SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

40 Rector Street, 9th Floor
New York, New York 10006
www.StopSpying.org | (646) 602-5600

COMMENT OF
EVAN ENZER AND ALBERT FOX CAHN
OF THE
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

TO THE
OFFICE OF ATTORNEY GENERAL

IN RESPONSE TO
PUBLIC INPUT ON REGULATING LAW ENFORCEMENT'S USE OF FACIAL RECOGNITION TECHNOLOGY

SUBMITTED
MARCH 11, 2022

Introduction.

The Surveillance Technology Oversight Project ("S.T.O.P.") is a community-based civil rights group that advocates and litigates against discriminatory surveillance at state and local levels. Our work highlights the impact of surveillance on Muslim Americans, immigrants, the LGBTQ+ community, indigenous peoples, and communities of color, particularly the unique trauma of anti-Black policing. We write to emphasize the harms inherent to facial recognition and urge the Office of the Attorney General ("OAG") to end its use.

New Jersey must ban government facial recognition entirely—adopting new rules is not enough. In fact, any use of facial recognition will violate the OAG's own guiding principles for facial recognition technology.[1] There is no acceptable way to collect biometric identifiers, no way to regulate away dragnet surveillance, and facial recognition's inaccuracy leaves no reasonable way to justify arrests. Even if technically perfect facial recognition existed, its application would still be discriminatory. New Jersey must not open the door to this dangerous technology.

Facial recognition endangers New Jersey.

A. Facial recognition's abusive applications.

Facial recognition can identify any person, at any time, in any place—giving its operator incredible power. Facial recognition surveils religious centers, abortion clinics, and protests to an otherwise impossible degree.

Given New Jersey's history of allowing abusive and unlawful surveillance, this is not a technology we can trust the police to take.[2] New Jersey police have a documented history of targeting the state's black residents.[3] Additionally, the OAG permitted out-of-state police to secretly film, photograph, and map entire religious communities,[4] violating the constitution.[5] Facial recognition would enable police to carry out these violations on a much larger scale.[6]

Facial recognition poses dangers for those who are seeking abortions. New Jersey has affirmed the right to choose,[7] but other states are moving in the opposite direction.[8] Problematically, Texas punishes friends who help friends travel to New Jersey for an abortion.[9] As long as New Jersey uses facial recognition,

---

[1] New Jersey Office of the Attorney General, "Facial Recognition Technology," last visited March 3, 2022, https://www.njoag.gov/facialrecognition/.
[2] "NJ Official: NYPD Muslim Surveillance Legal," accessed March 9, 2022, https://www.cbsnews.com/news/nj-official-nypd-muslim-surveillance-legal/. United States Department of Justice, Civil Rights Division, Investigation of the Newark Police Department, July 22, 2014, https://www.justice.gov/sites/default/files/crt/legacy/2014/07/22/newark_findings_7-22-14.pdf.
[3] United States Department of Justice, Civil Rights Division *supra* note 2
[4] Hasan v. City of New York, No. 2:12-cv-03401-SDW- MCA (D. N.J., October 3, 2012) (amended complaint), https://ccrjustice.org/sites/default/files/assets/10_First%20Amended%20Complaint.10.3.2012.pdf. "NJ Official: NYPD Muslim Surveillance Legal," accessed March 9, 2022, https://www.cbsnews.com/news/nj-official-nypd-muslim-surveillance-legal/.
[5] *See* U.S. Const. Amend. 1, 14.
[6] "How Accurate Are Facial Recognition Systems – and Why Does It Matter?," accessed March 4, 2022, https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter. "Law Enforcement," Clearview AI, accessed March 7, 2022, https://www.clearview.ai/law-enforcement.
[7] Sophie Nieto-Munoz, "Murphy Signs Law Solidifying Abortion Rights in New Jersey," New Jersey Monitor, January 13, 2022, https://newjerseymonitor.com/2022/01/13/murphy-signs-law-solidifying-abortion-rights-in-new-jersey/.
[8] Alan Feuer, "The Texas Abortion Law Creates a Kind of Bounty Hunter. Here's How It Works.," The New York Times, September 10, 2021, https://www.nytimes.com/2021/09/10/us/politics/texas-abortion-law-facts.html.
[9] S.B. 8, 87th Texas Legislature, 2022, https://legiscan.com/TX/text/SB8/id/2395961.

it threatens pregnant people seeking to exercise their reproductive rights. New Jersey surveillance data could easily flow to anti-choice states through state-federal information-sharing agreements and public-private partnerships.

