

**Congress of the United States**  
**Washington, DC 20515**

June 11, 2021

Adam H. Clammer  
Chief Executive Officer  
TWC Tech Holdings II Corp.  
Four Embarcadero Center, Suite 2100  
San Francisco, CA 94111

Mr. Clammer,

I write today with urgent concern over unresolved human rights risks linked to the sales history of Cellebrite, for which you are handling a forthcoming de-SPAC and NASDAQ listing. Cellebrite has an established pattern of selling data extraction devices to the world's most repressive security forces around the world—including in **China, Saudi Arabia, Bahrain, and Russia**—where they have been linked to the abuse of journalists, lawyers, political opposition leaders, and peaceful civil society activists. As such, **I urge you to immediately delay moving forward with this proposed listing until Cellebrite has taken credible steps to publicly demonstrate that their business model can tolerate a dramatic elevation of human rights risks in sales and export review processes.** I have also expressed these concerns to the U.S. Securities and Exchange Commission, NASDAQ, and investors, urging them to prohibit or reconsider Cellebrite's listing absent more meaningful commitments to human rights.

As you well know, 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 sensitive information from locked mobile phones and devices. According to Cellebrite's own Co-CEO Yossi Carmil, "with our capabilities, you can extract almost everything from the smartphone - open, hidden or deleted information."<sup>i</sup> 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.<sup>ii iii</sup>
- **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.<sup>iv</sup>
- **Myanmar:** Police used Cellebrite extraction on the devices of Reuters journalists following their arrest and detention on politically-motivated charges.<sup>v</sup> Cellebrite's devices have also been linked to the military's recent crackdown that has resulted in the deaths of over 750 people.<sup>vi</sup>
- **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.<sup>vii</sup>
- **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.<sup>viii</sup>

- **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.<sup>ix</sup>

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.<sup>x</sup> The fact that they were sold in the first place to governments with a track record of severe human rights abuses and repressive tactics call into questions Cellebrite terms of sale, due diligence practices, corporate priorities, and forthrightness through export licensing application processes. Moreover, Cellebrite only stopped selling its services to China and Hong Kong to comply with new US regulations restricting the transfer of surveillance technologies<sup>xi</sup>, and in other countries only after concerned pressure and media reports revealed the company's aggressive sales to abusive governments.

Cellebrite's clearly established track record of diminished concern for human rights abuse linked to their exports justifies an **elevated degree of skepticism toward their stated commitments to a completely different approach to evaluating human rights risks**. Therefore, I urge you to immediately **signal your intention to delay this proposed listing until the company takes the following actions:**

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. Works with civil society and human rights stakeholders to publicly vet a new human rights compliance system and policy that would have prevented sales such as those noted above, including credible and public commitments to implementing 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*.
3. Provides publicly-listed conditions on the uses of their items that would violate contract terms and result in suspension for all future sales (eg. use against opposition politicians, journalists, or peaceful activists).
4. Commits to including remote shutdown or clawback mechanisms in all products where possible to disable devices and services and suspend contracts without cost when clients violate clearly established and publicly-listed human rights abuse thresholds.

Thank you for your consideration of this urgent request.

Respectfully,



Tom Malinowski  
Member of Congress

- 
- <sup>i</sup> 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>
- <sup>ii</sup> 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>
- <sup>iii</sup> 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/>
- <sup>iv</sup> 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>
- <sup>v</sup> 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-b03311fbbbf\\_story.html](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-b03311fbbbf_story.html)
- <sup>vi</sup> 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>
- <sup>vii</sup> 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/>
- <sup>viii</sup> 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-lgbts-navalny-use-israeli-phone-hacking-tech-cellebrite-1.9179191>
- <sup>ix</sup> 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>
- <sup>x</sup> McLaughlin, “Security-tech companies,” *Washington Post*, May 4, 2019.
- <sup>xi</sup> 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/>