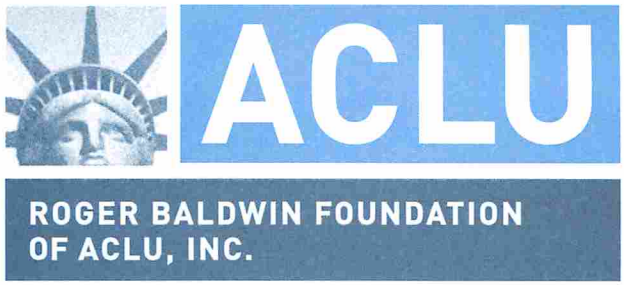
THE
ROGER
BALDWIN
FOUNDATION
OF ACLU,
INC.

SUITE 2300
180 NORTH MICHIGAN AVENUE
CHICAGO, ILLINOIS 60601-1287
(312) 201-9740
FAX (312) 201-9760
WWW.ACLU-IL.ORG



October 18, 2016

Via US Mail and Fax

Rahm Emanuel, Mayor
Office of the Mayor
121 N. LaSalle Street
Chicago City Hall 4th Floor
Chicago, IL 60602
Fax: 312-744-2324

Eddie T. Johnson, Superintendent
Chicago Police Department
3510 S. Michigan Avenue
Chicago, IL 60653
Fax: 312-745-6963

Dear Mayor Emanuel and Superintendent Johnson,

We are writing because the Chicago Police Department's ("CPD") face recognition policies are wholly inadequate to protect the rights of individuals in Chicago. The use of this technology represents a threat to the privacy to over 117 million American adults, whose driver's license and ID photos may regularly be subject to face recognition searches without their consent or even knowledge. In particular, a report issued today by the Center on Privacy & Technology at Georgetown Law ("the report") found that the use of face recognition is likely to have a disparate impact on racial and ethnic minorities, and, in particular, African Americans. Thus, we urge you to issue a moratorium on the use of face recognition until appropriate safeguards can be put in place. Such safeguards should include explicit legislative consideration of whether to approve the use of this new, invasive technology.

According to the report, CPD has the ability to conduct face recognition searches against databases containing mugshots, and may also have the ability to conduct searches against the driver's license and ID photos of everyone in Illinois. Despite its widespread capabilities, however, CPD's face recognition system lacks even baseline oversight, accountability, or transparency requirements, raising First and Fourth Amendment concerns. CPD's face recognition has apparently never been audited for misuse, bias, or inaccuracy. In addition, there appears to be no requirements that restrict searches to serious crimes where law enforcement has reason to believe that someone has committed a crime. Moreover, CPD does not have a policy that expressly prohibits officers from using face recognition to track individuals engaged in First Amendment protected activities.

Such a lack of safeguards is stunning given the growing evidence that face recognition in its current form is not simply a neutral investigative tool – but rather can be a biased technology that has a disparate impact on racial and ethnic minorities. A prominent 2012 study, co-authored by an FBI expert, found that several leading face recognition algorithms were 5 to 10 percent

less accurate on African Americans, women, and young people aged 18 to 30 than whites, men, and older people.[1] Such inaccuracies raise the risk that, absent appropriate safeguards, innocent African Americans and others may mistakenly be placed on a suspect list or investigated for a crime solely because a flawed algorithm failed to identify the correct suspect.

The effect of these biased algorithms is compounded by the fact that African Americans and other racial and ethnic minorities are likely overrepresented in the mugshot database that CPD relies on for face recognition. Specifically, in Cook County, people of color are arrested at a rate almost twice as high as their share of the population.[2] Thus, they are more likely to be included in such a database, even if they were never charged or convicted of a crime. In addition, they may be disproportionately likely to have encounters to police that subsequently result in a face recognition search. Thus, face recognition is least accurate for the population that it is most likely to be used against.

Given the evidence of disparate impact, CPD should not continue to use face recognition technology without appropriate safeguards. Thus, we urge CPD to issue a moratorium on the use of this technology until the adoption of proper safeguards, including:

- **Legislative Approval:** A surveillance technology of this magnitude should not be used without explicit legislative approval, which permits adequate opportunity for community engagement. If the legislature is to approve use of the technology, legislation should explicitly require individualized suspicion for face recognition searches, require robust auditing for bias and accuracy, and provide a remedy in cases where individuals' rights are violated.

- **Robust Internal Audits:** Law enforcement agencies should conduct robust and regular internal audits of their face recognition systems. Such audits should assess algorithmic accuracy and bias on the basis of race, gender, and age. In addition, such audits identify instances of misuse, and monitor the frequency and purposes for which the technology is used.

- **Individualized Suspicion:** Searches of mugshots should require individualized suspicion of criminal conduct, and in cases not involving in-person encounters, should only be performed as part of felony investigations. Mugshot databases should be scrubbed to exclude individuals who were found innocent of a crime or had charges dropped or dismissed and assessed to ensure their accuracy.

- **Transparency:** The public and legislators have the right to know how law enforcement officials are using this new technology. Thus, law enforcement officials should publicly report statistics on how often face recognition is used, the race, ethnic, gender, and age breakdown of the people it is used against, and the number of times use of face

---

[1] Brendan F. Klare et al., *Face Recognition Performance: Role of Demographic Information*, 7 *IEEE Transactions on Information Forensics and Security* 1789, 1797 (2012).

[2] http://www.icjia.state.il.us/sac/tools/DataProfiles/CriminalJusticeDataProfiles.cfm?ProfileNumber=10&ICJIANumber=1088&getProfile=1.

recognition leads to an arrest or prosecution. In addition, any audits of face recognition systems should be made public.

- **Restriction on the use of Civilian Databases:** Individuals should not have to sacrifice their privacy simply to obtain a driver's license. Indeed, law enforcement use of civilian databases for face recognition sets a dangerous precedent – opening the door to the possibility that sensitive information collected for non-law enforcement purposes can be routinely searched by police. Such a precedent could apply to other types of information, such as library, financial, or medical records. Thus, there should generally be a prohibition on the use of civilian databases for face recognition.

- **Prohibition on Real-Time Use:** Real-time face recognition would fundamentally redefine the privacy of individuals in public spaces, allowing the government to track large numbers of individuals in real-time. As the Supreme Court noted in *Jones*,[3] such data can provide insight into the most intimate details of individuals' lives, including visits to a doctor, place of worship, or political campaign office. Thus, real-time face recognition should be prohibited, unless it is a true emergency and surveillance is limiting in duration, geography, and scope.

- **First Amendment Protections:** The use of facial recognition has the potential to chill free speech. Thus, law enforcement agencies should be prohibited from using face recognition technology on individuals based on their First Amendment-protected activities.

Very truly yours,

Karen Sheley
Director, Police Practices Project

cc: Stephen R. Patton, Corporation Counsel
City of Chicago
121 N. LaSalle Street, Suite 600
Chicago, IL 60602
(via email at Stephen.Patton@cityofchicago.org)

Charise Valente, General Counsel
Chicago Police Department
3510 S. Michigan Avenue
Chicago, IL 60653
(via email at Charise.Valente@chicagopolice.org)

[3] U.S. v Jones, 132 S.Ct. 945 (2012).