Finally, police frequently deploy facial recognition to watch protestors. Continuing its long history of racism,[10] Baltimore police illegally and forcibly arrested a Black man named Freddie Gray in 2016.[11] Gray pleaded for medical attention, which the department denied…they kept him in custody as he passed away.[12] Too often, justice fails to hold police accountable when they kill Black men, but in this instance, the tragic murder inspired passionate cries for reform.[13] Instead of working with concerned citizens, police treated the protests as an opportunity to identify people with "outstanding warrants."[14] They used facial recognition to surveil thousands of protestors, criminalizing their speech, to track people on unrelated charges.[15] Permitting facial recognition in New Jersey could result in similar abuse.

B. Even a "perfect" facial recognition system is discriminatory.

Even if the OAG adopts non-discriminatory facial recognition software, the technology will still have a discriminatory impact. Law enforcement targets BIPOC communities at higher rates than their white counterparts,[16] and technology entrenches the established discrimination at every phase of policing and prosecution.[17] Where law enforcement gives white residents the benefit of the doubt, BIPOC residents face only baseless suspicion. Not only is facial recognition more likely to be targeted at BIPOC neighborhoods, but police are more likely to target BIPOC residents based on those surveillance systems' findings.[18] New Jersey already fills its prisons with its Black citizens.[19] Facial recognition will fill them with more.

The OAG understood facial recognition's dangers when it banned one of the most well-known facial recognition vendors, Clearview AI. In 2019, facial recognition misidentified a New Jersey resident named Nijeer Parks, and police jailed him for over a week.[20] Consistent with the growing national pattern of algorithmic profiling,[21] Mr. Parks, like so many others wrongfully arrested by facial recognition, is Black.[22] Later in 2020, former Attorney General Grewal learned about Clearview's technology and immediately

---

[10] German Lopez, "The 14 Worst Cases of Outright Racism the Justice Department Saw in Baltimore Police," Vox, August 10, 2016, https://www.vox.com/2016/8/10/12423474/baltimore-police-justice-department-racism.
[11] "Freddie Gray's Death in Police Custody – What we Know," B.B.C. News, May 23, 2016, https://www.bbc.com/news/world-us-canada-32400497.
[12] *Id.*
[13] *See id.*
[14] *See* Jameson Spivak, "Maryland's Face Recognition System is one of the Most Invasive in the Nation," Baltimore Sun, March, 9, 2020, https://www.baltimoresun.com/opinion/op-ed/bs-ed-op-0310-face-recognition-20200309-hg6jkfav2fdz3ccs55bvqjtnmu-story.html.
[15] *See id.*
[16] National Association of Criminal Defense Lawyers, "Garbage In, Gospel Out," 2021, https://www.nacdl.org/Document/GarbageInGospelOutDataDrivenPolicingTechnologies.
[17] *Id.*
[18] *Id.*
[19] The Sentencing Project, "The Color of Justice," 2021, https://www.sentencingproject.org/wp-content/uploads/2016/06/The-Color-of-Justice-Racial-and-Ethnic-Disparity-in-State-Prisons.pdf.
[20] Asa Fitch, "Facial-Recognition Tools in Spotlight in New Jersey False-Arrest Case," Wall Street Journal, December 29, 2020, https://www.wsj.com/articles/facial-recognition-tools-in-spotlight-in-new-jersey-false-arrest-case-11609269719.
[21] Tom Simonite, "The Best Algorithms Still Struggle to Recognize Black Faces," Wired, July 22, 2019, https://www.wired.com/story/best-algorithms-struggle-recognize-black-faces-equally/.
[22] Khari Johnson, "How Wrongful Arrests Based on AI Derailed 3 Men's Lives," Wired, March 7, 2022, https://www.wired.com/story/wrongful-arrests-ai-derailed-3-mens-lives/..

understood its dangers.[23] He issued a moratorium on police use while the OAG evaluated the technology.[24] Two years hasn't solved discrimination. Now is the time to push forward; we must not regress on facial recognition.

C. Facial recognition compared to face credentials

Government facial recognition is very different from consumer products' face credential security features.[25] And it is far more dangerous.

