As U.S. Government Report Reveals Facial Recognition Tech Widely Used, WEF-Linked Israeli Facial Recognition Firm Raises $235 Million

By Derrick Broze

In June the U.S. Government Accountability Office released a report detailing the widespread use of facial recognition technology, including law enforcement using databases of faceprints from government agencies and private firms. Privacy and civil rights organizations have been warning for the last few years that the use of facial recognition technology was a digital Wild West with little to no regulation determining the limits of the tech.

Now, the GAO's new report shows that at least twenty of the forty-two U.S. government agencies surveyed have used the

technology. These departments include those associated with law enforcement – the FBI, Secret Service, US Immigration and Customs Enforcement, US Capitol Police, Federal Bureau of Prisons, and the Drug Enforcement Administration – as well as less obvious departments such as the U.S. Postal Service, the Fish, and Wildlife Service and NASA.

Six U.S. agencies admitted to using facial recognition on people who attended the protests after the killing of George Floyd in May 2020. The report states that the agencies claim they only used the tech on people accused of breaking the law.

"Thirteen federal agencies do not have awareness of what non-federal systems with facial recognition technology are used by employees," the report said. *"These agencies have therefore not fully assessed the potential risks of using these systems, such as risks related to privacy and accuracy."*

The GAO calls for increased training for law enforcement, stating that such training could *"reduce risks associated with analyst error and decision-making; understand and interpret the results they receive; raise awareness of cognitive bias and improve objectivity; and increase consistency across agencies."* The GAO also calls for agencies to implement controls to better track what systems their employees are using.

While some of the U.S. government agencies have their own databases, the FBI's database of faceprints is likely the most extensive, with some estimates at over 100 million faceprints. The U.S. government's top law enforcement agency has been fighting to keep the database a secret since at least 2013.

Agencies have also used facial recognition databases from Amazon Rekognition, BI SmartLink, Giant Oak Social Technology, Clearview AI, and Vigilant Solutions. By far, government agencies used technology from Clearview and Vigilant the most.

The report provides further insight:

> *"Moreover, federal law enforcement can use non-government facial recognition service providers, such as Vigilant Solutions and Clearview AI. For example, law enforcement officers with a Clearview AI account can use a computer or smartphone to upload a photo of an unknown individual to Clearview AI's facial recognition system. The system can return search results that show potential photos of the unknown individual, as well as links to the site where the photos were obtained (e.g., Facebook). According to Clearview AI, its system is only used to investigate crimes that have already occurred and not for real-time surveillance."*

The US Postal Inspection Service said it has used Clearview AI's software to help track down people suspected of stealing and opening mail and stealing from Postal Service buildings. Altogether, ten agencies used Clearview AI between April 2018 and March 2020. The U.S. Capitol Police used the company's tech to investigate suspects from the event at the Capitol on January 6th.

TLAV has previously reported on the dangers associated with facial recognition technology, and specifically, how Clearview AI's technology was being used to target so-called domestic extremists.

In 2020, the NY Times wrote about Clearview's efforts to gather, store, and sell faceprint data as "the end of privacy as we know it" and they are not wrong. This company has been capturing billions of faceprints from online photos and now claims to have the world's largest facial recognition database. This gives Clearview the opportunity to sell customers access to all our faces to secretly target, identify, and track any of us. This could be for marketing and advertising purposes, but it could be for government and law

enforcement surveillance of activists, journalists, and organizers who are performing constitutionally protected activity. As the *Mind Unleashed* reported, Clearview is collecting data from unsuspecting social media users and the Chicago Police Department (CPD) is using the controversial facial recognition tool to pinpoint the identity of unknown suspects.

Clearview said in May it would stop selling its technology to private companies and instead provide it for use by law enforcement only – they have thus far made their technology available to some 2,400 law enforcement agencies across the United States. The American Civil Liberties Union has filed a lawsuit against Clearview, alleging that the company violated Illinois' Biometric Information Privacy Act (BIPA), a state law that prohibits capturing individuals' biometric identifiers without notice and consent.

