Congress of the United States
Washington, DC 20515

June 11, 2021

Glen Kacher
President, CIO
Light Street Capital
525 University Avenue, Suite 300
Palo Alto, CA 94301

Paul J. Glazer
Managing Member
Glazer Capital, LLC
Four Embarcadero Center, Suite 2100,
San Francisco, CA

Mike McCaffery
Chairman, Executive Committee
Makena Capital Management
2755 Sand Hill Road, Suite 200
Menlo Park, CA 94025

Rick Smith
Chief Executive Officer
Axon Enterprise
17800 N. 85th St
Scottsdale, AZ 85255

Kenneth Griffin
President, Chief Executive Officer
Citadel GP LLC
131 Dearborn St, 32nd Floor
Chicago, IL 60603

Ari Zweiman
Managing Member
683 Capital Management, LLC
3 Columbus Circle, Suite 2205
New York, NY 10019

Andrew Weiss
Managing Member
Weiss Asset Management LP
222 Berkeley St, 16th floor
Boston, MA 02116

Amos Meron
Managing Member
Empyrean Capital Partners
10250 Constellation Boulevard, Suite 2950
Los Angeles, CA 90067

Israel A. Englander
Chairman, CEO, and Co-CIO
Millennium Management LLC
666 Fifth Avenue
New York, NY 10103

Mendel Hui
Managing Member
Isomer Partners Fund GP LLC
420 Lexington Avenue, Suite 2007
New York, NY 10170

Peter Sang Hun Park
Chief Investment Officer
Park West Asset Management LLC
900 Larkspur Landing Circle, Suite 165
Larkspur, CA 94939

Michael Stark
Managing Member
Crosslink Capital, Inc
2180 Sand Hill Road, Suite 200
Menlo Park, CA 94025

Douglas K Edwards
Managing Member
Crescent Park Management, LP
1900 University Avenue, Suite 501
East Palo Alto, CA 94549

Hunter Armistead
Managing Member
Alaris Capital LLC
4900 Main Street, Suite 600
Kansas City MO 64112

Alex Lazovsky
Managing Member
West Coast Equity Partners LLC
703 Crestview Dr
San Carlos, CA 94070

Gentlemen,

I write today to alert you to deep and persistent concerns about the human rights record of digital forensic company Cellebrite, for which you are listed as primary investors for a forthcoming de-SPAC and NASDAQ listing. Cellebrite has an established pattern of selling data extraction devices to the 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 reconsider investing in Cellebrite until the company has taken credible public steps to elevate human rights risks in their sales and export review processes.** I have also expressed these concerns to the U.S. Securities and Exchange Commission and NASDAQ.

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."[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 were 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 corporate priorities. 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 highlighted the company's aggressive sales to abusive governments.

Given these concerning trends and in light of the company's clearly established track record of diminished concern for human rights abuse linked to their product exports, I urge you to **withdraw your intention to purchase shares in Cellebrite's proposed listing,** and for those who own shares in TWC Tech Holdings II Corp, to vote against the proposed merger and redeem those shares. If the company and its SPAC shareholders are serious about turning a corner, investors should expect to see Cellebrite take each of the following actions:

1. Provide a public accounting and remediation plan for Cellebrite's past sales to governments and entities with clearly established patterns of human rights abuse.
2. Work 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. Provide 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. Commit 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.

By following through with a *business-as-usual* SPAC and NASDAQ listing, I am concerned by the domestic mainstreaming in the United States of an *export first-ask questions later* attitude toward digital surveillance and intrusion goods. Bringing a company with Cellebrite's human rights record into mainstream investment circles could indelibly reshape the industry's values (and reputations)[xii]. While **journalists, human rights activists, and democracy defenders are under pressure from authoritarian regimes around the world, I believe it could undermine American national security interests to further empower a company providing repressive governments the tools to hunt down and undermine secure communications for these citizens.** 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 HoIll, "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/

[xii] Rights Groups: NSO Group Continues to Fail in Human Rights Compliance, April 27, 2021. https://www.amnesty.org/download/Documents/DOC1040362021ENGLISH.PDF