Facial recognition software compares a photo of an unknown individual, a "probe image," to an extensive photo database called a "gallery."[26] The software determines which faces in the gallery look least dissimilar to the face in the probe photo and presents these faces as purported "matches."[27] In contrast, face credentials only scan one face at a time, comparing it to a gallery of one authorized user. Because facial recognition seeks to surveil the entire population, not just a single face, the technology is much more error-prone.[28] Whereas face credentials allow us to shift around our device's camera until it finds the optimal angle, facial recognition scans a single static image or video clip. Except for the extraordinarily rare circumstances that a suspect looks directly at a CCTV camera, under optimal lighting conditions, the image quality and facial recognition accuracy will be much worse.[29] Lastly, where a lousy face credential scan, at worst, prompts us to enter our password, a flawed facial recognition search can rob us of our freedom.

Facial recognition systems fail the OAG's guiding principles.

Facial recognition is incompatible with the OAG's stated principles. It is impossible to restrict improperly obtained images from the facial recognition gallery, prohibit dragnet surveillance, or justify arrests with facial recognition.[30]

A. Facial recognition does not compile gallery images properly.

The OAG's first principle excludes "improperly" collected photos from law enforcement's facial recognition gallery.[31] This seems only to exclude images that vendors acquire in violation of law or corporate terms of service.[32] This is not enough to build an ethical or proper database. Even correctly licensed photographs will exacerbate discrimination and skirt accepted data use practices.[33]

---

[23] Kashmir Hill, "New Jersey Bars Police from Using Clearview Facial Recognition App," New York Times, January 24, 2020, https://www.nytimes.com/2020/01/24/technology/clearview-ai-new-jersey.html.
[24] *Id.*
[25] *See* "About Face ID Advanced Technology," Apple Support, accessed March 3, 2022, https://support.apple.com/en-us/HT208108.
[26] *Id.*
[27] *Id.* Partnership on AI, "Understanding Facial Recognition Systems," 6, February 19, 2020, https://partnershiponai.org/wp-content/uploads/2021/08/Understanding-Facial-Recognition-Paper_final.pdf.
[28] Bennett Cyphers Sheard, et. al., "Face Recognition Isn't Just Face Identification and Verification: It's Also Photo Clustering, Race Analysis, Real-Time Tracking, and More," Electronic Frontier Foundation, October 7, 2021, https://www.eff.org/deeplinks/2021/10/face-recognition-isnt-just-face-identification-and-verification.
[29] Tim Cushing, "Las Vegas Police Are Running Lots Of Low Quality Images Through Their Facial Recognition System," Techdirt, August 12, 2020, https://www.techdirt.com/2020/08/12/las-vegas-police-are-running-lots-low-quality-images-through-their-facial-recognition-system/.
[30] New Jersey Office of the Attorney General, *supra* note 1.
[31] *Id.*
[32] *Id.*
[33] *Infra.*

The OAG understands that many facial recognition vendors compile galleries by scraping images from the internet.[34] Data protection officers call this practice "mass surveillance" and "unacceptable."[35] Even privacy-destroying platforms like Facebook asserted that scraping violates its terms of service,[36] and the United Kingdom claimed it violates its laws.[37] The OAG is correct in its decision to ban this shunned practice.[38]

But it is impossible to have a truly ethical gallery. For instance, if New Jersey followed the lead of jurisdictions that populate facial recognition galleries with mugshots,[39] the system would only identify previously incarcerated people, sixty-one percent of whom in New Jersey are Black, despite being only thirteen percent of the state's population.[40] This is one of the worst racial disparities among U.S. prison systems.[41] A facial recognition system built on mugshots would surveil Black New Jerseyans disproportionately to their white counterparts.[42]

A broader facial recognition gallery built on existing databases is just as bad.[43] People increasingly realize that repurposing data goes against the public's interest.[44] We've seen how facial recognition works with government power to achieve illegitimate goals, transforming this privacy problem into an existential threat to our civil rights and liberties.[45] To minimize risk, we must hold governments and vendors accountable to higher standards. Even the most basic governance principles reject repurposing data.[46] It is not a proper way to build a facial recognition gallery. The OAG should reject this practice.

