

# UC Berkeley

## Recent Works

### Title

Establishing Privacy Advisory Commissions for the Regulation of Facial Recognition Systems at the Municipal Level

### Permalink

<https://escholarship.org/uc/item/7qp0w9rn>

### Authors

Jackson, Christopher  
Livingston, Morgan  
Velan, Vetri  
et al.

### Publication Date

2020-06-02

# Establishing Privacy Advisory Commissions for the Regulation of Facial Recognition Systems at the Municipal Level

Christopher Jackson, Vetri Velan, Morgan Livingston, Eric Lee, Kimberly Huynh, Regina Eckert  
Science Policy Group at Berkeley

**Keywords:** facial recognition, law enforcement, surveillance technology, privacy

## Executive Summary

As facial recognition systems (FRS) become widely available, a growing number of local governing bodies across the country have adopted these technologies. Without regulating how and when these technologies are used, the adoption of FRS by municipal governments has the potential to violate civil liberties and disproportionately harm marginalized groups. FRS may be an invaluable tool for law enforcement; however, best practices must be adopted to curb their misuse, specifically at the municipal level. We propose that cities considering procurement of FRS create an independent privacy advisory commission with a clear mandate, guaranteed cooperation from local government, technology expertise, and community stakeholder input. We focus on Raleigh, North Carolina as a case study of a city where such a commission would be useful.

## I. The Problems with Facial Recognition

Facial recognition systems (FRS) are increasingly used by municipal law enforcement to enhance safety and cut costs; however, the technology is prone to error and can lead to widespread surveillance, threatening residents' rights to privacy. FRS analyze an image of a person's face to create a unique mathematical 'facial signature' composed of measurements such as the distance between the eyes. This signature is compared to a database of identified faces and the FRS returns the top likely matches. Over 50 law enforcement agencies currently use FRS to match faces in real time, recorded video, or photos to databases including mug shots and DMV records.<sup>1</sup> While law enforcement has achieved great successes with FRS, such as identifying the suspect in the 2018 *Capital Gazette* shooting in Maryland, safeguards are necessary to protect vulnerable communities.<sup>2</sup>

Errors in FRS disproportionately affect individuals who are African American, other racial minorities, female, youth, and/or elderly. Some FRS falsely match African Americans up to 100

---

<sup>1</sup> Garvie, C., Bedoya, A., Frankle, J. "Perpetual Line Up." Georgetown Law Center on Privacy & Technology. 18 Oct. 2016, <https://www.perpetuallineup.org/>. Accessed 12 Apr. 2020.

<sup>2</sup> Brandom, R. "How facial recognition helped police identify the Capital Gazette shooter." The Verge. 29 Jun. 2018, <https://www.theverge.com/2018/6/29/17518364/facial-recognition-police-identify-capital-gazette-shooter>. Accessed 12 Apr. 2020.

times more often than white individuals.<sup>3</sup> These errors are due to lack of diversity in both the photo sets used to train the matching software and the technologists designing the software. Faces in training sets can be more than 83% white and 74% male, skewing software accuracy towards these demographics and limiting applicability for people of color and women.<sup>4</sup> Further, technologists developing the software are overwhelmingly white and male and may encode the software with their implicit biases, making decisions on the design and data that underrepresent the needs of other demographic groups.<sup>5</sup>

Despite well-documented concerns about the accuracy of FRS, law enforcement agencies deploy the technology with little to no testing, with errors often compounded by misuse.<sup>1</sup> Populations vulnerable to policing, such as African Americans, are disproportionately represented in mugshot databases, meaning that errors in FRS can lead to higher rates of African Americans being falsely labeled as criminals.<sup>6</sup> Other vulnerable populations, such as children, also generate high error rates for FRS; this is especially concerning as police departments like the NYPD already use facial recognition databases that include thousands of juveniles as young as 11.<sup>7,8</sup> Since half of all American adults are in a law enforcement facial recognition database, inaccurate matching by FRS could impact over 100 million people.<sup>1</sup>

Even if FRS were fully accurate, they increase widespread public surveillance by law enforcement. FRS used to profile political, religious or ethnic groups threaten freedoms of expression at the core of democracy. Chinese authorities use FRS to track and profile Uighurs, an ethnic minority group.<sup>9</sup> In 2015, police in Baltimore used facial recognition to identify protesters with outstanding unrelated warrants and make arrests.<sup>10</sup> Despite these abuses, in 2016, only one U.S. law enforcement agency had a policy preventing the use of FRS to surveil people

---

<sup>3</sup> Grother, P., Ngan, M., Hanaoka, K. "Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects." National Institute of Standards and Technology. Dec. 2019, <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>. Accessed 12 Apr. 2020.

