One out of two Americans in facial recognition databases

Shelley Connor
20 October 2016

Over 117 million Americans—half of the adult population—are in facial recognition databases used by law enforcement, according to a report released by Georgetown Law's Center on Privacy and Technology. The report, which the authors call "the most comprehensive survey to date of law enforcement face recognition," took a year to complete.

The report--titled "The Perpetual Lineup"--opens with a hypothetical situation. "There is a knock on your door. It's the police. There was a robbery in your neighborhood. They have a suspect in custody and an eyewitness. But they need your help: Will you come down to the station to stand in the line-up?"

Most Americans would find such an occurrence bizarre, and would accordingly object. Police lineups generally are composed of individuals with a criminal record. Due to facial recognition software and databases, though, the report contends, half of American adults unwittingly participate in a never-ending virtual lineup.

The authors proceed to outline the methods that law enforcement agencies throughout the US use to obtain and store photographic images of wide swaths of citizens, regardless of their criminal history.

Facial recognition software exists, along with fingerprinting and DNA evidence, on a continuum of what is known as biometric data. Biometric data uses the physical features of a person's body to identify them. As the report points out, though, facial recognition algorithms and photographic storage differs significantly from fingerprinting or other biometrics. These differences make the gathering and storage of photographic images both uniquely useful for law enforcement and distinctly problematic for the American public.

Fingerprints can only be left by a person who has actually deigned to touch an item. Photographs, by contrast, can be obtained by surveillance cameras, smart phones, social media sites, and driver licenses, in situations wherein individuals have no choice, and in most cases, no knowledge that their photographs are even being taken. "Face recognition isn't just a different biometric," the report states; "those differences allow for a different *kind of tracking* that can occur from far away, in secret, and on large numbers of people."

This is not, as the report makes clear, 'business as usual.' Taking peoples' photos without their consent or even knowledge represents a threat to constitutional rights. The practice allows for serious incursions against the First Amendment rights to peaceable assembly and freedom of speech, as well as Fourth Amendment rights against illegal search and seizure.

Police have already begun using facial recognition software, geolocation, and other real-time data in ways that violate the spirit of both the First and Fourth Amendments.

Earlier in October, the American Civil Liberties Union issued a statement on the cooperation between Baltimore Police Department (BPD) and a private company called Geofreedia, in which Geofreedia supplied police with information from private citizens' Facebook, Twitter, and Instagram accounts, during the protests and vigils following the police murder of Freddie Gray in 2015. Information supplied included protesters' photographs, locations, and hashtags.

While both police and Geofreedia have insisted that these data were used in order to monitor and proactively address growing unrest, the BPD used facial recognition software alongside information Geofreedia supplied in order to search for people with outstanding warrants amongst the protesters. Such

practices provide pretexts for the effective curtailment of freedom of assembly.

Baltimore is not the only municipal government to use such a service. Denver, Los Angeles, and New York have all admitted to using either Geofreedia or similar searches. Several social media sites, including Twitter, ended their agreements with Geofreedia earlier in the week due to fallout from the ACLU report.

In addition to the novel and problematic use of facial recognition software to do real-time surveillance, the secretive way which law enforcement agencies use this technology raises questions.

The Government Accountability Office revealed earlier this year that 16 states allow the FBI to use state driver license photos in facial recognition searches. These states handed over their citizens' photographs without obtaining their consent or informing them.

It should be assumed that state and municipal governments are taking even greater liberties with facial recognition technology behind the public's back. In response to requests for information on its use of facial recognition algorithms, New York Police Department and the Los Angeles Police Department simply refused to cooperate with the Center for Privacy and Technology's researchers. Other police departments, notably Baltimore and Denver, acknowledged that they used the technology but would not give specific instances of its use.

Law enforcement increasingly seeks, against overwhelming public opposition, to extend its reach well beyond its constitutional limits. The use of deadly force, the use of "resisting arrest" as reason in and of itself to arrest citizens, and tortuously attenuated interpretations of probable cause all signify a growth of law enforcement's power in direct contravention of constitutional principles.