World Socialist Web Site wsws.org

Hack of Department of Homeland Security contractor exposes government surveillance of drivers on US roads and border crossings

Kevin Reed
8 July 2019

On July 2 the *Washington Post* reported that US Customs and Border Protection (CBP) suspended the license of a long-standing contractor of surveillance technology on the grounds that the firm exhibited "evidence of conduct indicating a lack of business honesty or integrity."

CBP made the suspension more than a month after an anonymous hack of internal corporate data of Perceptics, a 35-year-old company based in Farragut, Tennessee. Perceptics is a supplier of license plate readers, facial recognition and artificial intelligence technologies to CBP and other government agencies at US border crossings, military facilities, electronic toll collection terminals and highway and city security systems.

The hack and subsequent publication of the data trove—including Department of Homeland Security handbooks, company PowerPoint presentations, equipment schematics, confidential agreements, technology lists, budget spreadsheets, internal photos and hardware blueprints of security systems—by a group of transparency advocates has exposed to the public the extensive infrastructure of government surveillance of drivers on roadways and at border crossings.

On June 10, CBP voluntarily reported to the *Post* that it had discovered the hack on May 31. At that time, CBP wrote that a subcontractor had transferred "copies of license plate images and traveler images" to its own network "in violation of CBP policies and without CBP's authorization or knowledge." The statement said the subcontractor's network "was subsequently compromised by a malicious cyber-attack" and that "none of the image data had been identified on the dark web or internet."

Without naming the subcontractor, CPB was clearly attempting to cover up the incident and the extent of the breach. However, weeks prior to the CBP admission, reports had already surfaced that the contents of the Perceptics server had been published on the dark web. On May 23, *The Registe r* —an independent news and commentary site serving the IT industry—reported that it had been contacted by an individual using the pseudonym "Boris Bullet-Dodger" who provided a list of the filenames of the Perceptics data as proof of the hack.

Beginning on June 14, the transparency advocate collective called Distributed Denial of Secrets (DDOS) announced via their Twitter account the publication of the first tranche of Perceptics data onto a public internet server. While DDOS said they had published the Perceptics data "without redaction," they explained that "a small number of documents related to medical insurance had been removed from the browsable version of the HR files." As of July 2, DDOS said it had published six tranches of data and were planning to post more, including corporate email communications.

Based on preliminary analyses of the Perceptics data, the CBP's initial report was false and tens of thousands of license plate images and individual driver's faces were in fact part of the hacked data. The contents of the Perceptics business information have opened a window into the relationship between the private surveillance industry and the US government. It has exposed details of the advanced technologies in use today for state monitoring of the traveling public.

CNN reported on June 17, based on its analysis of the Perceptics data, that 50,000 American license plate numbers are among the hacked data. When asked about this, a CBP representative did not deny that the plate numbers had been compromised but told CNN the agency "does not authorize contractors to hold license plate data on non-CBP systems."

A *Motherboard* report on June 13 said that many of the license plate images are not "from CPB or a border crossing" but appear to be part of a "Perceptics demo conducted for toll collection on the Pennsylvania Turnpike, which is operated by the Pennsylvania Turnpike Commission." The *Motherboard* report goes on to say, "In some of the Pennsylvania Turnpike images, drivers' faces are clearly visible; in many of them, license plate and car make-and-model information is easy to see."

The *Motherboard* report went on, "The images also show that automated toll collection on highways around the country has resulted in passive surveillance of drivers, which are in some cases added to databases that can be stored for years." *Motherboard* said these images were collected over a two-month period in 2017.

One Perceptics document analyzed by *Motherboard* showed a satellite image of the World Trade Bridge in Laredo, Texas, and another showed “zoomed-in black-and-white photos of drivers whose faces are easily visible.”

According to a Perceptics document that accompanied the turnpike demo, “The purpose of this project is to install the latest Perceptics license plate reader technology at an operational site to demonstrate the high accuracy of the Perceptics Optical Character Recognition (OCR) and high attach/yield rates that can be expected utilizing this solution.”

