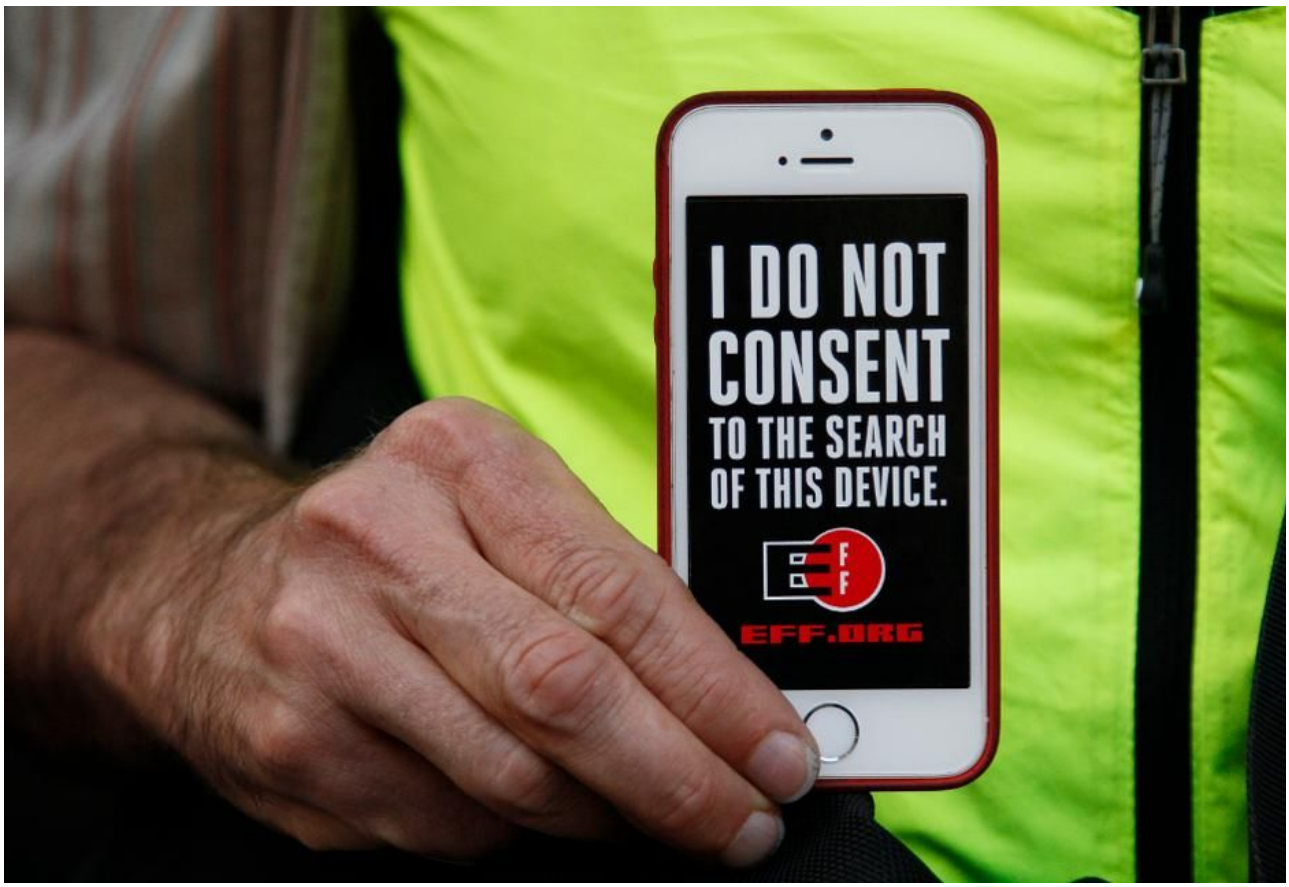
US Immigration Splurged $2.2 Million On Phone Hacking Tech Just After Trump's Travel Ban

Thomas Brewster Forbes Staff
Cybersecurity
Associate editor at Forbes, covering cybercrime, privacy, security and surveillance.

This article is more than 2 years old.



