

SUPREME COURT OF THE STATE OF NEW YORK  
COUNTY OF NEW YORK

NEW YORK CIVIL LIBERTIES UNION,

Petitioner,

-against-

NEW YORK STATE DEPARTMENT OF CORRECTIONS  
AND COMMUNITY SUPERVISION, and ANTHONY J.  
ANNUCCI, in his official capacity as Acting Commissioner of  
the New York State Department of Corrections and  
Community Supervision,

Respondents.

For a Judgment Pursuant to Article 78  
of the Civil Practice Law and Rules.

Index No.  
(NYSCEF Filed)

**VERIFIED PETITION**

**PRELIMINARY STATEMENT**

1. This Article 78 Proceeding seeks to vindicate the public’s right to know basic facts about the New York State Department of Corrections and Community Supervision’s (“DOCCS”) policies, practices, and use of face recognition technology at its facilities on family, friends, and loved ones, including children, who visit people under DOCCS’s custody.

2. Face recognition systems are built on computer programs that analyze images of human faces for the purpose of identifying them. Face recognition technology is notoriously inaccurate and prone to error. Facial recognition software is particularly bad at recognizing Black people and other people of color, women, and young people, often misidentifying or failing to identify them.

3. DOCCS has acknowledged that DOCCS uses face recognition technology for “visitation processing” – apparently to match family, friends, and loved ones seeking to visit

individuals under DOCCS’s custody against a database containing images of individuals that DOCCS, presumably, wishes to ban from visiting people incarcerated in DOCCS’s facilities. *See* the true and correct copy of DOCCS’s denial of the NYCLU’s administrative appeal dated March 1, 2021 at Exhibit 7.

4. To the extent that DOCCS is using a face recognition system to screen families, friends, and loved ones visiting people under DOCCS’s custody, DOCCS’s system inevitably will misidentify visitors as unwelcome and deny visitation. The consequences may be more dire if the DOCCS’s system misidentifies someone as a person who has justice system involvement, including, for example, an outstanding warrant, and DOCCS detains that person unjustifiably and/or calls upon law enforcement intervention. It is also unclear whether those visitors who are misidentified will suffer consequences that will lead to justice system involvement.<sup>1</sup>

5. New York’s Freedom of Information Law (“FOIL”) expresses this State’s strong commitment to open government and public accountability and imposes a broad standard of disclosure upon the State, the City, and their agencies. Public Officers Law § 84. FOIL proceeds under the premise that the public is vested with an inherent right to know and notes that “[a]s state and local government services increase and public problems become more sophisticated and complex and therefore harder to solve [...] it is incumbent upon the state and its localities to extend public accountability [...]” *Id.* Therefore, pursuant to FOIL, all government records are presumptively open for public inspection and copying. Although this presumption is subject to

---

<sup>1</sup> A little known collateral consequence of justice system involvement often is that a person’s photograph has been entered into a law enforcement or carceral system’s reference database of unwanted visitors. Face recognition data often is derived from mugshot images, which are taken upon arrest, before a judge ever has a chance to determine guilt or innocence. Mugshot photos are often never removed from the database, even if the arrestee has never had charges brought against them. *See e.g.* Clare Garvie, *The Perpetual Line-Up: Unregulated Police Face Recognition In America*, Georgetown Center for Privacy and Technology [Oct. 2016], available at <https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf> [accessed June 28, 2021]. A true and correct copy of this report is at Exhibit 10.

certain statutory exceptions, “the agency involved shall have the burden of proving that such record falls within” those exceptions. Public Officers Law § 89 [4] [b]. *See also* New York Corrections and Community Supervision, Directive No. 2010 § VI-A-3-b, *FOIL/Access to Departmental Records* (DOCCS FOIL Appeals Officer must fully explain in writing the factual and statutory reasons for denial) [Aug. 23, 2016], available at <https://doccs.ny.gov/system/files/documents/2020/11/2010.pdf> [last accessed June 28, 2021]. A true and correct copy of Directive 2010 is at Exhibit 22.