The reference to “high attach/yield rates” is concerning the ability of Perceptics’ automated technology to accurately read license plate data without human involvement. An earlier *Motherboard* report said that a Perceptics slide presentation from 2016 claimed that readers and cameras are designed to be combined with federal “biographic/passport data” of travelers.

Perceptics—previously a subsidiary of the defense contractor and maker of the B2 bomber Northrop Grumman—has contracts with the US, Canada and Mexico for license plate readers, under-vehicle cameras and driver cameras. The company has been a contractor for the US Customs Service (predecessor to CBP) since 1982 and, according to a DDOS representative, also has a relationship with the US Drug Enforcement Administration, Pentagon and other governments including the U.A.E., Saudi Arabia, Singapore and Malaysia.

The information made available by DDOS is further confirmation that the various domestic police agencies that operate under the umbrella of the Department of Homeland Security are expanding the surveillance of the traveling public at airports, border crossings and roadways using high definition cameras and artificial intelligence technologies. These practices represent an intensification of public spying operations by the US intelligence state beyond those revealed by Edward Snowden in 2013, which exposed National Security Agency monitoring of all electronic communications, such as phone calls and email messages.

Criticism of the latest revelations has focused on the carelessness of data handling and the threat it poses to national security with passing references to the attack on democratic rights. For example, Joseph Lorenzo Hall, chief technologist at the Center for Democracy & Technology, a Washington think tank, told the *Washington Post*, “This is a pretty stark view into one of the cogs of the U.S. surveillance state,” adding that the agencies “may have to change some of that operational stuff pretty quickly before people take advantage.”

When CNN interviewed the senior legislative counsel at the American Civil Liberties Union, Neema Singh Guliani, she said that the gathering of traveler information is not just a concern from a “privacy and civil liberties standpoint, but also from a security standpoint, given that they’ve not demonstrated they can safeguard that information.” In all of the concerns over the data breach and its security implications, it never occurs to these critics that the worst of the “bad actors” who will use this information to harm the public are the police agencies of the local and federal US government.

Democratic Party officials expressed concerns about the impact of the breach on state surveillance operations. Democratic Representative Bennie Thompson, chair of the House Homeland Security Committee, complained, “Government use of biometric and personal identifiable information can be valuable tools only if utilized properly. Unfortunately, this is the second major privacy breach at DHS this year.” Democratic Senator Ron Wyden, who presents himself as one of the few Congressmen concerned with civil liberties, told the *Washington Post*, “If the government collects sensitive information about Americans, it is responsible for protecting it—and that’s just as true if it contracts with a private company.”

As more details emerge about the content of the Perceptics data trove, it will become increasingly clear that the contractor—which had an exclusive contractual relationship with multiple federal agencies for decades—has been engaged with the US surveillance apparatus in a massive violation of basic constitutional rights.

With the development of end-to-end encryption technologies that prevent access to the private communications of individuals and organizations, the state is becoming increasingly dependent on video and physical biometric data such as facial recognition—along with social media activity—to gather a database of information on everyone.

That such things are going on in America should by now come as no surprise to anyone. The assault on basic rights—including the Fourth Amendment to the US Constitution that prohibits unreasonable searches and seizures—is an aspect of the breakdown of American democracy that has been accelerating since 2000, when the US presidential election was stolen by the Republican Party with the backing of the US Supreme Court.

Additionally, the expansion of the dragnet of government surveillance is a byproduct of the response to the attacks of September 11, 2001, which accompanied the drive by US imperialism to assert its military hegemony over the oil resources and strategic lands of the Middle East through wars and regime change campaigns. Ultimately, the buildup of domestic surveillance is part of the repressive apparatus erected by the ruling elite to suppress the coming revolutionary struggles of the working class.

To contact the WSWS and the Socialist Equality Party visit:

wsws.org/contact