Driver’s License Photos of Almost Half of US Adults Now Are Being Used in Virtual Line-Ups by Law Enforcement

Sixteen states allow the FBI to 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 addition, state and local police departments across the country are building their own face-recognition systems. Law enforcement networks include over 117-million American adults. It is unknown how this impacts privacy, civil liberties, or even accuracy of results. -GEG

I. Executive Summary

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.

One in two American adults is in a law enforcement face recognition network.

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.

A. 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**,whichevaluates
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.]

Read full article here…