US Police Capture 117 Million In Facial Recognition Systems

Massive nationwide study in 2006 reveals that thirty-six percent of Americans are in a facial recognition database, and the number is growing rapidly. Law enforcement is mostly unregulated and agencies are free to drift toward a police state reality. TN Editor

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 people would probably answer “no.” This summer, the Government Accountability Office revealed that close to 64 million Americans do not have a say in the matter: 16 states let the FBI use face recognition technology to compare the faces of suspected criminals to their driver’s license and ID photos, creating a virtual line-up of their state residents. In this line-up, it’s not a human that points to the suspect—it’s an algorithm.

But the FBI is only part of the story. Across the country, state and local police departments are building their own face recognition systems, many of them more advanced than the FBI's. We know very little about these systems. We don't know how they impact privacy and civil liberties. We don't know how they address accuracy problems. And we don't know how any of these systems—local, state, or federal—affect racial and ethnic minorities.

This report closes these gaps. The result of a year-long investigation and over 100 records requests to police departments around the country, it is the most comprehensive survey to date of law enforcement face recognition and the risks that it poses to privacy, civil liberties, and civil rights. Combining FBI data with new information we obtained about state and local systems, we find that law enforcement face recognition affects over 117 million American adults. It is also unregulated. A few agencies have instituted meaningful protections to prevent the misuse of the technology. In many more cases, it is out of control.

The benefits of face recognition are real. It has been used to catch violent criminals and fugitives. The law enforcement officers who use the technology are men and women of good faith. They do not want to invade our privacy or create a police state. They are simply using every tool available to protect the people that they are sworn to serve. Police use of face recognition is inevitable. This report does not aim to stop it.

Rather, this report offers a framework to reason through the very real risks that face recognition creates. It urges Congress and state legislatures to address these risks through commonsense regulation comparable to the Wiretap Act. These reforms must be accompanied by key actions by law enforcement, the National Institute of Standards and Technology (NIST), face recognition companies, and community leaders.

Key Findings

Our general findings are set forth below. Specific findings for 25 local and state law enforcement agencies can be found in our **Face Recognition Scorecard**, which evaluates these agencies' impact on

privacy, civil liberties, civil rights, transparency and accountability. The records underlying all of our conclusions are available online.

Law enforcement face recognition networks include over 117 million American adults.

Face recognition is neither new nor rare. FBI face recognition searches are more common than federal court-ordered wiretaps. At least one out of four state or local police departments has the option to run face recognition searches through their or another agency's system. At least 26 states (and potentially as many as 30) allow law enforcement to run or request searches against their databases of driver's license and ID photos. Roughly one in two American adults has their photos searched this way.

Different uses of face recognition create different risks. This report offers a framework to tell them apart.

A face recognition search conducted in the field to verify the identity of someone who has been legally stopped or arrested is different, in principle and effect, than an investigatory search of an ATM photo against a driver's license database, or continuous, real-time scans of people walking by a surveillance camera. The former is targeted and public. The latter are generalized and invisible. While some agencies, like the San Diego Association of Governments, limit themselves to more targeted use of the technology, others are embracing high and very high risk deployments.

By tapping into driver's license databases, the FBI is using biometrics in a way it's never done before.

Historically, FBI fingerprint and DNA databases have been primarily or exclusively made up of information from *criminal* arrests or investigations. By running face recognition searches against 16 states' driver's license photo databases, the FBI has built a biometric network that primarily includes *law-abiding Americans*. This is unprecedented and highly problematic.

Major police departments are exploring face recognition on live surveillance video.

Major police departments are exploring real-time face recognition on live surveillance camera video. Real-time face recognition lets police

continuously scan the faces of pedestrians walking by a street surveillance camera. It may seem like science fiction. It is real. Contract documents and agency statements show that at least five major police departments—including agencies in Chicago, Dallas, and Los Angeles—either claimed to run real-time face recognition off of street cameras, bought technology that can do so, or expressed a written interest in buying it. Nearly all major face recognition companies offer real-time software.

Law enforcement face recognition is unregulated and in many instances out of control.

No state has passed a law comprehensively regulating police face recognition. We are not aware of any agency that requires warrants for searches or limits them to serious crimes. This has consequences. The Maricopa County Sheriff's Office enrolled all of Honduras' driver's licenses and mug shots into its database. The Pinellas County Sheriff's Office system runs 8,000 monthly searches on the faces of seven million Florida drivers—without requiring that officers have even a reasonable suspicion before running a search. The county public defender reports that the Sheriff's Office has never disclosed the use of face recognition in *Brady* evidence.

Law enforcement agencies are not taking adequate steps to protect free speech.

There is a real risk that police face recognition will be used to stifle free speech. There is also a history of FBI and police surveillance of civil rights protests. Of the 52 agencies that we found to use (or have used) face recognition, we found only one, the Ohio Bureau of Criminal Investigation, whose face recognition use policy expressly prohibits its officers from using face recognition to track individuals engaging in political, religious, or other protected free speech.

Most law enforcement agencies do little to ensure their systems are accurate.

Face recognition is less accurate than fingerprinting, particularly when used in real-time or on large databases. Yet we found only two agencies, the San Francisco Police Department and the Seattle region's South Sound 911, that conditioned purchase of the technology on accuracy

tests or thresholds. There is a need for testing. One major face recognition company, FaceFirst, publicly advertises a 95% accuracy rate but disclaims liability for failing to meet that threshold in contracts with the San Diego Association of Governments. Unfortunately, independent accuracy tests are voluntary and infrequent.

The human backstop to accuracy is non-standardized and overstated.
Companies and police departments largely rely on police officers to decide whether a candidate photo is in fact a match. Yet a recent study showed that, without specialized training, human users make the wrong decision about a match half the time. We found only eight face recognition systems where specialized personnel reviewed and narrowed down potential matches. The training regime for examiners remains a work in progress.

Police face recognition will disproportionately affect African Americans.
Police face recognition will disproportionately affect African Americans. Many police departments do not realize that. In a Frequently Asked Questions document, the Seattle Police Department says that its face recognition system "does not see race." Yet an FBI co-authored study suggests that face recognition may be less accurate on black people. Also, due to disproportionately high arrest rates, systems that rely on mug shot databases likely include a disproportionate number of African Americans. Despite these findings, there is no independent testing regime for racially biased error rates. In interviews, two major face recognition companies admitted that they did not run these tests internally, either.

Agencies are keeping critical information from the public.
Ohio's face recognition system remained almost entirely unknown to the public for five years. The New York Police Department acknowledges using face recognition; press reports suggest it has an advanced system. Yet NYPD denied our records request entirely. The Los Angeles Police Department has repeatedly announced new face recognition initiatives—including a "smart car" equipped with face recognition and real-time face recognition cameras—yet the agency claimed to have "no records responsive" to our document request. Of 52 agencies, only four (less than 10%) have a publicly available use policy. And only one

agency, the San Diego Association of Governments, received legislative approval for its policy.

Major face recognition systems are not audited for misuse.

Maryland's system, which includes the license photos of over two million residents, was launched in 2011. It has never been audited. The Pinellas County Sheriff's Office system is almost 15 years old and may be the most frequently used system in the country. When asked if his office audits searches for misuse, Sheriff Bob Gualtieri replied, "No, not really." Despite assurances to Congress, the FBI has not audited use of its face recognition system, either. Only nine of 52 agencies (17%) indicated that they log and audit their officers' face recognition searches for improper use. Of those, only one agency, the Michigan State Police, provided documentation showing that their audit regime was actually functional.

Read full story here…