Congress of the United States
Washington, DC 20515

June 11, 2021

Gary Gensler
Chairman
U.S. Securities and Exchange Commission
100 F St NE, Washington, DC 20549

Chairman Gensler,

I write today to alert you to deep and persistent concerns about the human rights record of digital forensic company Cellebrite, scheduled for a de-SPAC and NASDAQ listing. Cellebrite has an established pattern of selling their data extraction devices to repressive governments and security forces around the world, where they have been linked to the abuse of journalists, lawyers, political opposition leaders, and peaceful civil society activists. As such, I ask that you **deny approval of the SPAC's proxy statements and Cellebrite's Form F-4** unless the company transparently addresses severe human rights risks linked to their products and potential exports, including a complete accounting of past sales and enforceable commitments to strengthened human rights due diligence.

Cellebrite's flagship product, the UFED (Universal Forensic Extraction Device), allows law enforcement and intelligence agencies to extract data, including messages, files, call logs, deleted files, and other information from locked mobile phones and other devices. According to Cellebrite's Co-CEO Yossi Carmil, "with our capabilities, you can extract almost everything from the smartphone - open, hidden or deleted information."[i] While many of Cellebrite's clients use the devices for legitimate investigative purposes, the company has demonstrated a consistent disposition to sell first and ask questions later. Reported abuses linked to Cellebrite's products include:

- **Hong Kong:** Cellebrite's tools have been used as recently as July 2020 by Chinese government security forces to hack into phones used by peaceful democracy activists, including Joshua Wong.[ii] [iii]
- **Saudi Arabia**: As recently as November 2019, Cellebrite reportedly sent an employee to Riyadh to hack into a phone at the request of the Saudi Justice Minister, despite widespread knowledge of the Saudi government's violent crackdown on dissidents, journalists, and activists.[iv]
- **Myanmar**: Police used Cellebrite extraction on the devices of Reuters journalists following their arrest and detention on politically-motivated charges.[v] Cellebrite's devices have also been linked to the military's recent crackdown that has resulted in the deaths of over 750 people.[vi]
- **Bahrain**: Police used Cellebrite UFEDs to strip data from the phones of human rights and political activists, compromising sensitive networks in a country noted for deep political repression, arbitrary detentions, and torture.[vii]
- **Russia**: Cellebrite devices have been used as part of widespread tracking and persecution of political opposition, ethnic minorities, LGBTQI+ activists, and rights defenders, including associates of Alexei Navalny.[viii]
- **Venezuela**: Cellebrite sold hacking tools to the Venezuelan government despite a US embargo. The company has since halted sales to the Maduro regime, but it has not provided transparency on when this stopped or if they have remotely disabled previously-transferred tools.[ix]

This selection of recent clients raises serious questions about the seriousness of Cellebrite's corporate safeguards on human rights. Security forces in most of these countries have had dark human rights records for a number of years, as covered by robust public reporting. While Cellebrite stopped selling their tools to some countries accused of misusing their products, reports suggest that those governments still have access to their services and products.[x] The fact that they were sold in the first place to governments with a track record of human rights abuses and repressive tactics call into questions Cellebrite terms of sale, due diligence practices, and willingness to sell its technology to abusive governments. Moreover, Cellebrite only stopped selling its services to China and Hong Kong to comply with new US regulations restricting the transfer of surveillance technologies,[xi] and in other countries only after pressure and media reports revealed the company's shortcomings.

