



accessnow

EMAIL SENT TO COMPANIES

Dear XXXX representatives,

My name is Gaspar Pisanu. I'm the Latin American Advocacy/Policy Manager at Access Now, an organization dedicated to extending and protecting human rights in the digital era.

More than a year ago we and XXXX (Local Partner), contacted you to obtain information about the selling and deployment of XXXXX technology in XXXXX (Country). Since then, we have had no response from you and have published the following [report](#) and educated the public on these issues through a [campaign](#).

Your silence on a topic that impacts the privacy rights of people throughout Latin America signals a lack of transparency that is at odds with responsible business practice. Beginning a dialogue with civil society is an important step in demonstrating that you take respect for human rights seriously.

We are making a final attempt to get a response to these questions:

1. Does your company distribute surveillance solutions to governments in Latin America? If so, which products and to which states in Latin America? Which of your surveillance solutions products and services are most widely distributed in Latin America?

2. Do third-party companies resell your surveillance solutions to Latin America states? If so, who are your resellers?

3. Do you or your resellers have contracts or agreements with Latin American governments to provide surveillance solutions? What do these agreements look like and what technologies are involved?

-
4. What kind of support do you provide to your clients after distributing your surveillance solutions?

 5. Do you or your resellers have access to data collected in any country in Latin America? If yes: What are the characteristics of that data? According to your privacy policy, could that data be shared with any third parties or companies in the same corporate group?

 6. Do you have a policy, protocol, or internal process governing your provision of surveillance solutions to governments? Do you do an assessment of the authority's human rights violations records before closing the agreements? Under what circumstances would you limit or restrict your provision of surveillance solutions to government clients?

We hope to hear from you and are happy to answer any questions you may have.

Sincerely,

COMPANIES ANSWERS

— Cellebrite

From: Jacqueline [REDACTED]
Date: Mon, May 16, 2022 at 2:49 PM
Subject: RE: Access Now - [Invitation to answer] Surveillance technology in Argentina
To: gaspar@accessnow.org <gaspar@accessnow.org>

Gaspar,

Thank you for your inquiry. I work for Reevemark, Cellebrite's PR firm. In response to your inquiry, please see below. This information is also on Cellebrite's [website](#).

Cellebrite is not an offensive cyber-technology company, and we do not produce technology solutions that support surveillance or monitoring efforts. It is important to make a distinction between the "surveillance and monitoring technologies" that are predictive and come into play before an event occurs and Cellebrite's Digital Intelligence solutions, which are used lawfully and with a warrant to help federal government agencies and law enforcement investigate an event after it has taken place. Further, Cellebrite has strict licensing policies and restrictions to govern how customers utilize our solutions, and we only sell our technology to companies, organizations, and agencies that agree to abide by the strict licensing policies that govern its proper use.

Thank you for reaching out; please let me know if you have any questions.

Best regards,
Jacqueline

From: Gaspar Pisano <gaspar@accessnow.org>
Date: Thu, Jun 2, 2022 at 11:24 AM
Subject: Re: Access Now - [Invitation to answer] Surveillance technology in Argentina
To: Jacqueline [REDACTED]
Cc: Angela Alarcón <angela@accessnow.org>, Isedua Oribhabor <isedua@accessnow.org>

Dear Jacqueline,

Thanks for your response and for pointing us to the resources on Cellebrite's website. Cellebrite's [corporate responsibility commitment](#) is remarkable but an important part of adhering to that commitment under the [UN Guiding Principles on Business and Human Rights](#) is providing transparency through meaningful engagement with stakeholders to understand the real world impacts of your products and services.

As we mentioned in our previous outreach, this topic touches on the human rights of people throughout the Latin America region and we would appreciate the opportunity to speak with the Cellebrite team in more detail about how they enforce their policies and about the impacts we as civil society see on human rights.

Please let me know if you have any questions. Can we arrange a time to talk with the Cellebrite team in the coming weeks? Our Business & Human Rights Lead, Isedua, is copied here.

Best regards,

From: Jacqueline [REDACTED]
Date: Fri, Jun 3, 2022 at 9:57 AM
Subject: RE: Access Now - [Invitation to answer] Surveillance technology in Argentina
To: Gaspar Pisano <gaspar@accessnow.org>
Cc: Angela Alarcón <angela@accessnow.org>, Isedua Oribhabor <isedua@accessnow.org>

Gaspar,

Thank you for your note. We appreciate your interest, but we are not able to accommodate your request to arrange a conversation with the Cellebrite team.

