Remote biometric surveillance in Latin America

Are companies respecting human rights?

What we asked companies

In August 2021, Access Now, Asociación por los Derechos Civiles (ADC, Argentina), Laboratory of Public Policy and Internet (LAPIN, Brazil), and LaLibre.net (Ecuador) launched a report, "Surveillance Tech in Latin America - Made Abroad, Deployed at Home," highlighting the sale and use of remote biometric surveillance technologies in the region. Ahead of publication, we gave all the companies concerned an opportunity to share their input. None opted to do so.

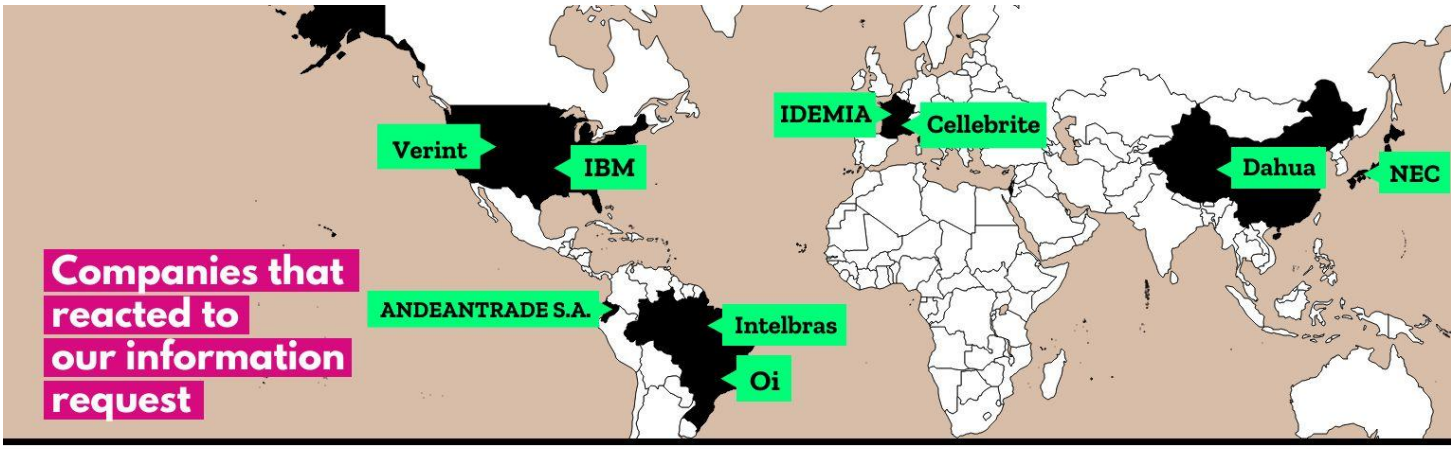
In 2022, Access Now extended its work on this topic, launching the #PorQuéNosVigilan (why they watch us) campaign on the dangers of mass surveillance technology deployed in countries across Latin America. Access Now also partnered with the Business and Human Rights Resource Centre to get answers from the companies that deploy technology with surveillance capabilities in the region. As a result, nine of the 23 companies we had mentioned in our 2021 report reacted, while the remaining 14 stayed silent.

The limited responses we received did little to clarify the scope of the technology with surveillance capabilities deployed in the region; most of the companies provided only a general answer, rather than answering each of our specific questions. We also noted that some responses suggest that the companies are not in compliance with the United Nations Guiding Principles on Business and Human Rights (UNGPs), notably when it comes to commitments on respecting human rights, conducting due diligence to identify and prevent salient human rights harms, and openly providing information about how the companies are enforcing applicable laws.

Companies must communicate openly and transparently with the public about steps taken to address the impact their activities may have on human rights, particularly when concerns are raised, directly or indirectly, by impacted communities or individuals. Staying silent on such issues is a way of avoiding accountability and making it harder for independent experts to assess their activities.

The following paper reviews the responses we received and the extent to which the information provided aligns with the UNGPs.

