June 22, 2026

Thomas Hogan
Chief Executive Officer
Cellebrite

Ronnen Armon
Chief Products and Technologies Officer
Cellebrite

Sigalit Shavit
Chief Information Officer
Cellebrite

Dear Mr. Hogan, Mr. Armon, and Ms. Shavit,

We are writing to you because The Citizen Lab, an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, University of Toronto, has uncovered that Cellebrite's products have been used by the Russian government against Andrey Pivovarov.

Pivovarov is a prominent Russian activist, opposition figure, and a former political prisoner, released as a result of the U.S.-negotiated prisoner exchange. Using Cellebrite technology, the Russian authorities collected the data as part of their politically motivated criminal case against Pivovarov, resulting in his conviction in July 2022. This conviction was widely condemned by democratic governments and human rights organizations as arbitrary and illegal.

According to the forensic report prepared by the Forensic Expert Center of the Russian Ministry of Interior (MVD), working at the behest of the Investigative Committee, which led the criminal case against Pivovarov, Russian Cellebrite's UFED 4PC device and UFED Physical Analyzer software were used to extract and analyze data from three Pivovarov's phones, one MacBook, and six SIM cards between June and July of 2021. The Citizen Lab's forensic analysis also found with high confidence forensic traces of Cellebrite's tool on Pivovarov's iPhone on or around June 17, 2021, three months after the company said it was ending sales to Russia "immediately."

The evidence uncovered in the aforementioned investigation, previous investigations by Russian human rights organization First Department as well as investigative media including Haaretz, Mediazona, and Intercept, suggest that Russia and other authoritarian governments are able to use Cellebrite's devices long after the contracts are cancelled.

In the light of this investigation, we request that Cellebrite answer the following questions:

1. Were you aware that the Russian government, including the Ministry of Internal Affairs and the Investigative Committee whose officials have been sanctioned by the U.S., UK, and EU authorities, continued to use Cellebrite's devices and software after your March 18, 2021 announcement that you would halt sales to the country?
2. Is the use of your products uncovered by our investigation in line with the "proper use," as outlined in your End-User Licensing Agreement (EULA) and Ethics policies?
3. What actions do you plan to take in response to our findings?
4. What is your response to allegations that your products have been widely employed to target peaceful activists, protesters, union leaders, human rights lawyers, journalists, and civil society members in countries around the world, including after you allegedly ended the business relationships with governments in some of those countries?
5. What measures do you have in place to ensure that your products are not misused by governments or other entities in a manner that is "incompatible with privacy rights or human rights" or in violation of U.S. and international sanctions after they have been sold?
6. Do you have any technical measures in place to track and stop product misuse of your products? If so, please explain in detail how these technical measures work in practice. Can you provide specific examples of when you have activated such a technical measure and why?
7. Has the "disabling code" feature outlined in some of your publicly available EULA versions been applied to the UFED devices sold to the Russian government or in other situations of product misuse or unauthorized third-party re-sales? Has this measure been effective at stopping future use of the products?
8. Can you describe the due diligence process that you follow before selling your product to a government, organization, or law enforcement agency? In particular, can you outline the "internal parameters and vetting procedures, which consider a potential customer's human rights record and anti-corruption policies" that you rely on in your assessment?
9. Do you have any policies or guidelines that explicitly prohibit the use of your products against human rights activists, journalists, and democratic opposition members?
10. What steps are you taking to prevent the future misuse of your products?

We also urge you to take the following measures to prevent future harms and misuse:

- Conduct robust, ongoing human rights due diligence, in consultation with civil society, before and after the sale of forensic extraction tools, to identify and mitigate adverse human rights impacts and to ensure that the tools are not abused;
- Refrain from providing tools to actors with a history of abusing similar technologies;
- Ensure immediate cessation of existing contracts and future sales to customers that have been credibly accused of abusing the technologies;
- Implement both legal and technical measures to prevent future abuses, such as contract clauses that explicitly prohibit the use of the technologies in violation of human rights law and provide for the revocation or restriction of access to the tool in case of abuse, and "killswitches" that immediately disable technologies and prevent future updates;

- Ensure tools and technologies are forensically discoverable to enable victims whose devices were unlawfully accessed to challenge these abuses in courts;
- Provide remedies to affected people and groups through investing in victim funds and engaging with experts and communities impacted by the technology; and
- Refrain from retaliating against victims, civil society, and researchers who expose the abuses of the technologies.

We would appreciate your answer by **June 24, 2026, 22:00 CEST**.

Sincerely,

Access Now

Ronald J. Deibert, O.C., O.Ont, Director, The Citizen Lab, Professor of Political Science Munk School of Global Affairs & Public Policy