*A Call for Transparency in Law Enforcement Use of Facial Recognition*

Benjamin Nober

**Introduction**

Calls to defund the police ring out across a country reeling from widespread protests against the use of unnecessary force on George Floyd and countless other Black individuals by police. As protestors this summer marched down streets around the country, local, state and federal authorities had the technology and power to locate and arrest protestors using facial recognition software.[[1]](#footnote-0)

Questions must be asked now about the continued use of facial recognition by law enforcement at every level. The inequality created by the failure of legislation to address the technology drives at the core of protests today. At the same time, reliable facial recognition technology under responsible and appropriate usage can certainly provide law enforcement with extraordinary help. The demanding task of balancing present and future concerns over the technology’s use with its promised benefits places legislators in a tough position. These problems are undergirded by a fundamental lack of transparency. Without knowledge of the extent to which this technology is used or even where it is in place, fair and accountable use will remain unachievable.

**Present Uses of Facial Recognition**

The advantages of facial recognition technology for law enforcement officials are clear. Technology can do what humans cannot. Credibility in court is easily established through eye-witness testimony giving positive identification, yet this testimony is often unreliable.[[2]](#footnote-1) Being able to positively identify criminals objectively through facial recognition technology provides law enforcement an opportunity to lend significantly more credibility in court, because facial recognition technology, in theory, is objective.

State and local law enforcement across the country are governed to varying degrees on their use of facial recognition technologies. Laws range from outright bans on their use in a few cities to minor restrictions or unfettered access in most.[[3]](#footnote-2) State police departments using facial recognition technologies have separate, local databases of photos compiled through mugshots, driver’s license photos and other sources.[[4]](#footnote-3)

Specific state uses of facial recognition have drawn scrutiny from both sides of the aisle. Following the killing of Freddie Gray at the hands of the police, the technology was used to locate and arrest specific protestors in Baltimore.[[5]](#footnote-4) Additionally, its use on police body cameras has pushed multiple states to pass laws banning the practice.[[6]](#footnote-5)

Facial recognition technology is used by many federal agencies. No law exists that directly forces disclosure of these practices. This creates a fairly standard lack of transparency across all agency use. Due to this lack of transparency, the full extent to which agencies use facial recognition remains fairly unknown to the public.

The Federal Bureau of Investigation (FBI) has disclosed its controversial use of facial recognition with a broad range of motives meant to “investigate, identify, apprehend, and prosecute” targets.[[7]](#footnote-6) As of 2016, the FBI was known to be using a database of State and Defense Department photos, as well as those of at least 16 state Departments of Motor Vehicles (DMVs), for facial recognition searches.[[8]](#footnote-7) By 2019, the number had increased to 21 states, with the total number of photos in the database numbering at around 640 million.[[9]](#footnote-8)

Another prominent departmental use of facial recognition exists within the U.S. Immigration and Customs Enforcement (ICE). ICE officials have admitted to using facial recognition to aid in ongoing investigations.[[10]](#footnote-9) One practice has been accessing state DMV driver’s license photo databases, including some states where undocumented individuals are permitted to obtain a driver’s license.[[11]](#footnote-10) In some cases, the agency independently accesses and purchases these state databases for searches without any notice or form of public approval.[[12]](#footnote-11)

**Technological Concerns**

Although touted as objective, facial recognition remains marred by technological shortcomings. While technology might improve over time, the imperfect algorithms in use today have real consequences which are detrimental to the most vulnerable Americans across the country.

A glaring fault entrenched in facial recognition technology today is inequality. Facial recognition systems rely on machine learning, an algorithmic computer science technique that makes predictions by figuring out connections between sets of data.[[13]](#footnote-12) Put plainly, facial recognition learns from the data humans feed it and uses that as training to make predictions.