6. DOCCS has failed to comply with FOIL and has failed to follow its own directives. DOCCS failed to produce any records in response, withholding vital information from the public about DOCCS’ use of this technology.

7. The records sought in this Article 78 proceeding are vital to the public’s right to know about the nature and scope of DOCCS’s use of a flawed technology – particularly against people of color, including children.

8. Having exhausted its administrative remedies, the NYCLU now seeks judicial relief to compel DOCCS to comply with its obligation to produce records as required by law.

### **VENUE AND JURISDICTION**

9. Pursuant to C.P.L.R. §§ 7804 [b] and 506 [b], venue in this proceeding lies in New York County, the judicial district in which Petitioner’s principal office is located.

10. This Court has jurisdiction over the matter because DOCCS’s denial of the NYCLU’s appeal cannot be further “reviewed by appeal to a court or to some other body or officer.” C.P.L.R. § 7801 [1].

### **PARTIES**

11. Petitioner the New York Civil Liberties Union (the “NYCLU”) is a not-for-profit, nonpartisan organization with eight regional offices, and more than 126,000 members across the state. The NYCLU’s mission is to defend and promote the fundamental principles and values embodied in the Bill of Rights, the U.S. Constitution, and the New York Constitution, including freedom of speech and religion, and the right to privacy, equality and due process of law, with particular attention to the pervasive and persistent harms of racism. The NYCLU maintains its office at 125 Broad Street, 19<sup>th</sup> floor, New York, New York 10004.

12. Respondent DOCCS is a public agency subject to the requirements of the Freedom of Information Law, New York Public Officers Law § 84 et seq. DOCCS maintains its office at Harriman State Campus, 1220 Washington Avenue, Albany, New York 12226-2050.

13. Respondent Anthony J. Annucci is a public officer who is named in his official capacity as Acting Commissioner of DOCCS. Respondent Annucci maintains an office at DOCCS, Harriman State Campus, 1220 Washington Avenue, Albany, New York 12226-2050.

## **FACTUAL BACKGROUND**

### **Accuracy of Face Recognition Technology**

14. Face recognition systems use computer algorithms to pick out specific, distinctive details about a person’s face. These details, such as distance between the eyes or shape of the chin, are then converted into a mathematical representation and compared to data on other faces collected in a face recognition database. The data about a particular face is often called a face template or digital signature. The face template or digital signature is distinct from a photograph because it is designed to include only certain details that can be used to distinguish one face from another. Some face recognition systems, instead of positively identifying an unknown person, are designed to calculate a probability match score between the unknown person and specific face templates stored in the database. These systems will offer up several potential matches, ranked in

order of likelihood of correct identification, instead of just returning a single result. Face recognition systems can be used to identify people against still photographs, video streams, or in real-time.

15. Face recognition technology can perform several functions, including facial recognition (comparing an unknown face against a database of known persons, or “one-to-many”) and facial verification (confirming someone’s identity, or “one-to-one”). See Congressional Research Service, *Federal Law Enforcement Use of Face Recognition technology* [R46586, 2020] <https://fas.org/sgp/crs/misc/R46586.pdf>. A true and correct copy of this report is at Exhibit 11.

16. A study of face recognition algorithms conducted by the US National Institute of Standards and Technology (NIST)<sup>2</sup> showed these algorithms to be biased against people of color. See Patrick Grother et al., *Facial Recognition Vendor Test (FRVT), Part 3: Demographic Effects* [NISTIR 8280, 2019], available at <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf> [accessed June 28, 2021]. A true and correct copy of this NIST report is at Exhibit 13. The study showed face recognition technology algorithms produced a higher rate of false positives (i.e., an inaccurate match from images of two different people; a “false alarm”) for people of color. *Id.* at

---

<sup>2</sup> Founded in 1901, the National Institute of Standards and Technology, or NIST, is a non-regulatory federal agency within the U.S. Department of Commerce. NIST's mission is to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life. See National Institute of Standards and Technology, *NIST General Information*, available at <https://www.nist.gov/director/pao/nist-general-information> [accessed June 30, 2021]. A true and correct copy of the NIST General Information document is at Exhibit 12.