Companies that responded to our request of information



- **ANDEANTRADE S.A**
- BGH Tech Partner
- **Cellebrite**
- **Dahua**
- Danaide
- El Corte Inglés
- Full Tecnología FullTec CIA. LTDA
- Hikvision
- Huawei
- IAFIS Argentina S.A
- **IBM**
- **Idemia (former Morpho)**
- **Intelbras**
- Johnson Controls
- **NEC**
- **Oi**
- Oosto (former Anyvision)
- RC International
- Security Team Network S.A
- Unión Eléctrica S.A.
- Unitech S.A
- **Verint***
- ZTE

Companies that responded.
Companies that did not respond.

* Verint's answer only informed that their "cyber security business is now a standalone independent public company called Cognyte Software Ltd." We contacted Cognyte, who originally was open to talk, but then they never confirmed a date.

The underlying problems with the companies' answers

In the answers we received we identified several recurring patterns:

1. Dodging accountability by mischaracterizing their products

Cellebrite pushed back against the characterization of their products as surveillance tools, describing them instead as "digital intelligence solutions" used in investigations by law enforcement. By failing to acknowledge that surveillance is a salient human rights risk of their service offering, these companies cannot conduct proper due diligence to identify and prevent human rights impact, as required by the UNGPs.

Meanwhile, **IDEMIA** (formerly Morpho) denied having "any type of surveillance technology in Argentina, Brazil or Ecuador." They said that the systems used by the company "in these countries are for the use of biometric identification for forensic practice" – a claim contradicted in information shared by the authorities.

In fact, Argentinian Law Enforcement Agencies began using Morpho products before 2010, and IDEMIA is responsible for installing and establishing the Ministry of Security's Automated Fingerprint Identification System (AFIS). Nowadays, their technology is in use across Argentina, such as in the cities of Campana, Luján, Balcarce, Córdoba, Chaco, and multiple towns in the Province of Buenos Aires.

Overall, IDEMIA's response ignores the reality that technology allowing remote biometric recognition *is* surveillance technology, and it can cause or contribute to negative human rights impacts. The company chose to dispute specific facts and misinterpreted our findings, such as trying to clarify that Morpho RapID uses fingerprints, when our report says the same, and it is biometric data.

In their short responses, neither Cellebrite nor IDEMIA mentioned human rights at all, let alone their corporate responsibility to respect these rights. This directly contravenes Principle 11 of the UNGPs: "Business enterprises should respect human rights. This means that they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved."

2. Deflecting their responsibility onto other actors

Several of the companies tried to distance themselves from their partners' actions. **Andeantrade**, a provider of Hikvision products, focused their response on public procurement aspects and did not provide us with information about human rights threats. Apparently seeing our information request as a liability issue, they did not address any human rights risks, and used the fact that they are providers, not users, of the technology to distance themselves from any impact the products might have.

Brazilian company **Intelbras** shared detailed answers to both our original and our follow-up questions. While they did reiterate the importance of complying with data protection laws, they underestimated the relevance of their business relationship with Dahua, the Chinese company that owns 10% of their business. Intelbras stated that "it has no connection or responsibility for the actions of the Chinese company," but as a shareholder, a Dahua representative sits on Intelbras's board of directors. This means that Dahua has a responsibility to ensure that its investment in Intelbras does not contribute to human rights harms, just as Intelbras must make sure human rights are respected within its business operations.

Brazilian company **Oi** (formerly Telmar) and **Intelbras** both argued that end users (their customers) are solely responsible for how their products or services are used. Meanwhile, **Dahua** said they "cannot fully control how [their] technologies are ultimately used by end users." This narrative ignores the fact that corporate responsibility extends throughout a business' value chain, with UNGP 13 (b) stating that enterprises must "[s]eek to prevent or mitigate adverse human rights impacts that are directly linked to their operations, products or services by their business relationships, even if they have not contributed to those impacts."