State databases of mugshots and other commonly used databases of law enforcement facial recognition are built upon years of racial profiling and discriminatory policies towards minorities.[[14]](#footnote-13) The National Institution of Standards and Technology’s (NIST) most recent report on discrimination documents disparities in performance across most algorithms, resulting in worse results for people of color, women, and young people aged 18-30.[[15]](#footnote-14) A 2018 American Civil Liberties Union (ACLU) report saw 28 false positives matching members of Congress to criminal mugshot photos through Amazon’s facial recognition software.[[16]](#footnote-15) Included in this abysmal performance was a disproportionately high number of nonwhite representatives. The bias stemming from this inadequate foundation is evident.

Compounding the inequality inherently present in the data are questions of accuracy. State and federal officials use separate databases, and even the most recent studies demonstrate that there is a significant amount of variance among the accuracies of such facial recognition algorithms.[[17]](#footnote-16) Even in departments employing the best technology, problems arise from input conditions that are far from optimal. Many photos provided in the field are of extremely low quality. The idea of a grainy image from a surveillance camera being enhanced to provide a clear view of a face is nothing more than an overly-repeated plot on a “CSI” television episode. While the best facial recognition algorithms performing under optimal conditions may produce accurate matches a staggering 99.7 percent of the time, real-world conditions significantly lowering success rates are the reality.[[18]](#footnote-17) There is little data available to the public on the accuracy of actual searches by law enforcement, and there are no baseline accuracy standards.[[19]](#footnote-18)

**Ethical Concerns**

Constitutional questions arising from both sides of the aisle surrounding the First, Fourth, and Fourteenth Amendments come into play with facial recognition. With constant surveillance by police, safeguarding rights to freedom of speech becomes necessary. Under surveillance, individuals are less likely to speak freely.[[20]](#footnote-19) Precedent has shown that the Fourth Amendment does not provide as much protection from unwarranted searches as lawmakers would hope.[[21]](#footnote-20) Looking at the FBI’s database of 640 million pictures, many of the images that are regularly included in searches come from innocent citizens, including the more than 146 million with valid passports as of 2019.[[22]](#footnote-21) This technology does not perform equally along lines of race and gender, spurring Fourteenth Amendment questions. Datasets referred to as “pale male” for their overrepresentation of older white men commonly train algorithms to perform worse by a substantial margin for people of color, women, and young people.[[23]](#footnote-22) This leads to unequal treatment under the law.

A concern exists surrounding the amount of surveillance that should be employed by the government. A Pew Research Center study from 2019 found that nearly two-thirds of Americans were concerned with the amount of data collected on them by the government.[[24]](#footnote-23) Using facial recognition technology to survey large crowds protesting in public and incorporating the technology into police body cameras drew widespread criticism. However, without any legislation drawing boundaries over what the role of facial recognition should be, little surprise can stem from these applications.

Proper and responsible use is another key ethical consideration. Facial recognition is a powerful tool. Reports of law enforcement officials inputting altered images and even hand sketches demonstrate how the imprecise practical uses of the technology do not reflect the highly touted accuracy standards of algorithms under optimal conditions.[[25]](#footnote-24) Additionally, the trend of law enforcement officers abusing their unfettered access to powerful databases for personal use is well documented.[[26]](#footnote-25) These considerations question those presently given access to the technology and force reflection as to whether more standards are necessary.

**Conclusion**

The plethora of issues, both technological and ethical, that stem from law enforcement’s use of facial recognition technologies should outrage the public. These problems affect Americans across all walks of life and must be treated with urgency. Underdeveloped technology that discriminates and a lack of transparency on its accuracy highlight the technical concerns, while bipartisan constitutional worries, surveillance levels, and irresponsible use characterize ethical worries.

Recent responses to national protests from big tech companies such as Amazon and Microsoft to suspend the sale of these technologies to law enforcement are a good first step, yet they do little to provide sustainable solutions.[[27]](#footnote-26) Private regulation has provided the framework that exists today, and that must be viewed as a failure.

