disclosing the potential uses and capabilities of their products, as well as the types of support provided, incidents of misuse, and information on the number and type of sales to government agencies.

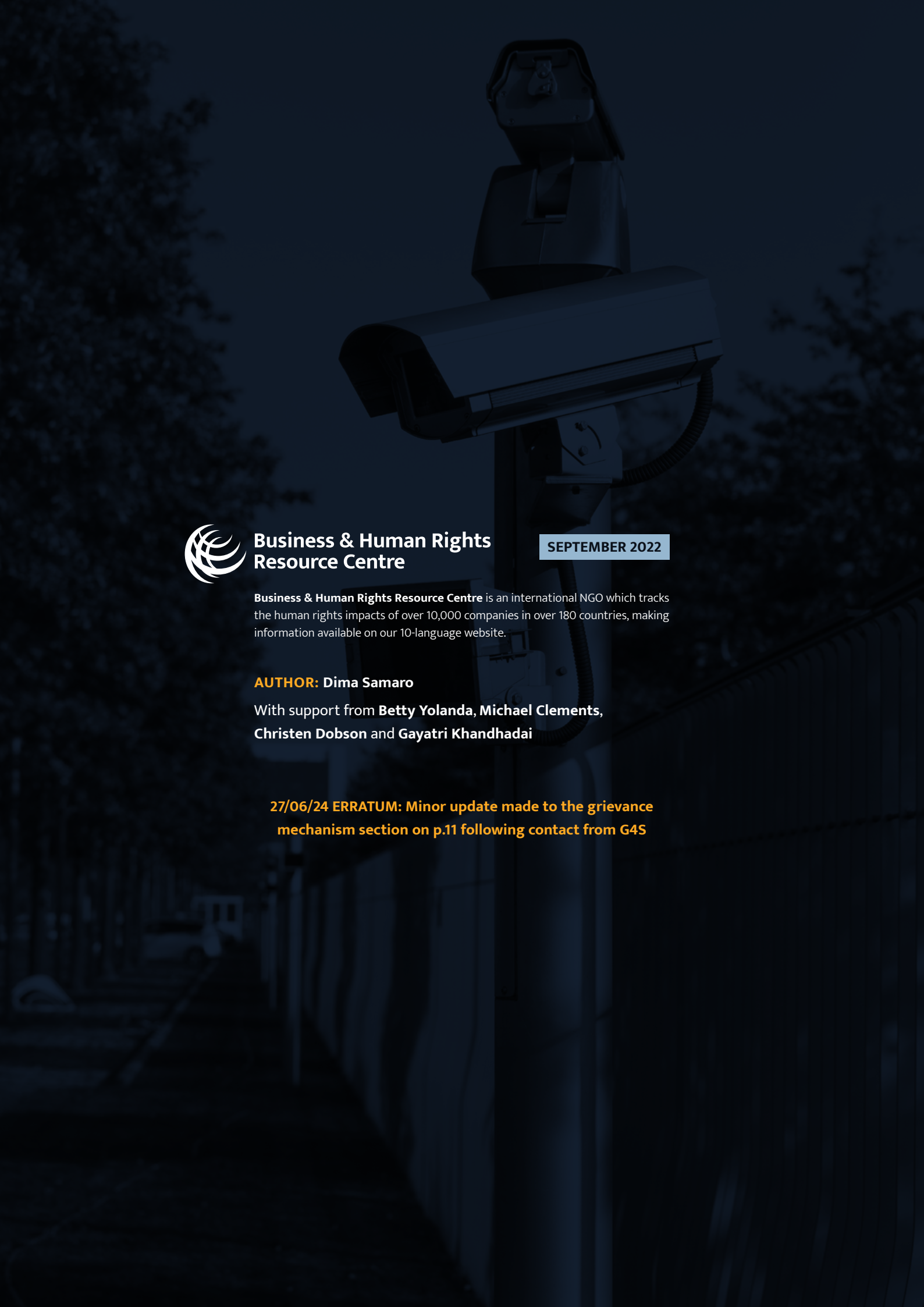
For investors:

- Strengthen and publish human rights policies in line with the UNGPs, including requiring investee companies to carry out robust human rights due diligence, with heightened due diligence for operations in conflict-affected areas.
- Review engagement with companies which provide authoritarian governments in the MENA region with surveillance tools and products, unless they have evidence the company's human rights compliance system is sufficient to address human rights risks.

Annex:

List of tech companies approached to answer survey questions

1. Safran Group
2. Cellebrite
3. IrisGuard
4. Airbus
5. Israel Aerospace Industries (IAI)
6. Elbit Systems
7. Sovereign Global UK
8. Nexa Technologies
9. Elettronica Mangione (Elman)
10. Dassault
11. G4S
12. AnyVision
13. TSG IT Advanced Systems
14. VideoTec
15. Evron Systems Ltd.
16. Dahua Technology
17. Sony
18. GEM Security Services Ltd.
19. Leonardo
20. Cisco
21. Indra
22. Thales Group
23. IDEMIA
24. BAE Systems



Business & Human Rights Resource Centre

SEPTEMBER 2022

Business & Human Rights Resource Centre is an international NGO which tracks the human rights impacts of over 10,000 companies in over 180 countries, making information available on our 10-language website.

AUTHOR: **Dima Samaro**

With support from **Betty Yolanda**, **Michael Clements**, **Christen Dobson** and **Gayatri Khandhadai**

27/06/24 ERRATUM: Minor update made to the grievance mechanism section on p.11 following contact from G4S