NIST has studied face recognition technology and has issued a series of face recognition vendor tests (FRVT), evaluating and assessing different algorithms over the past twenty years. In a recent series of reports, NIST has evaluated the performance of one-to-one face recognition algorithms used for verification of asserted identities, and performance of one-to-many face recognition algorithms used for identification of individuals in photo databases.

2. Importantly, the NIST noted there was significant variance between the algorithms, with some producing fewer errors or different types of errors. *Id.*<sup>3</sup>

17. NIST’s December 2019 report details the “empirical evidence” demonstrating that most of the face recognition algorithms in use currently exhibit “demographic differentials” that can diminish their accuracy based on a person’s age, gender or race. The report examines 189 facial recognition algorithms by 99 vendors and shows significant biases, with a high likelihood of misidentifying Asian American and Black people, as well as women, children, and older people.<sup>4</sup>

18. NIST’s December 2019 report confirms what many respected research academics have reported for the past several years relating to these demographic biases and finding that the darker the face, the less accurate the face recognition technology results are. *See, e.g.* Cynthia M. Cook et al., *Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems*, 1 IEEE Transactions On Biometrics, Behavior, And Identity Science 32–41 [ Jan. 2019], available at <https://ieeexplore.ieee.org/document/8636231> [accessed June 28, 2021]; Joy Buolamwini &

---

<sup>3</sup> NIST has also identified a significant “hardware” limitation with respect to the performance of face recognition algorithms. NIST indicates that while a reference database is generally comprised of “higher quality” or “clean” photos taken at a good angle, those reference database images are compared with surveillance footage that provides images at bad angles (usually overhead or at distanced] in an uncontrolled lighting situation. More often than not, these circumstances will also cause “false positive” identifications, *i.e.* the erroneous association of samples of two persons which occur when the algorithm determines that the digitized faces of two people are similar. These environmental circumstances occur no matter how high resolution the surveillance cameras are.

<sup>4</sup> Asian and Black people were up to 100 times more likely to be misidentified than white men, depending on the particular algorithm and type of search. Native Americans had the highest false-positive rate of all ethnicities, according to the study, which found that systems varied widely in their accuracy. The faces of Black women were falsely identified more often in the kinds of searches used by police investigators where an image is compared to thousands or millions of others in hopes of identifying a suspect. Women were more likely to be falsely identified than men, and the elderly and children were more likely to be misidentified than those in other age groups, the study found. Middle-aged white men generally benefited from the highest accuracy rates. *See also* William Crumpler, Center for Strategic & International Studies, *How Accurate are Facial Recognition Systems – and Why Does It Matter?*, <https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter> [April 14, 2020]. A true and correct copy of this report is at Exhibit 14.

Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 Proceedings Of Machine Learning Research 1 [2018], available at <http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf> [accessed June 28, 2021].

True and correct copies of these studies are at Exhibits 15 and 16, respectively.<sup>5</sup>

19. Problems with face recognition technology are not just theoretical. In New Jersey, face recognition technology false positives led to wrongful arrests on three separate occasions – all of black men. See Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, NY Times [Dec. 29, 2020], available at

<https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html>

[accessed June 28, 2021]. A true and correct copy of this news report is at Exhibit 18. New Jersey has since put a moratorium on the use of face recognition technology by law enforcement. *Id.*<sup>6</sup>

20. These instances of face recognition technology false positives are not unique. See e.g. U.S. Government Publishing Office, *Face Recognition Technology: Part I Its Impact on Our Civil Rights and Liberties*, H. Comm. on Oversight and Reform, 116th Cong. 9-11 [May 22,

---

<sup>5</sup> We are at a pivotal moment in society’s assessment of any utilization of biometric identifying technology given the dangerous biases evident in face recognition technology. The widespread affordability and availability of biometric recognition technologies has led to deployments across New York State: by law enforcement agencies, in schools, places of entertainment, housing, airports, toll gantries, and public transport infrastructure.