A man holds up his iPhone during a rally in support of data privacy outside the Apple store in San... [+]

On March 9, just three days after President Trump signed off his second attempt at a travel ban from Muslim-majority countries, U.S. Immigration and Customs Enforcement (ICE) ordered $2 million worth of what's believed to be some of the most powerful phone and laptop hacking technology available. The tech was sold by the U.S. government's go-to supplier when it wants to raid the contents of individuals' digital lives, Israeli supplier Cellebrite, as revealed in public records on a

purchase order discovered by *Forbes*. Together with evidence the DHS Agency went on a hacking tool shopping spree after Trump came into power, in which it spent record sums on Cellebrite and its competitors, the contracts have sparked alarm amongst privacy activists anxious about unnecessarily invasive searches of travelers' devices.

ICE's Mission Support unit in Dallas, Texas, made the massive order of Cellebrite Universal Forensic Extraction Devices (UFEDs), which have the ability to crack open mobile devices and rapidly rip out all the data inside for cops to poke through. Such Mission Support units work within ICE's Homeland Security Investigations division; one of its core roles is the execution of forensic searches on devices coming in at the border.

A single UFED unit sells for anywhere between $5,000 and $15,000, one forensics community source said, who described the deal as simply "massive" in a market where the typical contract rarely exceeds $100,000. Indeed, it's the biggest publicly-known U.S. government order of Cellebrite technology to date, and one of the single largest publicly-known purchases of deep forensics gear on record. And, according to other public contracts, it appears ICE is spending record sums on its other favorite hacking tools from two of Cellebrite's biggest rivals: Russia's Oxygen Forensics and Canada's Magnet Forensics.

Though it's unclear just how the ICE Mission Support will use its new equipment, human rights experts expressed deep concern at the potential for extremely powerful technology being used as part of the Department of Homeland Security's much-contested warrantless border searches. "We view with great alarm these purchasing documents," said the Electronic Frontier Foundation's senior staff attorney Adam Schwartz. "We assume this means more and more innocent people are going to have more of their private info searched... It tells us the government is not just thumbing through people's devices, their phones and laptops, but in many cases they're using very, very powerful technology produced by these companies to search this very private information on our phones."

Border police have faced strong criticism for their treatment of both American citizen and foreigners when entering the country, since the Trump administration came to

power, with stories ranging from the troubling to the obscene. Without a warrant, in January U.S. customs agents detained American-born NASA engineer Sidd Bikkannavar and demanded he hand over his smartphone password, while the same happened to U.S. citizen Haisam Elsharkawi was stopped in L.A. before travelling to Saudi Arabia, though he was handcuffed while being questioned. The government claims it can carry out these searches as the Constitution's protections against unjustified searches don't extend to the border.

The number of border searches has also risen at an astonishing rate, both in Presider Obama's last year and even more so once Trump was in the White House. It was recently reported the Department of Homeland Security searched 5,000 devices at tl border in February 2017 alone, up from 5,000 for the entirety of 2015. Continuing a numerical theme, the Trump executive order directed the Secretary of Homeland Security to hire an additional 5,000 border agents to help with the extra workload.

ICE is one of the two main agencies with the authority to search devices entering the country alongside Customs and Border Protection. Typically, CBP (also a Cellebrite customer) is the first port of call for intercepting devices as people land in America, but it often passes them on to ICE agents for more in-depth forensics. It appears ICE may have greater search powers too, in that CBP requires supervisory approval wher copying a phone's contents, whereas ICE does not, according to official guidance obtained by MuckRock. The two continue to work closely together under th Trump administration, which has tasked them with upping their efforts to detain and deport immigrants without the proper documentation, even if they haven't broken th law.

With the huge orders of Cellebrite and competitor gear, digital rights activists are fretting about not just the quantity of those searches, but the quality of them as well under the aegis of ICE. "We're seeing an increase in both the searches and in the [technological] capabilities," said Esha Bhandari, staff attorney at the American Civil Liberties Union (ACLU). "These technologies allow them not only to see current data but also deleted data... and into people's entire lives."

Phone hacking boom follows Trump order

Cellebrite is known as the world's biggest supplier of phone forensics, providing tools to police around the world looking to search all kinds of electronic media and cloud services. It was once linked to the hack of the San Bernadino shooter's iPhone 5C, bu

later reports indicated another supplier was contracted. Its software, once tested by *Forbes* at a policing tech conference, is remarkably easy to use: simply plug in a cellphone to the UFED and click on the touchscreen buttons to retrieve all data from apps inside. For instance, it can pull data hosted on Facebook, Google or even Tinder servers, as long as the phone is connected to the respective web account, and Cellebrite has the power to break through some lockscreens, though it's not known to be capable of breaking the most modern Apple iPhone and Google Android systems.

