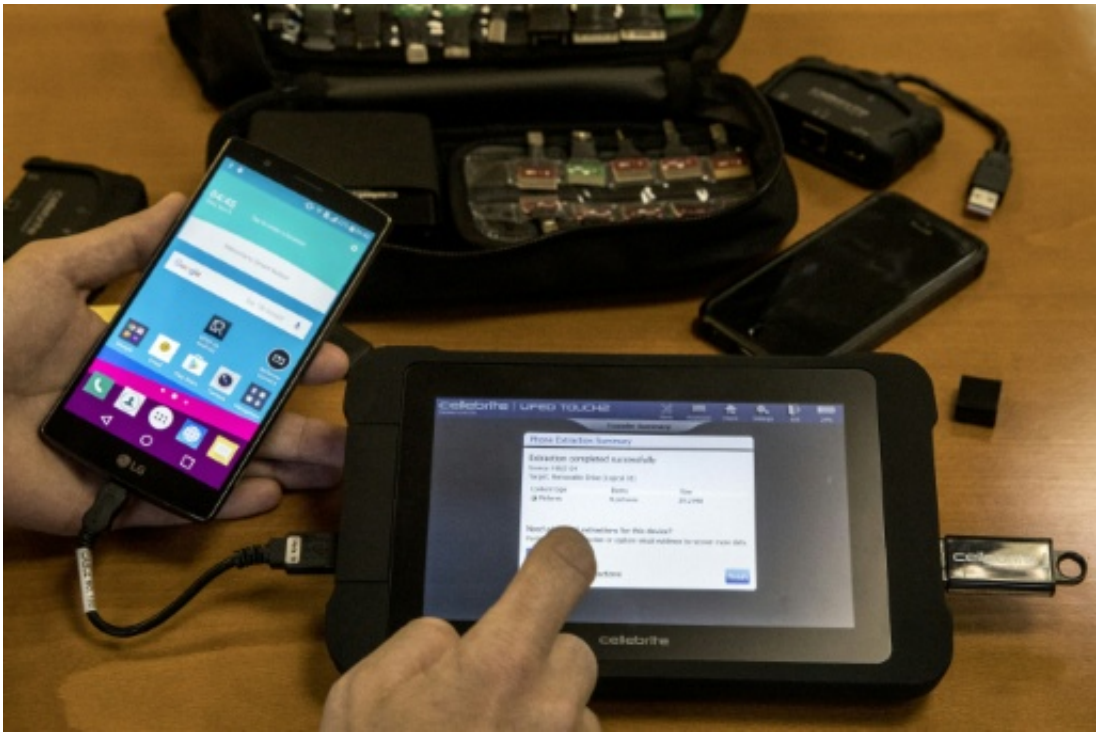
Israeli firm can steal phone data in seconds

November 23 2016, by Joe Dyke



A Cellebrite engineer explains the technology used to unlock smartphones and pull data

It only takes a few seconds for an employee of one of the world's leading hacking companies to take a locked smartphone and pull the data from it.

Israeli firm Cellebrite's technology provides a glimpse of a world of possibilities accessible to security agencies globally that worry privacy advocates.

The company has contracts in more than 115 countries, many with governments, and it shot to global prominence in March when it was reported the FBI used its technology to crack the iPhone of one of the jihadist-inspired killers in San Bernardino, California.

There have since been reports that Cellebrite was in fact not involved, and the company itself refuses to comment.

Regardless, it is recognised as one of the world's leaders in such technology.

It can reportedly take a wide range of information off devices: from the content of text messages to potentially details of where a person was at any given moment.

Even messages deleted years before can be potentially retrieved.

"There are many devices that we are the only player in the world that can unlock," Leeor Ben-Peretz, one of the company's top executives, told AFP in English.

But privacy and rights activists worry such powerful technology can wind up in the wrong hands, leading to abuses.

A Cellebrite employee opens a drawer where phones are stored to enable researchers to find vulnerabilities to crack into them

'Cat and mouse'

Cellebrite's technology is not online hacking. It only works when the phone is physically connected to one of the firm's devices.

The company recently demonstrated its capabilities for an AFP journalist.