<sup>4</sup> Shellenbarger, S. "A Crucial Step for Averting AI Disasters." The Wall Street Journal. 13 Feb. 2019, <https://www.wsj.com/articles/a-crucial-step-for-avoiding-ai-disasters-11550069865>. Accessed 12 Apr. 2020.

<sup>5</sup> Burke, A. "Science and Engineering Labor Force." National Science Board. 26 Sep. 2019, <https://nces.nsf.gov/pubs/nsb20198/assets/nsb20198.pdf>. Accessed 12 Apr. 2020.

<sup>6</sup> Snow, J. "Amazon's Face Recognition Falsely Matched 28 Members of Congress With Mugshots." American Civil Liberties Union. 26 Jul. 2018, <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28>. Accessed 12 Apr. 2020.

<sup>7</sup> Goldstein, J., Watkins, A. "She Was Arrested at 14. Then Her Photo Went to a Facial Recognition Database." The New York Times. 1 Aug. 2019, <https://www.nytimes.com/2019/08/01/nyregion/nypd-facial-recognition-children-teenagers.html>. Accessed 12 Apr. 2020.

<sup>8</sup> Grother, P., Ngan, M., Hanaoka, K. "Face Recognition Vendor Test (FRVT), Part 2: Identification." National Institute of Standards and Technology. Dec. 2019, <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>. Accessed 12 Apr. 2020.

<sup>9</sup> Wee, S., Mozur, P. "China Uses DNA to Map Faces, With Help From the West." The New York Times. 3 Dec. 2019, <https://www.nytimes.com/2019/12/03/business/china-dna-uighurs-xinjiang.html>. Accessed 12 Apr. 2020.

<sup>10</sup> Wenger, Y. "Police used facial recognition technology to help identify uncooperative suspect in Capital Gazette shooting." The Baltimore Sun. 29 Jun. 2018, <https://www.baltimoresun.com/news/crime/bs-md-facial-recognition-suspect-identity-20180629-story.html>. Accessed 12 Apr. 2020.

engaging in protected free speech.<sup>1</sup> Only 17% of U.S. adults greatly trust law enforcement to use FRS responsibly, with significant variability by race and age; African-Americans and young Americans are less likely to share this trust than their white and older counterparts.<sup>11</sup> This potential for abuse and lack of trust suggests a need for greater community input and oversight of how law enforcement uses FRS.

## II. Past Attempts to Regulate Facial Recognition Systems

The NYU Policing Project has identified three broad categories of FRS regulation in the U.S. These include (1) general regulations that ban, pause, or study FRS, (2) operations-based regulations that control how FRS are deployed, and (3) data-based regulations that restrict the images used to operate FRS.<sup>12</sup>

Local attempts to regulate FRS, particularly in government use, have struggled to keep up with rapid FRS deployment. Three states (California, New Hampshire, and Oregon) and five cities (Berkeley, Oakland, San Francisco, Brookline, and Somerville) have enacted some form of ban on government use of FRS.<sup>13</sup> However, these bans are facing legal challenges and do not prevent private institutions within a city from using their own FRS. Therefore, more thorough and evolving mechanisms must be established to regulate FRS across the country.

A well-documented attempt at local FRS regulation was the Automated Decision Systems Task Force in New York City. Established in 2017, the task force was supposed to examine how automated systems, including facial recognition software, were used throughout the municipal government to guide decision-making processes.<sup>14</sup> However, they encountered multiple administrative hurdles. First, agencies were required to self-identify automated systems for the task force to evaluate, but many employees were either unable to identify these or were unaware of which systems were automated. Furthermore, the task force did not have the legal authority to compel agencies to provide information.<sup>15</sup>

---

<sup>11</sup> Smith, A. "More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly." Pew Research Center. 5 Sep. 2019, <https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/>. Accessed 12 Apr. 2020.

<sup>12</sup> Hrick, P., Heydari, F. "The Growing World of Face Recognition Legislation." Policing Project. <https://www.policingproject.org/frlaws>. Accessed 12 Apr. 2020.

<sup>13</sup> Read, M. "Why We Should Ban Facial Recognition Technology." New York Magazine. 30 Jan. 2020, <https://nymag.com/intelligencer/2020/01/why-we-should-ban-facial-recognition-technology.html>. Accessed 12 Apr. 2020.

<sup>14</sup> Lecher, C. "NYC's algorithm task force was 'a waste,' member says." The Verge. 20 Nov. 2019, <https://www.theverge.com/2019/11/20/20974379/nyc-algorithm-task-force-report-de-blasio>. Accessed 12 Apr. 2020.