"What we've seen through other sources is that Cellebrite has the power to image the device - i.e. copy it all - and go to 'unallocated space' where information goes when w think we've deleted it and bring it back," said Schwartz.

The $2 million order is a huge one for Cellebrite, the biggest its received from any U. government agency, according to public records on the Federal Procurement Data System, which showed the company's annual revenue stood at $70 million. The next biggest appears to be a 2012 U.S. Air Force deal for $1.27 million and the second mos profitable contract with ICE was for $974,110 in 2014 (not all contracts are made public by the government). A recent Motherboard report using data from public access requests and other sources also puts the size of the $2 million transaction in a startling light: in a map of spending across different states, the biggest spender was Iowa at just $258,000.

The Cellebrite contract will last for two years. Neither Cellebrite nor the ICE commented on the deal or what the technology would be used for.

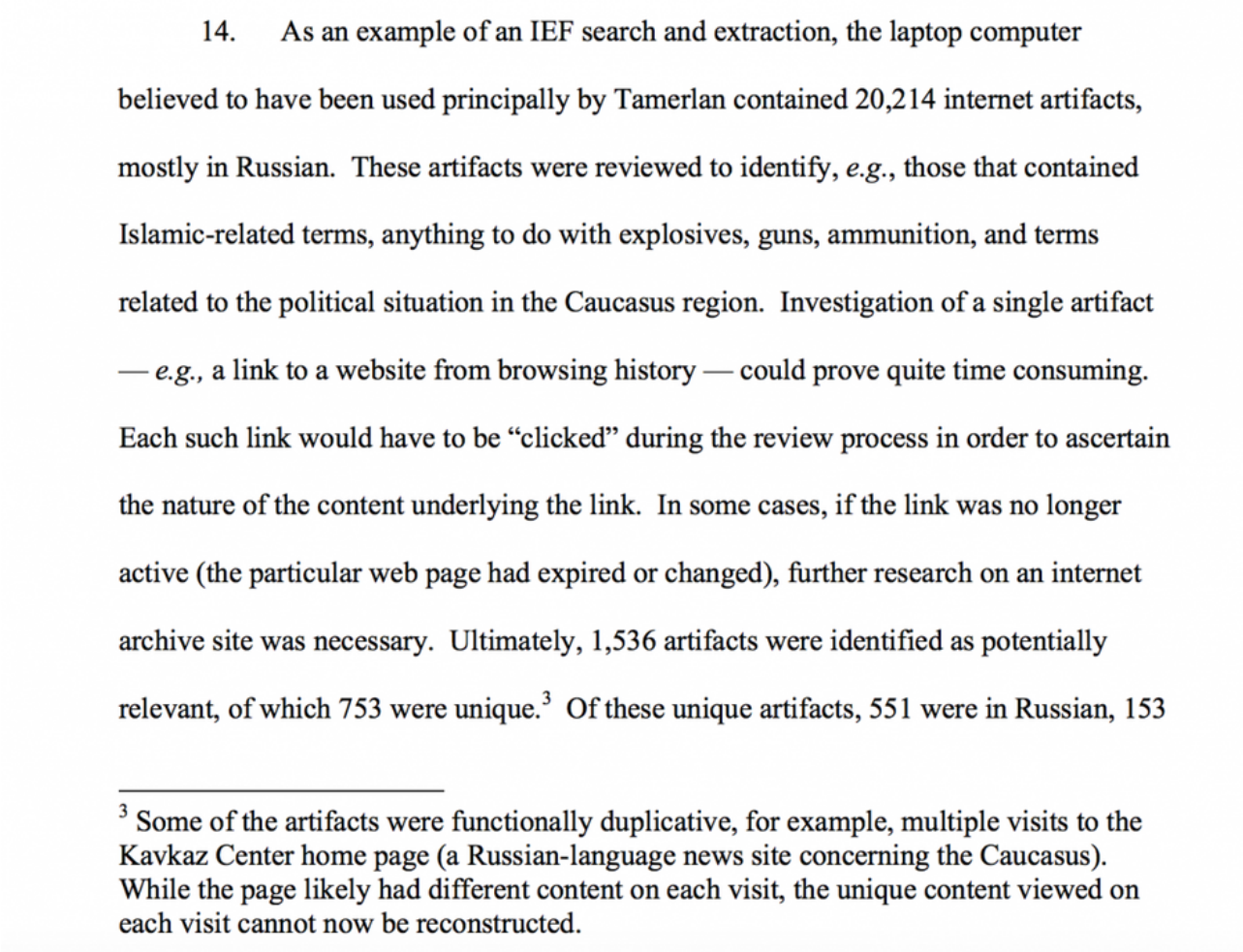
Not just Cellebrite celebrating Trump's "extreme vetting"

Cellebrite isn't the only forensics supplier profiting from ICE's increased tech requirements since the Trump order went through and the president demanded "extreme vetting" of people travelling from Muslim-majority nations, including Iran, Libya, Somalia, Sudan, Syria and Yemen. Indeed, the border agency is spending record sums on cellphone and laptop search tech.

