

Security #CyberSecurity

The Little Black Book of Billionaire Secrets

FACEBOOK GAVE ALL OF YOUR STUFF TO OVER 300 SPY AGENCIES AND POLITICAL MANIPULATION COMPANIES

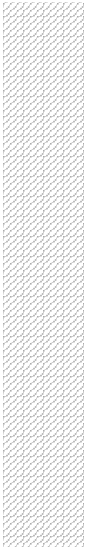


Thomas Fox-Brewster, FORBES STAFF

I cover crime, privacy and security in digital and physical forms.

Facebook CEO, Mark Zuckerberg, appeared for a hearing with the

When Mark Zuckerberg appeared before the House Energy and Commerce Committee last week in the [aftermath of the Cambridge Analytica revelations](#), he tried to describe the difference between "surveillance and what we do." "The difference is extremely clear," a nervous-looking Zuckerberg said. "On Facebook, you have control over your information... the information we collect you can choose to have us not collect."



But not a single member of the committee pushed the billionaire CEO about surveillance companies who exploit the data on Facebook for profit. *Forbes* has uncovered one case that might shock them: over the last five years a secretive surveillance company founded by a former Israeli intelligence officer has been quietly building a massive facial recognition database consisting of faces acquired from the giant social network, YouTube and countless other websites. Privacy activists are suitably alarmed.

That database forms the core of a facial recognition service called Face-Int, now owned by Israeli vendor Verint after it snapped up the product's creator, little-known surveillance company Terrogence, in 2017. Both Verint and Terrogence have long been vendors for the U.S. government, providing bleeding-edge spy [tech to the NSA](#), the U.S. Navy and countless other intelligence and security agencies.

As described on the [Terrogence website](#), the database consists of facial profiles of thousands of suspects "harvested from such online sources as YouTube, Facebook and open and closed forums all over the globe." Those faces were extracted from as many as 35,000 videos and photos of terrorist training camps, motivational clips and terror attacks. That same marketing page was online in 2013, according to internet archive the Wayback Machine, indicating the product is at least five years old. The age of the product also suggests far more than 35,000 videos and photos have been raided by the Face-Int technology by now, though Terrogence co-founder and research lead Shai Arbel declined to comment for this article.

Raising the stakes of facial recognition

Though Terrogence is primarily focused on helping intelligence agencies and law enforcement fight terrorism online, LinkedIn profiles of current and former employees indicate it's also involved in other, more political endeavours. One ex-staffer, in

describing her role as a Terrogenance analyst, said she'd "conducted public perception management operations on behalf of foreign and domestic governmental clients," and used "open source intelligence practices and social media engineering methods to investigate political and social groups." She was not reachable at the time of publication.

Recommended by Forbes

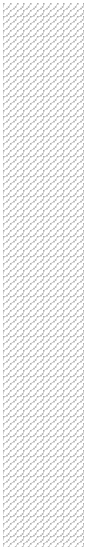


And now concerns have been raised over just how Terrogenance has grabbed all those faces from Facebook and other online sources. What's apparent, though, is that Terrogenance is yet another company that's been able to clandestinely take advantage of Facebook's openness, on top of Cambridge Analytica, which acquired information on as many as 87 million users in 2014 from U.K.-based researcher Aleksandr Kogan to help target individuals during its work for the Donald Trump and Ted Cruz presidential campaigns.

"It raises the stakes of face recognition - it intensifies the potential negative consequences," warned Jay Stanley, senior policy analyst at the American Civil Liberties Union (ACLU). "When you contemplate face recognition that's everywhere, we have to think about what that's going to mean for us. If private companies are scraping photos and combining them with personal info in order to make judgements about people - are you a terrorist, or how likely are you to be a shoplifter or anything in between - then it exposes everyone to the risk of being misidentified, or correctly identified and being misjudged."

Jennifer Lynch, senior staff attorney at the Electronic Frontier Foundation, said that if the facial recognition database had been shared with the US

government, it would threaten the free speech and privacy rights of social media users.



"Applying face recognition accurately to video is extremely challenging, and we know that face recognition performs poorly with people of color and especially with women and those with darker skin tones," Lynch told *Forbes*. "Combining these two known problems with face recognition, there is a high chance this technology would regularly misidentify people as terrorists or criminals.