Guaranteeing transparency across the board must be the top priority for state and federal lawmakers. These systems impinging on the liberties of Americans must eventually be addressed through legislation. However, the lack of information on the technology’s use prevents even proper discussion on what regulation should look like. At a local level, leaders must experiment with new strategies to discover which tactics work to target specific ethical and technological shortcomings of unconstrained surveillance.[[28]](#footnote-27)

References

American Civil Liberties Union. “Amazon’s Face Recognition Falsely Matched 28 Members of Congress With Mugshots.” Accessed June 9, 2020. https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

Auxier, Brooke, and Lee Rainie. “Key Takeaways on Americans’ Views about Privacy, Surveillance and Data-Sharing.” *Pew Research Center* (blog), November 15, 2019. https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/.

Benjamin, Ruha. “Race After Technology.” Ruha Benjamin. Accessed July 17, 2020. https://www.ruhabenjamin.com/race-after-technology.

Crawford, Susan. “Facial Recognition Laws Are (Literally) All Over the Map.” *Wired*. Accessed June 9, 2020. https://www.wired.com/story/facial-recognition-laws-are-literally-all-over-the-map/.

Cummings, Elijah. Facial Recognition Technology (Part 1): Its Impact on our Civil Rights and Liberties, § House Oversight Committee (2019).

Cummings, Elijah. Facial Recognition Technology (Part II): Ensuring Transparency in Government Use, § House Oversight Committee (2019).

Garvie, Clare. “Garbage In. Garbage Out. Face Recognition on Flawed Data.” Garbage In. Garbage Out. Face Recognition on Flawed Data, May 16, 2019. https://www.flawedfacedata.com.

Grother, Patrick, Mei Ngan, and Kayee Hanaoka. “Face Recognition Vendor Test Part 3:: Demographic Effects.” Gaithersburg, MD: National Institute of Standards and Technology, December 2019. https://doi.org/10.6028/NIST.IR.8280.

Gurman, Sadie. “AP: Across US, Police Officers Abuse Confidential Databases.” AP NEWS, September 27, 2016. https://apnews.com/699236946e3140659fff8a2362e16f43.

“OPA: Chicago Driver’s License Case,” November 17, 2014.

“Reports and Statistics.” Accessed July 17, 2020. https://travel.state.gov/content/travel/en/about-us/reports-and-statistics.html.

Smeets, Dirk, Peter Claes, Dirk Vandermeulen, and John Gerald Clement. “Objective 3D Face Recognition: Evolution, Approaches and Challenges.” *Forensic Science International* 201, no. 1–3 (September 10, 2010): 125–32. https://doi.org/10.1016/j.forsciint.2010.03.023.

Solow-Niederman, Alicia. Alicia Solow-Niederman Interview, April 23, 2020.

Vincent, James. “NYPD Used Facial Recognition to Track down Black Lives Matter Activist.” The Verge, August 18, 2020. https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram.

US Day One Blog. “We Are Implementing a One-Year Moratorium on Police Use of Rekognition,” June 10, 2020. https://blog.aboutamazon.com/policy/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition.