Operationally, companies' due diligence efforts must consider the human rights impacts, not only of their products but also of any related activities (UNGP 17 (a)). When companies fail to accept responsibility for harms caused by the technology they create, they limit the ability to protect the privacy of people affected by tools with surveillance capabilities.

3. Caring for clients, but not for impacted people

Oi's answer focused on how they have developed products and services in line with digital transformation and market trends, but failed to mention how they protect human rights. This contravenes the UNGPs' requirement for businesses to make a policy commitment to respect human rights (UNGP 15) and to publicly communicate how they address the human rights impacts of their products or services (UNGP 21).

Intelbras supplied information on the pre- and post-sales support they provide to clients and installers, as well as their commitment to notify "the user and the competent authorities" if there is an "incident involving the Personal Data of users of the Services." However, the real risks posed by technologies with surveillance capabilities is not to the clients deploying them, but to the individuals exposed to these technologies. So the real issue at hand is how the companies would limit government clients, especially those with human rights violations records. Yet Intelbras disregarded this in their answer, suggesting they have not assessed the human rights impacts of their business, as required by UNGP 18.

4. Being overconfident in their own internal policies, despite lack of transparency

In response to our question about any policies, protocols, or internal processes governing the companies' provision of surveillance solutions to governments, several companies referred to

their licensing and data privacy policies, product terms of use, and code of ethics, as well as to local regulations. While internal policies are a starting point for legal compliance, they are not sufficient to guarantee the protection of human rights. As UNGP 16 points out, “business enterprises should express their commitment to meet this responsibility.”

For instance, **Oi** shared that “it operates in all its operations and projects observing the highest levels of governance, integrity, corporate ethics and respect for all applicable laws and regulations.” Yet they failed to mention engaging with human rights or international standards.

Cellebrite provided an answer through a public relations firm, with their short response describing the type of products sold and stating that the company has “strict licensing policies and restrictions to govern how customers utilize [their]solutions, and [they] only sell [their] technology to companies, organizations, and agencies that agree to abide by the strict licensing policies that govern its proper use." However, the company provided no details of those policies, leaving civil society unable to monitor or verify the company’s adherence with their commitments.

IBM said they employ “rigorous processes across [their] global operations to protect against direct or third-party business engagements that may run counter to these commitments." Although their full answer lays out clear commitments in line with the UNGPs, such as condemning the use of technology for mass surveillance and racial profiling, the company shared no information on what these processes are, preventing us from conducting a full and thorough analysis.

NEC has gone one step further, in creating the NEC Group AI and Human Rights Principles to “demonstrate respect for privacy and human rights in relation to the application and utilization of AI and biometrics data across all businesses.” However, while their group does assess whether their products are being used to abuse human rights, there is no mention of any channel for reporting alleged human rights abuses, nor did they provide details on how any violations are assessed and addressed (UNGP 20). Adherence to human rights must go beyond a working group or a charter of principles.

In short, the companies referred us back to internal policies and principles, codes of ethics, or working groups – but failed to provide either details of these various mechanisms or detailed information about how they are implemented or monitored (UNGP 20).

Full, detailed, and ongoing transparency is crucial for the adequate protection of human rights, particularly when it comes to public-private partnerships enabling surveillance technology to be deployed. States have a duty to protect human rights, while companies must respect them. Companies must therefore comply with transparency and human rights due diligence standards, and provide enough information for civil society and other independent actors to hold them accountable.

Access Now

www.accessnow.org

Access Now defends and extends the digital rights of people and communities at risk. As a grassroots-to-global organization, we partner with local actors to bring a human rights agenda to the use, development, and governance of digital technologies, and to intervene where technologies adversely impact our human rights. By combining direct technical support, strategic advocacy, grassroots grantmaking, and convenings such as RightsCon, we fight for human rights in the digital age.

For more information, please contact:
Ángela Alarcón
Campaigner, Latin America & the Caribbean
angela@accessnow.org