But academic researchers have been joined by large technology in their assessment of the biases, and harmful consequences, evident in this technology. IBM, joined by Amazon and Microsoft, have all just announced that they will no longer offer, develop, or research facial recognition technology because the technology has been shown to suffer from bias along lines of age, race, and ethnicity, which can make the tools unreliable for law enforcement and security and ripe for potential civil rights abuses. See Jay Green, *Microsoft won’t sell police its facial-recognition technology, following similar moves by Amazon and IBM*, Washington Post [June 11, 2020] available at <https://www.washingtonpost.com/technology/2020/06/11/microsoft-facial-recognition/> [accessed June 28, 2021]. A true and correct copy of this article is at Exhibit 17.

<sup>6</sup> Moratoria are an increasingly being imposed against use of this technology. New York State, for example, has imposed a moratorium on the use of face recognition technology in K-12 school settings, pending further investigation by the New York State Office of Information Technology and the New York State Education Department. See N.Y. State Technology Law Technology Law § 106-b.

2019] (Statement of Neema Singh Guliani, Senior Legislative Counsel, American Civil Liberties Union), available at <https://www.govinfo.gov/content/pkg/CHRG-116hhrg36663/html/CHRG-116hhrg36663.htm> [accessed June 28, 2021]. A true and correct copy of the Oversight Hearings Record is at Exhibit 19.

21. Utilization of face recognition systems in low-rights environments such as prisons carries staggering potential costs including, at the very least, denial and deterrence of families and friends from visiting their incarcerated loved ones. This technology exacerbates systemic racism as it could disproportionately impact people of color, who are already subject to discrimination and violations of their human rights by law enforcement officials.

22. It is more likely than not that the family, friends, and loved ones who visit people under DOCCS's custody will be disproportionately people of color and that those family members, friends and loved ones will inevitably be misidentified by DOCCS's face recognition screen system. It is well documented that there are gross racial and ethnic disparities in the nation's prison population where incarceration rates for Black people are six times higher than for white people; Latinx people are incarcerated more than twice as often as those who are white, yet these racial disparities in the prison population do not necessarily reflect higher rates of offending among those groups in the general population. The racial and ethnic disparities in New York State's prison population are particularly stark: approximately 75 percent of those incarcerated are Black or Latinx. People of color are disproportionately overrepresented in New York State's prisons. *See* New York State Department of Corrections and Community Supervision, *Under Custody Report: Profile of Under Custody Population, As of January 1, 2019*, available at <https://DOCCS.ny.gov/system/files/documents/2021/05/under-custody-report-2019.pdf> [accessed June 28, 2021]. A true and correct copy of DOCCS's report is at Exhibit 9.

## **DOCCS'S Visitation Policies**

23. The NYCLU works toward its mission by advocating for all New Yorkers to have equal access to opportunities and the equal ability to participate in government decisions that affect them. This includes planning and development decisions, which historically have excluded or intentionally discriminated against Black, Indigenous, and Latinx New Yorkers. Among other activities, the NYCLU engages in disseminating information to inform the public about actual or alleged government activity. Obtaining information about government activity, analyzing that information, and widely publishing and disseminating that information to the press and public are critical and substantial components of the NYCLU's work.

24. The NYCLU frequently receives queries on issues involving government law, policy, or practice affecting the constitutional rights of a significant number of people arising in New York State.

25. The NYCLU has received queries relating to denial of visitation rights to the relatives of people held in DOCCS's custody based on utilization of face recognition technology to screen visitors.<sup>7</sup>

26. DOCCS notes on its website that it "maintains comprehensive directives detailing the proper management and operation of its many functions. These documents also provide general information/guidance to assist regulated parties in complying with statutes, rules, and other legal requirements." *See* New York State Department of Corrections and Community

---

<sup>7</sup> As but one example, it was reported to the NYCLU that DOCCS denied a man permission to visit his relative in a DOCCS's facility solitary housing unit because the face recognition technology mistakenly matched him with a person who is banned from visiting that correctional facility. In a clear demonstration of automation bias, the DOCCS visitor processing officer refused to accept a valid state-issued identification despite the fact that the officer acknowledged that the prospective visitor's appearance did not at all match the appearance of the person that showed up as a match through DOCCS's face recognition technology.

