Cellebrite sent the following responses on Botswana to CPJ Senior Africa Researcher Jonathan Rozen on April 22, 2021.

When and under what circumstances was Cellebrite's technology provided to Botswana's police?

Please understand that we cannot speak to any specifics about our customers and their use of our technology. We can tell you that Cellebrite is the global leader in Digital Intelligence (DI), empowering public and private sector customers to manage DI in legally sanctioned investigations and modernize the investigative workflow. Digital Intelligence is the process and technology used to analyze and safeguard data, and Cellebrite's DI solutions equip customers with the tools they need to accelerate justice, save lives, and preserve data privacy. Cellebrite partners with public and private organizations to transform how they manage data in investigations to accelerate justice, preserve data privacy, and keep communities safe.

Is the use of Cellebrite's technology to extract information from journalists' devices considered an appropriate use of this technology? If not, what actions will your company take?

We have multiple checks and balances to ensure our technology is used as intended. We require that agencies and governments that use our technology uphold the standards of international human rights law. In the extremely rare case when our technology is used in a manner that does not meet international law or does not comply with Cellebrite's values, we take swift and appropriate action, including terminating agreements.

We work diligently to ensure our users understand and abide by their contractual obligations, in accordance with our license agreements and terms of use. Our compliance solutions enable an audit trail and can discern who, when and how data was accessed, which leads to accountability in the agencies that use our tools.

We take these steps for both ethical and business reasons. The law enforcement entities and businesses we work with need to know they're working with a company that cares about public safety and transparency.

Cellebrite's terms and conditions of sale have said that "Products or Software, or any Services or results of Service" are to be used "in a manner that does not violate the rights of any third party." Could you expand on what kind of rights this includes? Would

the right of a reporter engaging in legitimate journalism to protect their source be included? How does Cellebrite determine if rights have been violated?

Cellebrite's technology is no different than any other forensic or evidence gathering tool (such as DNA collection kits). There is nothing about our technology that makes it more capable of being misused than any other technology used by law enforcement. Further, Cellebrite carefully controls to whom it sells its technologies: law enforcement and government users which are obligated to follow Federal, State and Local laws. Cellebrite's technologies are not used for "on-the-wire" surveillance or intelligence gathering. Rather, Cellebrite is used by law enforcement to access data in accordance with due process (i.e., a warrant or appropriate equivalent depending on the jurisdiction) when there is probable cause.

We sell our digital intelligence solutions to government agencies, law enforcement and enterprises around the globe for their use to lawfully access and analyze legally obtained data to bring resolution to investigations, create a safer world and preserve privacy.

Does Cellebrite consider the human rights and press freedom records of countries before providing them with technology, including UFED? If so, what factors are considered?

We have strict criteria. There are the obvious criteria – of course, if a country is under sanction by Israel, the U.S., or the international community, we won't sell to them. We also examine a government's recent and long-term human rights record and look at any other factors that we consider restrictive in terms of giving them access to this type of technology.

We go through all of this for ethical reasons – but we do it for business reasons, too. The law enforcement entities and businesses we work with need to know they're working with a company that cares about public safety and the truth. They don't want to be using the same tools as dictators. Having governments on the "do not sell" list costs us millions of dollars every year but keeping such a list isn't just ethical – it's good business.

Can you comment on the use of your technology alongside alleged torture in an effort to extract information from Justice Motlhabani and Oratile Dikologang?

It is Cellebrite's protocol and policy to not comment on specific customers or uses of our technology. We sell our digital intelligence solutions to law enforcement agencies and authorized enterprises for their use in lawfully accessing and analyzing legally obtained data, to bring resolution to investigations and create a safer world.

Cellebrite has strong licensing policies in place that govern how our technology may be utilized. Additionally, we leverage leading compliance solutions to safeguard from transacting with restricted and denied parties worldwide.

CPJ has previously documented journalists' concerns that Cellebrite's technology can be used to access their private information, including about their sources. Can you comment on these concerns? Has Cellebrite taken, or does Cellebrite intend to take, any action to mitigate the risks your technology pose to journalists, their sources, and press freedom more broadly?

We do everything in our power to avoid such an outcome. We strive to guard against our products ending up in the wrong hands and we do not sell to governments who are likely to misuse our tools. Second, our terms of service spell out exactly how the tools we provide can – and cannot – be used. If governments are in violation of those terms, we reserve the right to demand they give back their equipment. Third, we are working on proprietary technological solutions to protect against this; for example, there are mechanisms in place on most of our devices to ensure they do not function past their expiration dates if not legally renewed. We cannot say more than this because the technology is proprietary.