CRS INSIGHT

Exposed Data Highlights Law Enforcement Use of Selected Technologies

July 10, 2019 (IN11143)

|

Related Author

- Kristin Finklea

|

Kristin Finklea, Specialist in Domestic Security (kfinklea@crs.loc.gov, 7-6259)

Official use of image capturing and facial recognition technology—particularly by law enforcement—has been the subject of recent congressional attention. Specifically, there is interest in facial recognition's accuracy, the databases against which faces are compared, which individual data are subject to collection and retention, how agencies ensure data security, and public notification regarding the use of facial recognition and other image capturing technology. Many of these issues were highlighted following a recently acknowledged breach of certain data held by a U.S. Customs and Border Protection (CBP) subcontractor. The breach was not of a CBP network. Notably, available information on developments related to the breach remains incomplete. Early speculation about the nature, origins, extent, and implications of the data breach may change, and some media reporting may conflict with official statements.

On June 10, 2019, CBP revealed that images of faces and license plates were compromised in a "malicious cyberattack" on one of its subcontractors that provides automated license plate recognition (LPR) technology to the agency. CBP, in its December 2017 privacy impact assessment (PIA) of LPR technology, noted that data generated from the fixed and mobile LPRs can include the license plate number; digital images of the vehicle's make, model, and license plate; vehicle registration location; and time, date, and location information about the images captured. It notes that images may also capture the environment surrounding the license plates, including vehicle drivers and passengers, and that "LPR technology is designed to collect information from all vehicles that pass the camera."

Data Exposure

CBP suggested, but did not confirm, that Perceptics—a firm providing LPR systems—was the subcontractor involved in the breach. In late May, Perceptics verified that its network had been compromised, and its breached data were reportedly offered—for free—on the dark web. It is not clear whether the breach confirmed by Perceptics is the same one reported by CBP.

A hacker using the name Boris Bullet-Dodger first alerted the media to the Perceptics hack and reportedly provided certain news sites with direct links to the breached data that had been posted on the dark web. Later, a transparency collective, Distributed Denial of Secrets, posted some of the documents to the surface web as well. Reporters who scoured through the data posted online indicated that in addition to images of faces and license plates, the cache of hacked data includes "detailed schematics, confidential agreements, equipment lists, budget spreadsheets, internal photos and hardware blueprints for security systems." However, no photos from passports or travel documents were reportedly compromised.

Federal Law Enforcement's Response

A number of issues arise when events such as this occur, including how the federal government will react and which agencies will respond. A 2016 Presidential Policy Directive (PPD-41) outlined how the government responds to significant cyber incidents, which includes (1) threat response, (2) asset response, and (3) intelligence support. The Department of Justice (DOJ), through the Federal Bureau of Investigation (FBI) and National Cyber Investigative Joint Task Force (NCIJTF), is the designated lead on threat response, which involves investigating and attributing specific cyber activities to particular individuals or entities as well as facilitating intelligence and information sharing. CBP noted that it is "working closely with other law enforcement agencies and cybersecurity entities, and its own Office of Professional Responsibility to actively investigate the incident" involving the breach of its subcontractor's data. The FBI has not officially attributed the hack, and neither CBP nor the FBI has released official information on specific actions the federal government may take in response to the breach.

Federal Law Enforcement Use of Face Data

In the course of carrying out their law enforcement duties, various federal law enforcement agencies make use of image capturing, including LPR, and facial recognition technologies. For instance, as part of its responsibility to develop and implement an automatic biometric entry and exit control system for noncitizen travelers into and out of the country, CBP is using a variety of technologies to assist with biometric matching. An article in the *Washington Post* stated that "CBP makes extensive use of cameras and video recordings at airports and land border crossings, where images of vehicles are captured. Those images are used as part of a growing agency facial-recognition program designed to track the identity of people entering and exiting the [United States]." Notably, it is unclear whether any images exposed in the recent breach of CBP data may be used in CBP's facial recognition program. CBP is not the only federal agency capturing images containing faces; the FBI, Drug Enforcement Administration, and U.S. Immigration and Customs Enforcement, among others, rely on such information as well.

The breach of CBP image data held by a subcontractor highlights ongoing questions about the vulnerability of facial image data captured by the government. Specifically, there are concerns around the collection, use, and protection of these images. These concerns have manifested in actions such as city, state, and federal level efforts to prohibit or bound companies' and law enforcement's use of facial recognition technology.

In light of these issues, policymakers may continue oversight of federal law enforcement acquisition and use of technologies such as facial recognition and LPR systems as well as agencies' storage and protection of data. Moreover, they may consider benefits to law enforcement alongside risks to data privacy and security. Policymakers may also examine agencies' oversight of contractors involved in developing or maintaining these technologies. For instance, some have noted that "[b]reaches of government contractors have been a persistent security issue." Indeed, while the breach discussed here involved CBP data, the data had purportedly been downloaded to a subcontractor's network—reportedly in violation of CBP security and privacy rules—where it was subsequently exposed in the breach. As such, lawmakers may question what measures federal agencies have in place to ensure the security of data used by or in the possession of its contractors.