While Vigilant Solutions is less well-known than Clearview, they are an essential part of the growing surveillance apparatus operated by private industry and shared with U.S. government agencies. The company is listed in the GAO report for their role in facial recognition technology, but they are widely known for their database of license plate records. In 2018 it was revealed that Vigilant Solutions signed a contract with U.S. Immigration and Customs Enforcement (ICE) making the controversial agency the latest of several federal agencies that have access to billions of license plate records that can be used for real-time location tracking.

Vigilant Solutions has more than 2 billion license plate photos in its database due to partnerships with vehicle repossession firms and local law enforcement agencies with vehicles equipped with cameras. Local law enforcement agencies typically use some version of an Automatic License Plate Reader. ALPRs are used to gather license plates, times, dates, and locations that can be used to create a detailed map of what individuals are doing. The devices can be attached to

light poles, or toll booths, as well as on top of or inside law enforcement vehicles.

AnyVision, Softbank, and the Push Towards a Technocratic Surveillance Grid

While the GAO report stands as a warning to anyone paying attention, the reality is that facial recognition technology is already ubiquitous. Despite the warnings of privacy organizations, the public has blindly walked into an era of facial recognition for opening your smartphone while purchasing groceries, and for video games. Generally speaking, the public seems downright ignorant of the attacks on privacy taking place every single day.

The GAO report notes that places like San Francisco and Portland, Oregon have banned police from using facial recognition technology, and Amazon currently has a moratorium on selling their Rekognition program to law enforcement. Most recently, Maine has passed what is being called the strongest law against facial recognition in the country. (The law does allow law enforcement to make use of the federal databases mentioned in the GAO report.)

Will these steps be enough to stem the tide of facial recognition cameras intruding into every aspect of your life? Not likely.

In the month since the release of the GAO report, we have seen Israeli facial recognition firm AnyVision raise $235 million in startup funding. AnyVision uses Artificial Intelligence techniques to identify people based on their faces. *TechCrunch* notes that *"AnyVision said the funding will be used to continue developing its SDKs (software development kits), specifically to work in edge computing devices – smart cameras, body cameras, and chips that will be used in other devices – to increase the performance and speed of its systems."*

AnyVision has not been without controversy. A report in 2019 alleged that AnyVision's technology was being secretly used by the Israeli government to run surveillance on Palestinians in the West Bank. AnyVision denied the claims. Another report published in The Markup examined public records for AnyVision, including a user guidebook from 2019, which showed the company is collecting vast amounts of data. One report involved tracking children in a school district in Texas. AnyVision collected 5,000 student photos in just seven days.

An April report from *Reuters* detailed how many companies are using AnyVision's technology today, including hospitals like Cedars Sinai in Los Angeles, retailers like Macy's, and energy giant BP. AnyVision was also the subject of a *New York Times* report in 2020 which highlighted how the company was partnering with Israel's Defense Ministry to use its facial recognition technology to "detect COVID-19 cells".

As further evidence that companies offering facial recognition technology are here to stay – and play a vital role in the Great Reset agenda – we need look no further than the institutions investing in AnyVision. The latest round of fundraising is being co-led by SoftBank's Vision Fund 2 and Eldridge. Interestingly, AnyVision's CEO Avi Golan is a former operating partner at SoftBank's investment arm. Softbank is also a partner organization with the World Economic Forum, the international public-private organizations pushing for The Great Reset.

The reason this small detail matter is because the technocratic agenda being promoted by the fine folks at the WEF will absolutely involve a world of AI and facial recognition. The technology is ostensibly being used to catch criminals for the moment, but it's also ripe for abuse by law enforcement agencies. Not to mention the larger role the technology will play in implementing future "social credit score" schemes, as seen in China.

The U.S. GAO is right to warn about the widespread use of this dangerous technology, but the fact is that it is already pervasive. It has become extremely difficult to avoid having your faceprint stolen and stored by both governmental agencies and private organizations. If we are to regain any semblance of privacy we must find a way to put an end to this technology before it is too late.

Source: The Last American Vagabond

Visit TheLastAmericanVagabond.com. Subscribe to TLAV's independent news broadcast on iTunes. Follow on Facebook, Twitter, and Minds. Support at PayPal or with Bitcoin.