The password on a phone was disabled and newly taken photos appeared on a computer screen, complete with the exact location and time they were taken.

The phone in the demonstration, an LG G4 run on Google's Android

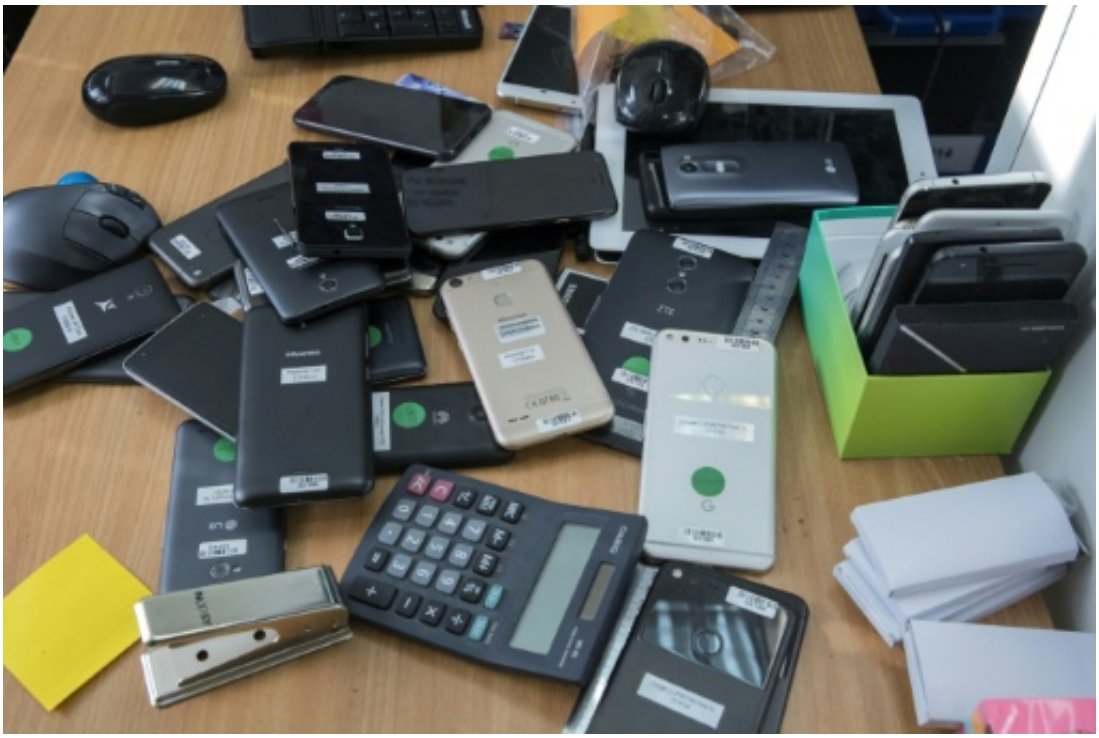
operating system, is a model Cellebrite had already cracked, so the extraction did not take long.

The real challenge, Ben-Peretz agrees, is staying in the lead in a race where phone manufacturers constantly launch new models and update software with ever more complicated security.

In the firm's lab they have 15,000 phones—with around 150-200 new models added each month.

When a new phone is launched, Ben-Peretz said, their 250-person research team races against competitors to find a chink in its armour, a process that can range from a few days to months.

iPhones present a particular challenge because, unlike many firms, Apple designs everything from the device's hardware to software, making its technology particularly difficult to hack, explained Yong Wang, a professor at Dakota State University in the United States.



It only takes a few seconds for an employee of Cellebrite, one of the world's leading hacking companies, to take a locked smartphone and pull the data from it

Ben-Peretz remains confident his company can crack even the newest iPhones.

"iOS devices have strong security mechanisms that give us a challenge, but if anyone can address this challenge and provide a solution to law enforcement, it is Cellebrite," he said, referring to Apple's operating system.

Legitimate means?

According to Ben-Peretz, there is no phone on the market that is impossible to crack.