1. This footnote has been updated after the writing of the original piece with a report verifying previous claims. James Vincent, “NYPD Used Facial Recognition to Track Down Black Lives Matter Activist,” The Verge, August 18, 2020, https://www.theverge.com/2020/8/18/21373316/nypd-facial-recognition-black-lives-matter-activist-derrick-ingram. [↑](#footnote-ref-0)
2. Dirk Smeets et al., “Objective 3D Face Recognition: Evolution, Approaches and Challenges,” *Forensic Science International* 201, no. 1–3 (September 10, 2010): 125–32, https://doi.org/10.1016/j.forsciint.2010.03.023. [↑](#footnote-ref-1)
3. Susan Crawford, “Facial Recognition Laws Are (Literally) All Over the Map,” *Wired*, accessed June 9, 2020, https://www.wired.com/story/facial-recognition-laws-are-literally-all-over-the-map/. [↑](#footnote-ref-2)
4. Elijah Cummings, “Facial Recognition Technology (Part II): Ensuring Transparency in Government Use,” § House Oversight Committee (2019). [↑](#footnote-ref-3)
5. Cummings. [↑](#footnote-ref-4)
6. Crawford, “Facial Recognition Laws Are (Literally) All Over the Map.” [↑](#footnote-ref-5)
7. Cummings, Facial Recognition Technology (Part II): Ensuring Transparency in Government Use. [↑](#footnote-ref-6)
8. Elijah Cummings, “Facial Recognition Technology (Part 1): Its Impact on Our Civil Rights and Liberties,” § House Oversight Committee (2019). [↑](#footnote-ref-7)
9. Cummings, Facial Recognition Technology (Part II). [↑](#footnote-ref-8)
10. “OPA: Chicago Driver’s License Case,” November 17, 2014. [↑](#footnote-ref-9)
11. Cummings, Facial Recognition Technology (Part II) [↑](#footnote-ref-10)
12. Ibid. [↑](#footnote-ref-11)
13. Alicia Solow-Niederman, Alicia Solow-Niederman Interview, April 23, 2020. [↑](#footnote-ref-12)
14. Ruha Benjamin, “Race After Technology,” Ruha Benjamin, accessed July 17, 2020, https://www.ruhabenjamin.com/race-after-technology. [↑](#footnote-ref-13)
15. Patrick Grother, Mei Ngan, and Kayee Hanaoka, “Face Recognition Vendor Test Part 3:: Demographic Effects” (Gaithersburg, MD: National Institute of Standards and Technology, December 2019), https://doi.org/10.6028/NIST.IR.8280. [↑](#footnote-ref-14)
16. “Amazon’s Face Recognition Falsely Matched 28 Members of Congress With Mugshots,” American Civil Liberties Union, accessed June 9, 2020, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28. [↑](#footnote-ref-15)
17. Grother, Ngan, and Hanaoka, “Face Recognition Vendor Test Part 3.” [↑](#footnote-ref-16)
18. Grother, Ngan, and Hanaoka. [↑](#footnote-ref-17)
19. Cummings, Facial Recognition Technology (Part II): Ensuring Transparency in Government Use. [↑](#footnote-ref-18)
20. Ibid. [↑](#footnote-ref-19)
21. Ibid. [↑](#footnote-ref-20)
22. “Reports and Statistics,” accessed July 17, 2020, https://travel.state.gov/content/travel/en/about-us/reports-and-statistics.html. [↑](#footnote-ref-21)
23. Patrick Grother, Mei Ngan, and Kayee Hanaoka, “Face Recognition Vendor Test Part 3: Demographic Effects” (Gaithersburg, MD: National Institute of Standards and Technology, December 2019). [↑](#footnote-ref-22)
24. Brooke Auxier and Lee Rainie, “Key Takeaways on Americans’ Views about Privacy, Surveillance and Data-Sharing,” *Pew Research Center* (blog), November 15, 2019, https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/. [↑](#footnote-ref-23)
25. Clare Garvie, “Garbage In. Garbage Out. Face Recognition on Flawed Data,” Garbage In. Garbage Out. Face Recognition on Flawed Data, May 16, 2019, https://www.flawedfacedata.com. [↑](#footnote-ref-24)
26. Sadie Gurman, “AP: Across US, Police Officers Abuse Confidential Databases,” AP NEWS, September 27, 2016, https://apnews.com/699236946e3140659fff8a2362e16f43. [↑](#footnote-ref-25)
27. “We Are Implementing a One-Year Moratorium on Police Use of Rekognition,” US Day One Blog, June 10, 2020, https://blog.aboutamazon.com/policy/we-are-implementing-a-one-year-moratorium-on-police-use-of-rekognition. [↑](#footnote-ref-26)
28. This paper was adapted from its original version submitted in class to *Introduction to Law and Digital Technologies* taught Spring 2020 at Northwestern University by Prof. Daniel Linna and Prof. John Villasenor. [↑](#footnote-ref-27)