Best regards,
Jacqueline

— Dahua

From: PR_Global <PR_Global@dahuatech.com>
Date: Mon, May 16, 2022 at 12:05 AM
Subject: 答复: Access Now - [Invitation to answer] Surveillance technology in Brazil
To: Gaspar Pisani <gaspar@accessnow.org>
Cc: Angela Alarcón <angela@accessnow.org>

Hi Gaspar,

Thanks for reaching out to Dahua Technology (hereinafter referred to "Dahua" or "Dahua Technology"). To our knowledge, our employees in Brazil have never heard from Access Now in the past year. However, Dahua recognizes and understands the concerns of our stakeholders about the challenges facing the surveillance industry. Regarding your questions and report, we would like to share our understanding and commitment in this regard.

Emerging technologies like artificial intelligence and surveillance technology are playing important roles in advancing the developments of human society and promoting the safety, security, and prosperity of human beings. At the same time, it is an industry challenge to work to appropriately manage and regulate applications which carry with them potential risks. This requires close international cooperation from all stakeholders.

At Dahua Technology, we attach great importance to this task, which rests equally on our ethics and our compliance processes. We established an ethics and compliance management committee precisely for this purpose. We design our products, services and solutions to help make the world safer and more secure. Our technologies enable families and businesses to detect and respond to safety and security risks more quickly, accurately and effectively than ever before. They also provide value-add beyond security, such as enabling cities, businesses, and other organizations to incorporate the visual data captured on our cameras as part of their "smart" solutions for everything from reducing traffic congestion, wildlife monitoring, tracking waste streams, to enhancing sales at retail outlets.

Like any other security solutions company in the world, we cannot fully control how our technologies are ultimately used by end users. We need and expect our end users to comply with all applicable local, national and international laws, regulations and conventions, just as we do. We accept our responsibility to design our technologies in ways that mitigate the risk of abuse. This includes a commitment to never develop solutions to identify a single ethnic, racial or national group. That commitment extends to every market in which we operate, anywhere in the world.

As you know, cybersecurity is the global challenge in the digital era and vulnerabilities are discovered in the products manufactured by any technology company in the world. Dahua maintains extremely high standards to protect the security and privacy protections of its customers' data, and has developed and rigorously applies industry best practices related to data protection in all of our solutions and products. Moreover, the company has established audit and certification cooperation with a number of international security institutions, including British Standards Institution (BSI), Bureau Veritas (BV), TÜV Rheinland, Intertek EWA-Canada as well as many others. While complying with applicable laws and regulations such as GDPR, Dahua's capability in product security and corporate cybersecurity management has been certified by ISO/IEC27001, ISO/IEC 27701, FIPS 140-2, ETSI EN 303645, ETSI TS103645 and other global standards.

At the same time, we strongly encourage our partners, customers and end users to conduct regular firmware updates and maintenance during the product life cycle, and report to us any vulnerability discovered on any Dahua devices. Dahua Cybersecurity Center is committed to handling all cases with transparency and speed in line with industry best practices and international standards.

Regards,
Dahua Technology

— IBM

From: Sarah [REDACTED]
Date: Fri, Jun 10, 2022 at 2:28 PM
Subject: Your IBM Inquiry
To: gaspar@accessnow.org <gaspar@accessnow.org>, veronica@accessnow.org <veronica@accessnow.org>, angela@accessnow.org <angela@accessnow.org>

Hi Gaspar, Veronica, and Angela –

Your inquiry to IBM about the Surveillance Tech in Latin America report made its way to me.

Feel free to use the following comment from IBM:

"IBM opposes and does not condone the use of technology for mass surveillance, racial profiling, violations of basic human rights and freedoms, or any purpose that conflicts with the company's values, principles and commitment to the responsible stewardship of technology. We employ rigorous processes across our global operations to protect against direct or third-party business engagements that may run counter to these commitments."

"Further, IBM no longer supplies technology to the Intelligent Operations Center in Davao and has not done so since 2012. We never supplied facial recognition capability for the center. IBM divested the i2 product portfolio in December 2021."

Thank you and enjoy the weekend.



— VERINT

Due to a confidentiality note in Verint's email, Access Now is not able to share their response. But we can confirm it was a pretty short message indicating that the portion of their business related to Access Now's querie is part of Cognyte Software Ltd. since Frebruary 2021.