



October 18, 2016

Vanita Gupta
Principal Deputy Assistant Attorney General
U.S. Department of Justice, Civil Rights Division
950 Pennsylvania Ave. NW
Washington, D.C. 20530

Dear Principal Deputy Assistant Attorney General Gupta:

On behalf of the 52 undersigned civil liberties, civil and human rights, immigrant rights, faith, digital rights and transparency organizations, we write to express our deep concern regarding the use of face recognition technology by federal, state, and local law enforcement agencies.¹ A growing body of evidence, including a report released today by the Center on Privacy & Technology at Georgetown Law (“the Georgetown report”), suggests that law enforcement use of face recognition technology is having a disparate impact on communities of color, potentially exacerbating and entrenching existing policing disparities.² Face recognition systems are powerful—but they can also be biased. Thus, we urge the Department of Justice (DOJ) Civil Rights Division (CRT) to:

1. Expand ongoing investigations of police practices, and include in future investigations an examination of whether the use of surveillance technologies, including face recognition technology, has had a disparate impact on communities of color; and
2. Consult with and advise the Federal Bureau of Investigation (FBI) to examine whether the use of face recognition technologies has had a disparate impact on communities of color.

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 than Caucasians.³ Such inaccuracies raise the risk that, absent appropriate safeguards, innocent African Americans may mistakenly be placed

¹ Many of the of these organizations have written to Congress and the FBI previously, expressing concerns regarding the FBI NGI system and proposals to exempt it from provisions of the privacy act. See Electronic Privacy Information Center, *Coalition Letter to Congress Regarding the FBI’s Use of Facial Recognition and Proposal to Exempt the Bureau’s Next Generation Identification Database from Privacy Act Obligations* (June 23, 2016), <https://epic.org/privacy/fbi/NGI-Congressional-Oversight-Letter.pdf>. See also, Electronic Frontier Foundation, *Comment Letter on Proposed Exemption of FBI’s Next Generation Identification (NGI) System from Key Provisions of the Privacy Act of 1974* (July 6, 2016), https://www.eff.org/files/2016/07/06/eff_comments_on_proposed_privacy_act_exemptions_and_sorn_for_fbi_ngi_system.pdf.

² See Clare Garvie, Alvaro M. Bedoya, & Jonathan Frankle, *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, Center on Privacy & Technology at Georgetown Law (Oct. 18, 2016) available at <http://www.perpetuallineup.org>.

³ Brendan F. Klare et al., *Face Recognition Performance: Role of Demographic Information*, 7 *IEEE Transactions on Information Forensics and Security* 1789, 1797 (2012), <http://openbiometrics.org/publications/klare2012demographics.pdf>.

on a suspect list or investigated for a crime *solely because a flawed algorithm failed to identify the correct suspect*. Despite these findings, there is no regular, independent testing regime for racial bias in face recognition algorithms. In fact, the Georgetown report found that two major face recognition vendors did not conduct internal tests for bias either.

The effect of these inaccuracies is compounded by the fact that biased policing practices often mean that African Americans and other people of color are also likely to be overrepresented in the mugshot databases that many jurisdictions rely on for face recognition. For example, the report found that African Americans are likely overrepresented in the face recognition repository searched by the Baltimore Police Department (BPD), in part because they are arrested at a rate close to twice as high as their share of the state population. Similarly, African Americans are likely overrepresented in the face recognition database used by Maricopa County Sheriff's Office (MCSO) since they are arrested at a rate three times higher than their share of the state population. The database used by MCSO also includes every Honduran driver's license and booking photo—a particularly disturbing fact given court findings that Maricopa County has engaged in unconstitutional stops, arrests, and detentions of Hispanics.⁴

Neither Maryland nor Arizona has a statute in place to restrict police use of face recognition. The face recognition system used by BPD has never been audited for misuse, and it appears that the MCSO system has not been audited either. In fact, the MCSO system does not even require that an officer have reasonable suspicion that someone has conducted a crime before the police can search their face against a face recognition database. The Georgetown report found that only nine of the 52 agencies reporting use of face recognition had any type of auditing requirement—and that only one in 52 had a clearly functioning audit regime. Indeed, the FBI has yet to conduct even one audit of its own face recognition systems,⁵ and continues to disclaim responsibility for assessing the accuracy of the partner state and federal systems that it uses on a daily basis. In other words, the FBI is leading by bad example, and many jurisdictions are following.