B. Facial recognition is a dragnet.

The OAG's guiding principles say, "Any policy…must prohibit 'dragnet' surveillance."[47] But facial recognition is a dragnet. When there is a camera on every corner, law enforcement can identify any person, anywhere, anytime.[48]

---

[34] Leading developers train their systems and build databases by using open-source internet images. *See* Exposing.ai, last visited March 1, 2022, https://exposing.ai/datasets/.
[35] Office of the Privacy Commissioner of Canada, "News Release," February 3, 2021, https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/nr-c_210203/.
[36] Jon Porter, "Facebook and LinkedIn are Latest to Demand Clearview Stop Scraping Images for Facial Recognition Tech," The Verge, February 6, 2020, https://www.theverge.com/2020/2/6/21126063/facebook-clearview-ai-image-scraping-facial-recognition-database-terms-of-service-twitter-youtube.
[37] Tim Cushing, "UK Government Says Clearview Owes It $23 Million For Violating Privacy Laws," December 9, 2021, https://www.techdirt.com/2021/12/09/uk-government-says-clearview-owes-it-23-million-violating-privacy-laws/.
[38] New Jersey Office of the Attorney General, *supra* note 1.
[39] "Edmonton Police Using Facial Recognition Software to Search Mugshot Database," Global News, accessed March 7, 2022, https://globalnews.ca/video/8587770/edmonton-police-using-facial-recognition-software-to-search-mugshot-database/.
[40] The Sentencing Project, "The Color of Justice," 2021, https://www.sentencingproject.org/wp-content/uploads/2016/06/The-Color-of-Justice-Racial-and-Ethnic-Disparity-in-State-Prisons.pdf.
[41] *Id.*
[42] *See id.*
[43] Thomas Germain, "Federal Agencies Use DMV Photos for Facial Recognition. Here's What You Need to Know," Consumer Reports, July 8, 2019, https://www.consumerreports.org/privacy/federal-agencies-use-dmv-photos-for-facial-recognition-a1704098825/.
[44] Stefano Tagliabue, "The Working Party's Views on Purpose Limitation and Big Data," IAPP, August 13, 2013, https://iapp.org/news/a/the-working-partys-views-on-purpose-limitation-and-big-data/.
[45] *Supra,* Introduction.
[46] Tagliabue, *supra* note 44.
[47] New Jersey Office of the Attorney General, *supra* note 1.
[48] Cameras cover almost every intersection in New York City. *See* "Inside the NYPD's Surveillance Machine," last visited March 3, 2022, https://nypd-surveillance.amnesty.org/.

Government facial recognition is growing immensely. In New York City, there are tens of thousands of government CCTV cameras capable of supplying probe photos to facial recognition software.[49] From everyday work commutes to families visiting historical landmarks, the government sees all.[50] NYPD alone has used facial recognition in over 22,000 cases since 2017.[51] Police turned facial recognition into a "routine" tool for investigating non-violent offenses.[52] They promised that facial recognition would solve serious crimes but turned around to use it for policing "crimes of poverty."[53] Facial recognition is unquestionably a dragnet.

San Francisco starkly reveals how half measures and half-hearted protections will fail New Jersey. The city received international praise for restricting the surveillance technology.[54] But only a year later, San Francisco police weaponized the technology to target protestors, the exact type of abuse lawmakers sought to avoid.[55] How? Loopholes that let police use their digital dragnets under certain circumstances.[56] The lesson should be clear: Where you give police an inch of facial recognition, they monitor a mile.

C. Facial Recognition is unreliable; calling it a "lead" circumvents judicial review.

The OAG wants to prevent "the use of facial recognition technology as the sole basis for arresting or prosecuting an individual" by limiting "the use of this technology to generating investigative leads."[57] Instead of limiting facial recognition's harms, this will amplify them.

Facial recognition introduces error even when it is only a lead. When facial recognition finds a match, it still requires a human to confirm the identification.[58] People are comically terrible at identifying others.[59] Decades of research found that misidentification plays a role in 80% of wrongful convictions.[60] Memories are imperfect, minds are influenced, and emotions cloud perception.[61] Vendors sell facial recognition as a miracle cure to this problem, but it doesn't fix misidentification at all. Facial recognition just presents several people with similar features[62] and tells its audience, "One of them is the person you are looking for."[63] The