"This could impact the travel and civil rights of tens of thousands of law-abiding travelers who would then have to prove they are not the terrorist or criminal the system has identified them to be."

It's unclear just how the Face-Int product acquires faces, though it appears similar to a project run by the NSA, as [revealed by whistleblower Edward Snowden in 2014](#), where the intelligence agency had gathered 55,000 "facial recognition quality images" from the web back by 2011. Co-founder Arbel, a former intelligence officer with the Israeli military, declined to respond to questions about how the tech works, though he described Face-Int as "amazing" in a text message and confirmed it continues to operate under Verint.

A spokesperson for Facebook, which [employs its own facial recognition tech](#) to help identify users' visages in photos across the platform, said it appeared Terrogen's product would violate its policies, including one that prohibits the use of data grabbed from the social network to provide tools for surveillance. Facebook also doesn't allow accessing or collecting information via automated methods, such as harvesting bots or scrapers. The spokesperson noted that it hadn't found any Facebook apps operated by the company.

A social media monitor

There's no evidence America has purchased Face-Int. But it has benefitted from other intelligence



services built by Terrogence. The vendor has scored at least two contracts with the U.S. government, both with the U.S. Navy and worth a total of \$148,000, according to public records. The contracts, one from 2014 the other signed off in 2015, were for subscriptions to the company's [Mobius](#) and TGAAlertS products.

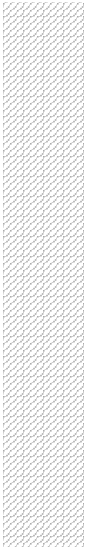
Mobius consists of reports on the latest trends in terrorists' improvised explosive devices (IEDs) and their tactics. The reports are based on intel gathered from various social media platforms "where global terrorists seek to recruit, radicalize and plot their next attack," according to a company [brochure](#). TGAAlertS, meanwhile, provides "near real-time" information on urgent issues uncovered by Terrogence staff trawling the web.

Those employees gather information in part through fake profiles. As another [brochure](#) put it, they "elicit information by carefully guiding online discussion, often drumming up interest and facilitating communication by employing multiple virtual entities in a single operation."

This is far from Arbel's first rodeo in the surveillance industrial complex: he co-founded [SenseCy](#), which was acquired by Verint in 2017. It too sets up "virtual entities" to gather intelligence. "Perfected over many years of practice, SenseCy operates dozens of virtual entities combine strong, believable cover stories with well-perfected web interaction methodologies, and are sourcing invaluable intelligence from all relevant web platforms," a blurb on its site currently reads. The company appears to be more focused on cybersecurity protection than government surveillance, however.

The privatization of blacklists

If Terrogence isn't solely focused on terrorism, but has a political side to its business too, its facial recognition work could sweep up a vast number of people. That brings up another particularly worrying aspect of the business



in which Terrorence operates: the dawn of "the privatisation of blacklisting," warned Stanley. "We've been fighting with the government for years over due process on those lists... people being put on them without being told why and not being sure how those lists are being used," he told *Forbes*.

"A lot of those problems could intensify if you have a bunch of private quasi-vigilantes making their own blacklists of all kinds." Just earlier this month, Verint [launched](#) what appeared to be an entirely separate facial recognition product, FaceDetect. It promises to identify individuals "regardless of face obstructions, suspect ageing, disguises and ethnicity" and "allows operators to instantaneously add suspects to watch-lists."

But Stanley also questioned Facebook's policies on user control of profile photos. The social network has the largest collection of faces in the world, and yet profile pictures, to an extent, can't be entirely locked down, he said. A Facebook spokesperson said profile photos are always public but it's possible to [adjust the privacy settings](#) of previous profile snaps to limit who can see them.

Privacy advocacy groups like the ACLU now want to see users given more control over those images. Given the recent furore surrounding Cambridge Analytica, such changes might come sooner rather than later.

Got a tip? Email at TFox-Brewster@forbes.com or tbthomasbrewster@gmail.com for [PGP mail](#). Get me on Signal on +447837496820 or use [SecureDrop](#) to tip anyone at Forbes.