<sup>15</sup> Richardson, R. "Confronting Black Boxes: A Shadow Report of the New York City Automated Decision System Task Force." AI Now Institute. 4 Dec. 2019, <https://ainowinstitute.org/ads-shadowreport-2019.pdf>. Accessed 12 Apr. 2020.

Similarly, the United Kingdom has struggled to regulate FRS because it lacks a centralized law guiding the use of live facial recognition despite its ongoing use by the Metropolitan Police Service.<sup>16</sup> Instead, different components of FRS, such as surveillance cameras, data, and legislative oversight, are delegated to at least four different independently appointed commissioners.<sup>17</sup> This ambiguity has caused confusion over who has the jurisdiction to regulate FRS and their use by law enforcement. These problems could be addressed through the creation of a centralized authority with clearly delineated authorities and jurisdiction.

On the other hand, Illinois' 2008 Biometric Information Privacy Act (BIPA) has been hailed by privacy advocates for its strength in addressing biometric privacy violations.<sup>18, 19, 20</sup> BIPA regulates the use and storage of biometric data, including eye scans, fingerprints, voiceprints, and facial/hand scans. Its most important provisions include: requiring collectors of biometric data to establish guidelines for securely storing and permanently destroying data within three years after collection; informing subjects of the collection of their biometric data; a ban on the sale of a person's biometric information; and a ban on disclosures of a person's biometric information without their consent, except in extraordinary circumstances such as a court warrant. In 2019, two court cases, *Rosenbach v. Six Flags* and *Patel v. Facebook*, upheld the use of BIPA to maintain accountability and provide financial compensation for privacy violations.<sup>21, 22</sup> However, BIPA exempts state and local governments from its requirements, allowing for the use of FRS in policing, prisons, and other public services and leaving a regulatory gap for the oversight of these important operations.

The city of Raleigh, NC presents a useful demonstration of issues that can arise without a concrete procedure for FRS implementation. In 2019, the Raleigh Police Department (RPD) contracted with Clearview AI, a FRS with extraordinary precision and a widespread facial database built from social media.<sup>23</sup> After extensive media reporting on the capabilities of

---

<sup>16</sup> Thomas, E. "Facial recognition is in London. So how should we regulate it?." *Wired*. 16 Mar. 2020, <https://www.wired.co.uk/article/regulate-facial-recognition-laws>. Accessed 12 Apr. 2020.

<sup>17</sup> Chertoff, P. "Facial Recognition Has Its Eye on the U.K." *Lawfare*. 7 Feb. 2020, <https://www.lawfareblog.com/facial-recognition-has-its-eye-uk>. Accessed 12 Apr. 2020.

<sup>18</sup> "Biometric Information Privacy Act." <http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57>. Accessed 12 Apr. 2020.

<sup>19</sup> Wessler, N. "A Federal Court Sounds the Alarm on the Privacy Harms of Facial Recognition Technology." *American Civil Liberties Union*. 9 Aug. 2019, <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/federal-court-sounds-alarm-privacy-harms-face>. Accessed 12 Apr. 2020.

<sup>20</sup> Schwartz, A. "New Attack on the Illinois Biometric Privacy Act." *Electronic Frontier Foundation*. 10 Apr. 2018, <https://www.eff.org/deeplinks/2018/04/new-attack-illinois-biometric-privacy-act>. Accessed 12 Apr. 2020.

<sup>21</sup> "Rosenbach v. Six Flags Entertainment Corp." *Illinois Courts*. 25 Jan. 2019, <https://courts.illinois.gov/Opinions/SupremeCourt/2019/123186.pdf>. Accessed 12 Apr. 2020.

<sup>22</sup> "Patel v. Facebook." *Electronic Privacy Information Center*. <https://epic.org/amicus/bipa/patel-v-facebook/>. Accessed 12 Apr. 2020.

<sup>23</sup> Shaffer, J. "Raleigh police stop using controversial facial recognition technology." *The News & Observer*. 12 Feb. 2020, <https://www.newsobserver.com/news/local/crime/article240221072.html>. Accessed 30 May. 2020.

Clearview AI, the RPD broke its contract with the company in February 2020.<sup>24</sup> Fortunately, there had not been any demonstrated abuse of privacy by the RPD—searches were never used as the sole evidence for charging a suspect—but the potential for this abuse certainly existed.

### III. Policy Recommendations

We recommend that local municipalities establish a privacy advisory commission modeled after the Privacy Advisory Commission in Oakland, CA.<sup>25</sup> In particular, Raleigh, a similar sized-city to Oakland, should implement this proposal. To ensure its effectiveness and avoid challenges similar to those faced in the UK and New York City, this commission should meet the following criteria.