Given these concerning trends, I urge you to **deny approval of the SPAC's proxy statements and Cellebrite's Form F-4** until Cellebrite takes the following steps as part of a thorough accounting to the SEC of heightened *risk factors* under 17 CFR § 229.503:

1. Provides a public accounting and remediation plan for Cellebrite's past sales to governments and entities with clearly established patterns of human rights abuse.
2. Provides a public accounting of likely continued use of Cellebrite products by governments and security agencies linked to human rights abuse and makes a public statement on the ability of the company to shutoff or terminate any such agreements and servicing of products.
3. Works with civil society and human rights stakeholders to develop and publicly vet a new human rights compliance system and policy that would have prevented sales such as those noted above, informed by the United States Department of State's *Guidance on Implementing the UN Guiding Principles for Transactions Linked to Foreign Government End-Users for Products or Services with Surveillance Capabilities.*

Cellebrite has a clearly established track record of diminished concern for human rights abuse linked to their product exports. By following through with a *no-questions-asked* SPAC and NASDAQ listing, I am deeply concerned by the domestic mainstreaming of an *export first-ask questions later* attitude for digital surveillance and intrusion goods. This has acute implications for US national security interests linked to secure communications for journalists, human rights activists, and democracy defenders worldwide—under increasing pressure from authoritarian regimes. Thank you for your consideration of this urgent request.

Respectfully,

Tom Malinowski
Member of Congress

[i] Shahaf, Tal, "I sleep well at night because I know for whom I work and whom I serve," *Ynetnews*, November 4, 2019. https://www.ynetnews.com/articles/0,7340,L-5618901,00.html

[ii] Harkov, Lahav, "Hong Kong democracy activists to Israel: Stop exporting tech to police." *Jerusalem Post*, July 31, 2020. https://www.jpost.com/israel-news/hong-kong-democracy-activists-to-israel-stop-exporting-tech-to-police-636918

[iii] O'Neill, Patrick Howell, "Israeli phone hacking company faces court fight over sales to Hong Kong," *MIT Technology Review*, August 25, 2020. https://www.technologyreview.com/2020/08/25/1007617/israeli-phone-hacking-company-faces-court-fight-over-sales-to-hong-kong/

[iv] Megiddo, Gur, "Revealed: Israeli Firm Provided Phone-hacking Services to Saudi Arabia," *Haaretz*, September 16, 2020. https://www.haaretz.com/israel-news/tech-news/.premium-revealed-israeli-firm-provided-phone-hacking-services-to-saudi-arabia-1.9161374

[v] McLaughlin, Timothy, "Security-tech companies once flocked to Myanmar. One firm's tools were used against two journalists," *Washington Post*, May 4, 2019. https://www.washingtonpost.com/world/asia_pacific/security-tech-companies-once-flocked-to-myanmar-one-firms-tools-were-used-against-two-journalists-/2019/05/04/d4e9f7f0-5b5d-11e9-b8e3-b03311fbbbfe_story.html

[vi] Beech, Hannah, "Myanmar's Military Deploys Digital Arsenal of Repression in Crackdown," *New York Times*, March 1, 2021. https://www.nytimes.com/2021/03/01/world/asia/myanmar-coup-military-surveillance.html

[vii] Biddle, Sam & Desmukh, Fahad, "Phone-Cracking Cellebrite Software Used to Prosecute Tortured Dissident," *The Intercept*, December 8, 2016. https://theintercept.com/2016/12/08/phone-cracking-cellebrite-software-used-to-prosecute-tortured-dissident/

[viii] Yaron, Oded, "Putin Investigators Targeting LGBTQs, Navalny, Use Israeli Phone-hacking Tech," *Haaretz*, September 23, 2020. https://www.haaretz.com/israel-news/tech-news/.premium-putin-investigators-targeting-lgbtqs-navalny-use-israeli-phone-hacking-tech-cellebrite-1.9179191

[ix] Yaron, Oded, "Despite Sanctions, Israeli Firm Cellebrite Sold Phone-hacking Tech to Venezuela," *Haaretz*, September 10, 2021. https://www.haaretz.com/israel-news/tech-news/.premium-despite-sanctions-israeli-firm-sold-phone-hacking-tech-to-venezuela-1.9144879

[x] McLaughlin, "Security-tech companies," *Washington Post*, May 4, 2019.

[xi] Cellebrite Press Release, "Cellebrite to Stop Selling Its Digital Intelligence Offerings in Hong Kong & China," October 7, 2020. https://www.cellebrite.com/en/cellebrite-to-stop-selling-its-digital-intelligence-offerings-in-hong-kong-china/