The Dallas mission support department spent $151,848 in early April on upgrades to its licenses for phone and laptop software called Axiom from Magnet Forensics, the marketing material for which claims it can quickly create a copy of an "iOS or Androi device, hard drives, and removable media" so agencies can find "evidence you didn't know was there." Again, according to public records, that was the biggest ever single

payment to the firm from ICE. The firm also received purchase orders from ICE on March 15 for $15,586 and on March 9 $8,600, though records indicated the latter wa for an investigation into a peer-to-peer network. (To be clear, ICE does a lot more than just border searches, investigating child exploitation, narcotic sales and fraud, amongst other crimes).

Magnet is a Canadian company founded by former police officer Jad Saliba, which in 2016 announced a strategic partnership with and funding from In-Q-Tel, an investor for the U.S. intelligence community. It's been growing in prominence, in part becaus of its involvement in the Boston Bomber case, in which its Internet Evidence Finder was used to uncover "artefacts" of web-related activity from the PC of Tamerlan Tsarnaev, the younger brother involved in the terrorist attack of 2013, a court document showed.



14. As an example of an IEF search and extraction, the laptop computer believed to have been used principally by Tamerlan contained 20,214 internet artifacts, mostly in Russian. These artifacts were reviewed to identify, *e.g.*, those that contained Islamic-related terms, anything to do with explosives, guns, ammunition, and terms related to the political situation in the Caucasus region. Investigation of a single artifact — *e.g.*, a link to a website from browsing history — could prove quite time consuming. Each such link would have to be "clicked" during the review process in order to ascertain the nature of the content underlying the link. In some cases, if the link was no longer active (the particular web page had expired or changed), further research on an internet archive site was necessary. Ultimately, 1,536 artifacts were identified as potentially relevant, of which 753 were unique.[3] Of these unique artifacts, 551 were in Russian, 153

[3] Some of the artifacts were functionally duplicative, for example, multiple visits to the Kavkaz Center home page (a Russian-language news site concerning the Caucasus). While the page likely had different content on each visit, the unique content viewed on each visit cannot now be reconstructed.

Magnet's Internet Evidence Finder proved useful for drawing out evidence for the Boston Bomber case. FORBES SCREENSHOT

Oxygen Forensics received two delivery orders from the department in March, totalling just over $58,000. The first, signed off before Trump's second order but aft his first attempt (blocked by American courts), came to $55,509 and appears to be fc

a short, week-long contract. It was also a record sum for Oxygen to have received fro ICE. Oxygen was set up in Russia by founders Oleg Fedorov and Oleg Davydov. Now with a base in the heart of the U.S. surveillance industrial complex in Alexandria, Virginia, it also claims contracts with the FBI, Department of Defense and the U.S. Army, as well as global law enforcement agencies, boasting the ability to hack into th "widest range" of mobile operating systems, from Apple's iOS to Google's Android, BlackBerry and Windows Phone.

Neither Magnet nor Oxygen responded to requests for comment.

'Lack of transparency'

According to Bhandari, the contract awards only begged more questions of the Trum administration's warrantless border searches. "This kind of tech acquisition really calls out for more transparency on what are they searching, how often, how long are they storing the data, who are they sharing it with?"

Currently, the U.S. government does not believe it requires a warrant to search devices on people passing into the country, even if they amount to what Bhandari described as "digital strip searches." But the administration is being taken to task by the ACLU and others over its claim that Fourth Amendment privacy protections do not apply at the border.

But as long as that confusion over the legalities of customs searches, the government is continuing to invest heavily in the technology and personnel that can open up the private lives of anyone entering America.

Follow me on Twitter. Check out my website. Send me a secure tip.

Thomas Brewster

I'm associate editor for Forbes, covering security, surveillance and privacy. I've been breaking nev and writing features on these topics for major publications since ... **Read More**