---

[49] "USA: Decode Surveillance NYC: Methodology," Amnesty International, accessed March 9, 2022, https://www.amnesty.org/en/documents/amr51/5205/2022/en/.
[50] "Look inside the NYPD's Surveillance Machine, *supra* note 48.
[51] "S.T.O.P. Condemns NYPD For 22K Facial Recognition Searches," The Surveillance Technology Oversight Project, accessed October 23, 2020, https://www.stopspying.org/latest-news/2020/10/23/stop-condemns-nypd-for-22k-facial-recognition-searches.
[52] Claire Merchlinsky, "'We Try to Use It as Much as We Can': How Facial Recognition Became a Routine Policing Tool in America," NBC News, accessed May 11, 2019, https://www.nbcnews.com/news/us-news/how-facial-recognition-became-routine-policing-tool-america-n1004251.
[53] *Id.*
[54] Laura Hautala, "San Francisco Becomes First City to bar Police from Using Facial Recognition," CNET, May 14, 2019, https://www.cnet.com/tech/services-and-software/san-francisco-becomes-first-city-to-bar-police-from-using-facial-recognition/.
[55] Maria Dinzeo, "Judge Mulls Legality of San Francisco Police's Use of Surveillance Cameras to Monitor Protesters," Courthouse News Service, February 1, 2022, https://www.courthousenews.com/judge-mulls-legality-of-san-francisco-polices-use-of-surveillance-cameras-to-monitor-protesters/.
[56] *Id.*
[57] New Jersey Office of the Attorney General, *supra* note 1.
[58] *Id.*
[59] American Psychological Association, "Eyewitness Accuracy in Police Lineups," 2014, https://www.apa.org/topics/forensics-law-public-safety/eyewitness-accuracy-police-lineups.
[60] *Id.*
[61] *Id.*
[62] New Jersey Office of the Attorney General, *supra* note 1.
[63] Reliance on biometric identification can lead to confirmation bias. Sidney Perkowitz, "The Bias in the Machine: Facial Recognition Technology and Racial Disparities," MIT Case Studies in Social and Ethical Responsibilities of Computing, no. Winter 2021 (February 5, 2021), https://doi.org/10.21428/2c646de5.62272586.

technology delivers pseudoscience to law enforcement under the guise of objectivity when it asks police and witnesses to guess whether one of the look-a-likes is the person in the probe photo. Even if facial recognition is "just a lead," it suffers from the same inaccuracies as eyewitness identification.

Worse, designating facial recognition as a "lead" enables prosecutors and police to circumvent judicial review. This came to light in neighboring New York City when police accused a man of stealing a pair of socks.[64] Police purported to identify him using facial recognition.[65] Then they texted a photo of the man to the store's security guard and asked, "Is this him?"[66] But the court never reviewed the technology.[67] The police technically based the arrest warrant on witness identification, not facial recognition.[68] Dodging any judicial review of the technology's reliability. Similarly manipulative facial recognition identifications may be the basis of many more prosecutions, but judges will never review them because facial recognition is just a "lead."

Limiting facial recognition to lead generation does not reduce its inaccuracy.[69] It merely exacerbates the existing problems of eyewitness identification and avoids judicial review.[70] The best way to eliminate these problems isn't by limiting use cases; it's by banning facial recognition altogether.

Conclusion.

We thank the OAG for attempting to mitigate the risks associated with facial recognition, but half measures will do little to meet the OAG's guiding principles. New Jersey must ban facial recognition—anything less is dangerous. General Grewal understood the risks when he prohibited Clearview AI in 2020.[71] Nothing has changed. Facial recognition is as hurtful as ever. Facial recognition is invasive, indiscriminate, and inaccurate.[72] Even a perfect facial recognition policy cannot mitigate this reality.[73] Worse, facial recognition entrenches discrimination under the guise of objectivity and circumvents judicial review.[74] This is unacceptable. We urge the OAG to adopt the most responsible policy. Ban facial recognition.

---

[64] Khari Johnson, "The Hidden Role of Facial Recognition Tech in Many Arrests," Wired, accessed March 7, 2022, https://www.wired.com/story/hidden-role-facial-recognition-tech-arrests/.
[65] *Id.*
[66] *Id.*
[67] *Id.*
[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] Hill, *supra* note 23.
[72] *Supra*, Facial recognition systems fail the OAG's guiding principles.
[73] *Supra*, Even a "perfect" facial recognition system is discriminatory.
[74] *Id. Supra*, Facial recognition systems fail the OAG's guiding principles.