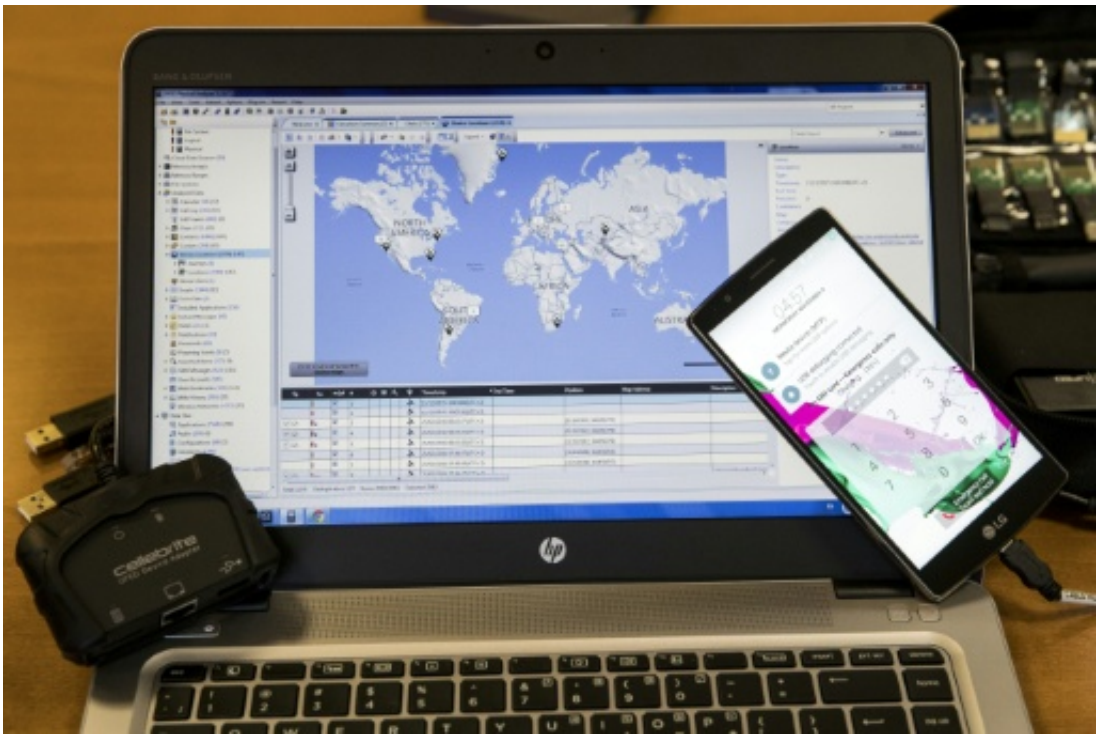
"Yes it is getting harder, it is getting more complex," he said. "But we still deliver results and they are results on the latest devices and latest operating systems."

Among the data the firm claims to be able to access are text messages deleted years previously.

"In some devices even if you would format the device and you would believe the data is deleted, still a significant portion of it exists," Ben-Peretz added.

The company sells its products largely to police and law enforcement agencies across the globe, though also increasingly to private firms doing corporate investigations.

It has seen particularly high growth in Asia, multiple times the 15 percent global growth rate, Ben-Peretz said without providing specific numbers.



The Israeli firm Cellebrite shot to global prominence when it was reported the FBI used its technology to crack the iPhone of one of the jihadist-inspired killers in San Bernardino

Rights groups worry that the technology can be used by dictatorial regimes to abuse peoples' privacy.

"Any company, including Cellebrite, has a responsibility to ensure their business activities don't contribute to or benefit from serious human rights violations," said Sari Bashi, Israel advocacy director at Human Rights Watch.

Ben-Peretz said the company vets clients and always respects local laws, but the governments are primarily responsible.

"Take a look at any regime, potential regime around the world: Could

you do anything to deprive them from throwing a stone at someone or from driving a car and running over people?

"You can't blame the car manufacturer at that point for delivering a car that was utilised to commit that kind of crime," he said.

Bashi called the comparison misleading as cars are mass-produced.

"A surveillance contract is a bit different. You have a small number of clients and there is an opportunity to ask questions or to ask for a commitment that the technology will not be used for X, Y and Z."

Citation: Israeli firm can steal phone data in seconds (2016, November 23) retrieved 27 April 2024 from https://phys.org/news/2016-11-israeli-firm-seconds.html