Supervision, *Laws, Rules & Directives Listing*, available at <https://DOCCS.ny.gov/laws-rules-directives-listing> [accessed June 28, 2021].

27. DOCCS “encourages visits by family and friends, which can be a positive influence during the time a person spends in prison and after their release. Research shows that incarcerated individuals who receive regular visits adjust much better once they are released from prison when the privilege is used to maintain positive relationships.” See New York State Department of Corrections and Community Supervision, *Visitors*, available at <https://DOCCS.ny.gov/visitors> [accessed June 28, 2021]. A true and correct copy of this landing page is at Exhibit 20.

28. DOCCS also makes available a comprehensive called *Handbook for Families and Friends of New York State DOCCS Inmates* (“DOCCS Handbook”) [Dec. 2019], available at <https://DOCCS.ny.gov/system/files/documents/2020/01/family-handbook-english-final-12.2019-002.pdf> [accessed June 28, 2021]. A true and correct copy of the DOCCS Handbook is at Exhibit 21.

29. Visitors to New York State Prisons are subject to stringent security measures. All visitors must be pre-approved. N.Y. Correct. Law § 146 [1]; see also New York Corrections and Community Supervision, Directive No. 4935 § V-C, *Outsiders Visiting or Applying to Visit Facilities* [May 19, 2020], available at <https://doccs.ny.gov/system/files/documents/2020/11/4935.pdf> [last accessed June 28, 2021]. A true and correct copy of Directive 4935 is at Exhibit 23. All visitor names are reported to the facility’s Superintendent. *Id.* § V-D. Visitors with criminal histories must receive the Superintendent’s permission to visit a facility. *Id.* § V-C. See also New York Corrections and Community Supervision, Directive No. 4403 § IV-B, *Inmate Visitor Program* [Aug. 23, 2016],

available at <https://doccs.ny.gov/system/files/documents/2020/11/4403.pdf> [last accessed June 28, 2021]. A true and correct copy of Directive 4403 is at Exhibit 24.

30. All visitors are searched and kept under careful observation during their visit. DOCCS Directive No. 4403 § III-E. Visitors must show valid identification. *Id.* § V-A. Visitors must pass through a metal detector or be searched with a hand scanner, or both. *Id.* § VI-A-1. If necessary, prison staff may conduct a limited visual search of a visitor’s person (*e.g.*, instructing a visitor to lift their shirt to show their waistline). *Id.* § VI-A-6. Prison Officers may conduct strip searches if they believe it to be necessary. *Id.* § VI-B. If a visitor refuses, they may be denied entry. *Id.* § VI-B-5. Additionally, visitors may be subject to substance detection/ion scan testing. *Id.* § VI-C. If a visitor refuses, they will be denied entry. *Id.* § VI-C-2.

31. No DOCCS Directive mentions visitor procedures concerning face recognition technology.

32. In fact, DOCCS has no publicly available information about the utilization of face recognition technology to screen, and potentially deny visitation to, visitors in any of its laws, rules or directives. *Id.* Indeed, none of DOCCS’s laws, rules or directives, nor DOCCS’s Visitor Page nor the DOCCS Handbook, mention face recognition technology at all. *Id.*

33. DOCCS notes that it “wants the visiting experience to be family friendly and positive.” *Id.* DOCCS makes “information concerning rules and regulations pertaining to visitation [...]available. *Id.* DOCCS advises visitors that “[t]o ensure the safety of family, friends who are visiting, as well as our facilities staff and the incarcerated population, visits are subject to DOCCS rules. To help address questions you may have about visitations, DOCCS has prepared a variety of resources” which are maintained on the webpage dedicated to Visitors. *Id.*

34. DOCCS makes no mention of face recognition technology at all, much less that “families and friends” would be subject to screening, and potentially denied visitation rights, through a face recognition system. And, of course, there is no publicly available information concerning access to, and use of, a visitor’s sensitive biometric information.

