THE ISRAELI COMPANY HACKING INTO YOUR LOCKED MOBILE PHONE

The use of military grade spyware by Australian government departments means our most personal data stored on our mobile phones – from financial details, contacts, and private photos, to an archive of messages and movements – is no longer secure.

by Antony Loewenstein | 31 May, 2023 | Israel, Palestine, surveillance

The Israeli surveillance company Cellebrite product, Universal Forensic Extraction Device (UFED), used to hack mobile phones across the world. Photo credit: Cellebrite.

From the provision of spyware and equipment, to electronic hardware and training programs, Israeli technology company Cellebrite is an integral part of Australia's security infrastructure.

A look at the AusTender website, where federal government contracts are listed, details 128 contracts between Australian government agencies and the Israeli company since 2011.

Cellebrite is an Israeli digital intelligence company, staffed by former Israeli military and intelligence officers, that is now commonly used by law enforcement across the globe to hack and access data – yet barely anybody in the public has heard of it.

During the writing of my new book, *The Palestine Laboratory*, it was a firm that featured heavily. The most infamous Cellebrite spyware tool, the Universal Forensic Extraction Device (UFED), has been deployed by some of the most repressive states in the world, such as Russia and China, and across virtually all levels of the US government. A former Cellebrite employee wrote in 2020 that the company did nothing to stop the abuse of its products and was happy to sell them to the worst offenders on the planet.

In Australia, Cellebrite is rarely in the headlines. The company enjoys little scrutiny, apart from recent stories in iNews and the Guardian, detailing how Services Australia is using Cellebrite spyware to pursue alleged welfare fraud by cracking into individuals' locked mobile phones. The hacking technology was allegedly used against a woman receiving single parent payments to determine if she had been in a relationship at the time. Although no charges were ever laid, the woman was chased for repayments.

The range of Australian government departments now using Cellebrite's unique phone spying abilities, from the Australian Tax Office to the Australian Federal Police and the Australian Criminal Intelligence Commission to the Department of Home Affairs, shows that the corporation's troubling record and accuracy across the globe has had no impact on it being able to secure contracts in Australia.

The history of Cellebrite and its role as an unaccountable arm of the Israeli state is detailed in this edited extract from my new book, *The Palestine Laboratory*.

The Palestine Laboratory: How Israel Exports The Technology Of Occupation Around The World is published by Scribe and available now.

It is not only NSO Group that's causing harm around the globe. Cellebrite is another Israeli company that works with repressive states and yet it has received far less criticism. It is hard to know exactly why it has escaped NSO's notoriety, but perhaps it's because Cellebrite prefers to operate under the radar with its phone hacking capabilities or because NSO's alliance with despots has uniquely captured the attention of researchers and media outlets that often fail to make the necessary ties to the Israeli state. "Cellebrite sells equipment to hack phones from short distance and NSO Group from long distance, but the effect is the same for activists," Israeli human rights lawyer Eitay Mack told me.

Founded in the 1990s, Cellebrite started out as a consumer technology firm but by the 2010s was deep into the surveillance business and mobile phone hacking because it saw the potential of huge profits from working with law enforcement officials around the world. In late 2021, Cellebrite launched a large–scale PR campaign called "Heroes behind the Heroes," featuring online ads and physical billboards that promoted the essential work being performed by their "digital intelligence solutions" in police forces around the globe.

Unsurprisingly, the PR blitz was selective about what services Cellebrite offered and who these advertisements were intended to influence. In 2022 Eitay Mack wrote to the company and Israel's Defense Ministry to remind it where Cellebrite equipment had ended up, including Russia, where journalists are pursued, and the Philippines, where countless reporters were murdered during the reign of President Rodrigo Duterte.

The Australian Federal Police Commander signed over two Cellebrite machines to the Royal PNG Police Commissioner in June 2021 as part of the PNG–Australia Policing Partnership. Photo credit: Australian High Commission PNG.

Neither the Israeli government nor Cellebrite could claim ignorance of what might happen to sophisticated surveillance gear in the hands of autocrats. There is a published photograph of Cellebrite employees meeting Duterte in 2018 and admitting that the corporation had trained a range of public bodies, some of whom were directly complicit in the murder of thousands of Filipinos during Duterte's brutal "war on drugs." When challenged on its complicity, Cellebrite told *Haaretz* that it had "strict oversight mechanisms" over its sales. It was a statement that was remarkably similar to NSO's when pushed on its international relations.

The countries where Cellebrite surveillance tech has been used against critics, journalists, dissidents, or human rights workers include Botswana, Vietnam, Bangladesh, and Uganda. This includes the Universal Forensic Extraction Device (UFED) hacking tool, which allows the extraction of information from mobile phones. In Bangladesh the hardware was used by the Rapid Action Battalion, a notorious paramilitary unit, which has been accused of extrajudicial killings and disappearances. When this connection was exposed in 2021, the company quickly announced that sales to Bangladesh were being suspended, though it was likely Bangladesh could still use the tech that had already been acquired.