First, the commission must have a clear mandate and responsibilities. Commission responsibilities should include advising and providing technical assistance for the city government on best practices for the use of FRS. The commission should review and advise the city council on FRS technology prior to adoption, conduct public hearings, create model legislation, and analyze legislation related to resident privacy. This commission should also have veto, or at minimum voting, authority over the procurement and use of FRS on a case-by-case basis and on any future legislation pertaining to FRS. As necessary, the commission can also advise on the use of other surveillance technologies that may infringe upon privacy concerns.

Second, the commission must be guaranteed cooperation and financial support from the local governing body, including some degree of authority over relevant stakeholders, including law enforcement. We recommend that this commission work closely with counterparts such as the NC Civil Rights Division and Raleigh Police Oversight Board. The city will need to commit staffing to support the commission's investigations, provide documentation of technologies, allocate City Council time, and ensure transparent communication. Costs to enact the commission's recommendations may include increasing cybersecurity and technical infrastructure, strengthening procurement procedures, and facilitating cooperation with vendors. Incorporating commission recommendations can ensure city investment is directed effectively, prevent lawsuits on mishandling of data, foster community trust, and protect the residents' civil liberties.

Third, the commission should include technology expertise alongside representation from legal, law enforcement, and auditing experts. Technology expertise is crucial to understanding the ethical implications of rapidly changing FRS. We recommend that the Raleigh city council turn

---

<sup>24</sup> Hill, K. "The Secretive Company That Might End Privacy as We Know It." <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html> Accessed 30 May 2020.

<sup>25</sup> "Privacy Advisory Commission." City of Oakland. <http://www2.oaklandnet.com/government/o/CityAdministration/d/PrivacyAdvisoryCommission/index.htm>. Accessed 12 Apr. 2020.

to local research institutions such as the University of North Carolina, or networks such as the American Civil Liberties Union, the Electronic Frontier Foundation, and the National Science Policy Network to ensure this commission is properly equipped to regulate potential challenging technical issues.

Finally, the commission should be composed of volunteer members dedicated to community representation. Similar to other Raleigh commissions, and the Oakland Privacy Advisory Commission, appointments can be made by elected by a combination of city council members and the mayor. To ensure a variety of community stakeholder inputs, the city should also consider designating positions for representatives from traditionally underrepresented interest groups. This commission should host regular (e.g. monthly) meetings that are open to the community and include opportunities for public comment.

#### **IV. Community Return on Investment**

We understand that the creation and support of such a commission will require local resources from the City of Raleigh. Based on the City of Oakland's Privacy Advisory Commission, we estimate this at 10-15 staff hours per month to support a monthly meeting, with potential additional to implement any commission proposals.<sup>26</sup> We anticipate that such responsibilities can be absorbed by existing government infrastructure. Furthermore, as the city of Raleigh considers the adoption of FRS, it could see overall costs decrease by using commission resources to perform work that would have previously been outsourced or done less efficiently by other government entities, such as vetting or reporting on the use of FRS technology.

The creation of a privacy advisory commission can also preserve democratic and local control over law enforcement. As the federal government has increased grants for surveillance equipment in local municipalities, law enforcement has become less financially dependent and subject to oversight by local government.<sup>27</sup> A privacy advisory commission in Raleigh, if properly structured, can create ordinances and provide oversight to ensure the ethical use of FRS by law enforcement, regardless of funding sources.

#### **V. Conclusion**

As FRS continue to proliferate and cities like Raleigh are forced to contend with its use, we recommend that cities create an independent advisory commission to safeguard against the

---

<sup>26</sup> "Creation of a Privacy Advisory Commission." City of Oakland. 26 Oct. 2015, <https://oakland.legistar.com/LegislationDetail.aspx?ID=2503814&GUID=DD0D90E4-1084-44D0-8E74-D7FA2530724D&Options=&Search=>. Accessed 12 Apr. 2020.

<sup>27</sup> Katayama, D. "Oakland's Privacy Commission Could Lead Nation on Surveillance Oversight." KQED. 22 Jan. 2016, <https://www.kqed.org/news/10824952/oaklands-privacy-commission-could-be-one-of-most-active-in-country>. Accessed 12 Apr. 2020.

violation of civil liberties and disproportionate harm to marginalized groups. Such a commission must include a clear mandate, guaranteed cooperation from local government, technology expertise, and community stakeholder input. The commission's role is not to impede technological development, but to ensure implementation is safe, efficient and in line with the needs of the local community. If properly implemented with these guidelines, our proposal can decrease costs and ensure local control over the ethical governmental use of FRS.