35. There is no public information about DOCCS’s utilization of face recognition technology for “visitation processing.”

36. There has been no public process, and no oversight or accountability, concerning DOCCS acquisition and deployment of this technology in DOCCS facilities.

37. There are no regulations, directives, guidance or publicly facing policy that address DOCCS’s utilization of this technology, let alone how to account for the serious inaccuracy of this technology that most often misidentifies people of color.

38. There is no publicly facing policy in place that speaks to limitations, if any, on who will have access to, and how they may use, the sensitive biometric data collected from the family members, friends, and loved ones who visit people who are under DOCCS’s custody.

39. There are no regulations, directives, guidance or public-facing policy that address what privacy protections, if any, accrue to the visiting families, friends and loved ones whose biometric data may be captured by DOCCS.

40. Among the questions raised by DOCCS’s deployment of face recognition technology are the following: What are the procedures or training materials for staff to explain what should happen when an “unwanted person” is identified by the system or what should happen when the system makes a false identification? How does DOCCS guard against automation bias, *i.e.* the propensity for humans to favor suggestions from automated decision-making systems and to ignore contradictory information made without automation, even if that

contradictory information is correct? Who will have access to the database? Will it be shared with local law enforcement or federal enforcement authorities like the United States Immigration and Customs enforcement agency? Who is in DOCCS's "unwanted visitor" database? How does someone get on that list and how might they get off of it? Will this technology be used to track those who associate with incarcerated individuals?

41. The NYCLU submitted a FOIL Request to DOCCS on September 23, 2020 (the "FOIL Request") seeking information about, among other things, the use by DOCCS of facial recognition technology at correctional facilities, including its use to screen family members, friends and other loved ones visiting those in DOCCS's custody. A true and correct copy of the FOIL Request is at Exhibit 1.

#### **The NYCLU's FOIL Request and DOCCS's Denials**

42. The FOIL Request" seeks information about, among other things, the use by DOCCS of face recognition technology at correctional facilities, including its use to screen visitors to those facilities.

43. The NYCLU's FOIL Request sought seven categories of records regarding the facial recognition system:

1. Records relating to DOCCS's adoption and/or use of the face recognition technology, including training materials, policies, protocols, or procedures addressing or relating in any way to:
  - a. any use of the face recognition technology by DOCCS at correctional facilities or elsewhere and the intended purpose of each such usage;
  - b. how the face recognition technology functions, or is designed to function;
  - c. instances when the face recognition technology has not functioned properly (e.g., when it has produced incorrect identification data or mismatched individuals in any way), including any actual or

- perceived bases or reason(s) for such improper operation or misidentification(s);
- d. how inaccurate results generated by the face recognition technology are supposed to be handled; and
  - e. how any and all inaccurate results generated by the face recognition technology have in fact been handled;
2. Any and all records regarding DOCCS's policies, procedures, and/or practices regarding visitors to DOCCS facilities, including all means to identify such visitors so as to permit visitation;
  3. Any and all records reflecting the process undertaken by DOCCS to review any proposals to obtain any form of the face recognition technology, including records of, or relating to, communications: (a) among employees, agents or representatives of DOCCS; (b) with any other New York State governmental agency or organization; or (c) with any vendor offering the face recognition technology;
  4. Any and all records reflecting research, studies, or data regarding the accuracy and/or efficacy of the face recognition technology that was reviewed by DOCCS at or before acquisition or deployment of the face recognition technology, or at any time since then, including the accuracy or efficacy with respect to various racial or ethnic groups;
  5. Any and all records indicating the ownership, maintenance, retention, destruction, access to, and security of the images and/or data produced by the face recognition technology, and any related procedures or protocols, relating to, among other things, whether any private company or entity, correctional facility, State or Federal law enforcement, or other agencies (including the United States Immigration and Customs Enforcement) are involved in its ownership, maintenance, retention, access, and/or security;
  6. Any and all records regarding the databases and/or other datasets used for individual identification, tracking, hot lists, or other matching functionalities, as well as how and under what circumstances new entries can be added; and
  7. Any and all records regarding the accuracy of face recognition technology across racial demographics, including accuracy or inaccuracy for particular racial or ethnic groups.