Moreover, there is evidence that this technology is being used at protests and rallies, raising significant First Amendment concerns. Specifically, an investigation by the ACLU of North California, the Center for Media Justice, and ColorofChange.org revealed that the Baltimore Police Department had used face recognition technology, in conjunction with social media monitoring tools, to locate, identify, and arrest certain protesters in the wake of Freddy Gray's death.⁶

Such facts are particularly disturbing given that face recognition technology is increasingly being used by federal, state, and local law enforcement for routine investigations, and face recognition networks have grown to include half of all American adults. According to the Georgetown report, more than 117 million American adults are included in face recognition networks across the country, and at least one in four state or local police departments can run facial recognition searches through their own network or the

⁴ Melendres v. Arpaio, et. al., 598 F.Supp.2d 1025 (D. Ariz. Feb. 10, 2009).

⁵ Government Accountability Office, *Face Recognition Technology: FBI Should Better Ensure Privacy and Accuracy, 10* (May 2016), available at <http://www.gao.gov/assets/680/677098.pdf>.

⁶ See Russell Brandom, *Facebook, Twitter, and Instagram Surveillance Tool Was Used to Arrest Baltimore Protestors*, THE VERGE (Oct. 11, 2016), <http://www.theverge.com/2016/10/11/13243890/facebook-twitter-instagram-police-surveillance-geofeedia-api>.

network of another agency. For example, the Sheriff's Office in Pinellas County, Florida alone estimates that more than 8,000 face recognition searches are conducted on its system every month. Similarly, the FBI is expanding the reach of its face recognition unit (FACE Services), through which it can access more than 30 million photos in its own database and scan the driver's license photos of 16 states.⁷ From August 2011 through December 2015, the FBI requested nearly 215,000 searches of external partners' databases alone.⁸

Thus, face recognition technology is rapidly being interconnected with everyday police activities, impacting virtually every jurisdiction in America. Yet, the safeguards to ensure this technology is being used fairly and responsibly appear to be virtually nonexistent.

Examination of face recognition technologies and their impacts fits squarely within the jurisdiction of the DOJ CRT. It is also particularly incumbent on the DOJ CRT to examine this issue given that the federal government has funded the acquisition of state and local face recognition systems with little consideration of whether appropriate protections are in place. For example, in Pinellas County, Florida, the Sheriff's Office only initiated its law enforcement face recognition program after receiving a grant awarded by the DOJ's Office of Community Oriented Policing Services (COPS).⁹ If the use of face recognition technologies is contributing to disparities, it calls into question whether this is a responsible use of federal funds and may violate Title VI of the Civil Rights Act of 1964, thus requiring the withdrawal of federal funds to such agencies.

Face recognition technology has enormous civil liberties implications and its use must be closely examined to ensure that it is not violating Americans' civil rights. We stand ready to work with you to ensure that the voices of our communities are heard in this important, ongoing national conversation. If you have any questions, please contact Neema Singh Guliani (nguliani@aclu.org or 202-675-2322) or Sakira Cook (cook@civilrights.org or 202-263-2894).

Sincerely,

18millionrising.org

A. Philip Randolph Institute

Advocacy for Principled Action in Government

American Civil Liberties Union

Amnesty International USA

Arab American Institute

American-Arab Anti-Discrimination Committee

Asian Americans Advancing Justice - Asian Law Caucus

Asian Pacific American Labor Alliance, AFL-CIO

Bill of Rights Defense Committee/Defending Dissent Foundation

Center for Democracy & Technology

⁷ GAO, *supra* note 5.

⁸ *Id.*

⁹ According to the findings of the Georgetown report, the San Diego Association of Governments and Seattle systems also appear to be funded by DHS Urban Security Initiative Grants.

Center for Media Justice
Color of Change
Constitutional Alliance
The Constitution Project
Consumer Action
Consumer Watchdog
Council on American-Islamic Relations (CAIR)
Demand Progress
Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
Equity Matters
Fight for the Future
Free Press
Hip Hop Caucus
The Innocence Project
The Lawyers' Committee for Civil Rights Under Law
The Leadership Conference on Civil and Human Rights
MPower Change
Media Alliance
Media Mobilizing Project
MommieActivist and Sons
MomsRising
NAACP
National Action Network
National Association of Social Workers (NASW)
National Center for Transgender Equality
National Council of Churches
National Employment Law Project
National Immigration Law Center
National Network for Arab American Communities
New America's Open Technology Institute
Oakland Privacy
OneAmerica (Washington State)
OpenTheGovernment.org
Restore The Fourth
South Asian Americans Leading Together
Sunlight Foundation
Transformative Justice Coalition
Women Who Never Give Up
United Church of Christ, OC Inc.
UNITED SIKHS