Furthermore, Cellebrite said it would establish an advisory committee to ensure that "ethical considerations" were prioritized moving forward. Once again, Cellebrite used the same PR–driven tactic employed by NSO. Bangladesh has no formal ties with the Israeli government, but this did not stop Israeli intelligence experts from training Bangladeshi officers during a four–day event on the outskirts of Budapest, Hungary, in 2019. The Ethiopian federal police use Cellebrite products despite the government's mass detention of minorities and repression of dissidents, journalists and activists.

Ethiopian police officers display Cellebrite's UFED system. Photo credit: Ethiopian federal police Facebook page.

Like NSO, Cellebrite resists media scrutiny. According to reporting in *Haaretz*, the Israeli Defense Ministry does not oversee Cellebrite sales because its products are somehow classified as dual–use civilian services and not a security–related export, a definition that therefore allows Cellebrite to operate in dozens of countries with no serious Israeli oversight.

The company has never had problems getting high–paying clients. Over 2,800 US government customers, including law enforcement agencies, including the Department of Veterans' Affairs, and the Department of Agriculture, have purchased the company's equipment, and the firm has hired prosecutors, police officers, and Secret Service agents to train people to use it. The company has announced that it has secured business with six of the world's biggest oil refiners and six of the planet's largest pharmaceutical firms. It has also moved into the increasingly profitable field of corporate surveillance. Elsewhere, Cellebrite systems were purchased around 2015 by the Venezuelan government amid allegations that it was used by the regime to target dissidents.

However, bad press has nevertheless sometimes impacted the company's reach. The corporation said that it would no longer sell its UFED to Russia and Belarus after Eitay Mack revealed in court documents in 2021 that it had been used to surveil gay activists and opposition figures in both nations, including an associate of Russian political dissident Alexei Navalny and critics of Belarussian dictator Alexander Lukashenko.

In 2021 the company claimed to have withdrawn from activities in China and Hong Kong, but the *Intercept* later discovered that the brokers who had sold Cellebrite were still selling its hacking technology to Chinese police on the mainland and in Tibet. Human rights groups posited that the company was cutting official ties with some repressive states because it went public on the Nasdaq market in 2021 and wanted to leave controversy behind.

But doing that was not so easy. Cellebrite had sold its tools to Indonesia, a Muslim nation with no diplomatic relations with Israel, and the country had used them to target political opponents and activists, including in West Papua, as well as members of the gay community who used dating apps such as Grindr. Saudi Arabia was also a willing customer even after its 2018 assassination of *Washington Post* journalist Jamal Khashoggi.

In a 2020 interview, Cellebrite CEO Yossi Carmil rejected any suggestion that his firm was similar to NSO because what his company did was "very limited in its authority, unlike the world of the clients of NSO and others, where illegal things as well as covert things are done. Cellebrite is entirely in the good zone, with judicial orders. We don't create hacking devices for private entities or espionage agencies."

Upturn, a nonprofit in Washington, found in 2020 that Cellebrite tech was used frequently by US law enforcement to hack into smartphones, allegedly to fight crime. At least forty–nine out of the fifty biggest police department had used the tool to investigate crimes such as shoplifting, rape, and murder. Encrypted smartphones are routinely and successfully broken with Cellebrite tech. Upturn found that it had been done hundreds of thousands of times between 2015 and 2020.

Like NSO, Cellebrite operates in nations that have friendly relations with Israel and in those with whom there's little to no official diplomacy, on the basis that cyberweapons sales do not need to respect these niceties. Ethical considerations are not a factor in Israeli government decision–making. "It was amazing that Cellebrite wasn't worried about US sanctions on countries like Russia and China and were still happy to sell equipment to Moscow and Beijing," Eitay Mack told me. "Not only when there was publicity against them they reacted and canceled contracts in both countries." The advantage for Israel, Mack said, is that "while it will be hard for Israel to sell Israeli guns or weapons that can be identified (as happened for decades before the cyber age), Israeli surveillance is different" and less identifiable as originating in Israel.

A former Cellebrite employee, previously a member of the defense establishment, wrote anonymously in *Haaretz* that "I am free from personal experience that the company does nothing to prevent the abuse of its products by customers." The reason repressive states want Israeli tech, whether from Cellebrite or NSO, is simple: China and other states make "inferior alternatives."

LATEST ARTICLES


THE ISRAELI COMPANY HACKING INTO YOUR LOCKED MOBILE PHONE


SNUBBING THE NEIGHBOURS

THE TIME FOR LOUD DIPLOMACY – A COMMENTARY

THE PATHWAY TO FREEDOM FOR JULIAN ASSANGE

THE AMBASSADOR AND THE HIT LIST

GREEN ENERGY'S DOWN SIDE

Antony Loewenstein

ANTONY LOEWENSTEIN *is co–editor of DECLASSIFIED AUSTRALIA, and an independent journalist, author and film–maker who has written for the Guardian, New York Times and many others. His books include Disaster Capitalism: Making A Killing Out Of Catastrophe and Pills, Powder and Smoke: Inside The Bloody War On Drugs* View all posts by Antony Loewenstein