44. DOCCS acknowledged receipt of the NYCLU's FOIL Request on September 23, 2020, indicating that it would respond to the NYCLU's FOIL Request within approximately 20 business days. A true and correct copy of this response is at Exhibit 2. On October 13, 2020,

DOCCS informed the NYCLU that it needed to extend its response time to the NYCLU's FOIL Request to December 30, 2020. A true and correct copy of this extension letter is at Exhibit 3.

On December 28, 2020, DOCCS wrote the NYCLU to extend once again the DOCCS's time to respond to the NYCLU's FOIL Request to February 16, 2021. A true and correct copy of this extension letter is at Exhibit 4.

45. On January 29, 2021 -- four months after the NYCLU filed its FOIL Request, DOCCS denied the NYCLU's FOIL Request in its entirety without producing any responsive records. A true and correct copy of DOCCS's January 29, 2021 response to the FOIL Request is at Exhibit 5.<sup>8</sup> DOCCS's denial merely recited a list of FOIL exemptions without providing facts or reasoning for withholding the presumptively public requested information. DOCCS did not even bother to indicate which exemption they claimed applied to which record request, all in violation of Public Officers Law § 89 [4] [a].

46. DOCCS set forth the following FOIL exemptions:

Public Officers' Law § 87 [2] [f] where the records, if disclosed, could endanger the life or safety of any person;

- §87 [2] [g] where the records where records which are inter-agency or intra-agency materials which are not: statistical or factual tabulations or data; instructions to staff that affect the public; final agency policy or determinations; or external audits, including but not limited to, audits performed by the comptroller and the federal government;
- §87 [2] [i] where, if disclosed, would jeopardize the capacity of an agencies electronic information systems and infrastructure; and
- §87 [2] [d] where the records are trade secrets or are submitted to an agency by a commercial enterprise or derived from information obtained from a commercial enterprise and which if disclosed would cause substantial injury to the competitive position of the subject enterprise.

---

<sup>8</sup> DOCCS's January 29, 2021 denial letter is mistakenly dated January 29, 2020.

See Exhibit 5.

47. The NYCLU filed an administrative appeal with DOCCS's Office of Counsel, DOCCS's Records Access Appeals Officer, on February 11, 2021 (the "Appeal"). The Appeal explained that DOCCS had not provided sufficient justification for withholding records, did not provide a specific justification for each claimed FOIL exemption, and did not satisfy the statutory requirements for denying NYLPI's FOIL request. A true and correct copy of the NYCLU's Appeal is at Exhibit 6.

48. On March 1, 2021, DOCCS's Records Access Appeals Officer denied the Appeal. A true and correct copy of the March 1, 2021 denial of NYCLU's Appeal is at Exhibit 7.

49. DOCCS predicated its denial of six of the seven requests on the blanket assertion that the records sought could endanger the life and safety of any person, pursuant to Public Officers Law §87 [2] [f]. Yet DOCCS did not provide any information about how disclosure of the records sought would endanger anyone's life or safety.<sup>9</sup> See Exhibit 7.

50. Regarding requests 1 and 6 of the FOIL Request, DOCCS further asserted that the records sought were exempt under Public Officers Law §87 [2] [g], claiming production of any responsive record would jeopardize its electronic information systems and infrastructure because "[a]ll information can only be viewed by authorized and approved users, and only used in accordance with the policies and procedures of the Department." *Id.* Yet DOCCS did not identify how the requested records "could allow unauthorized access to, and potentially the disclosure of, confidential security information." *Id.*

51. DOCCS also failed to provide any explanation for its claim that the interagency materials exemption under Public Officers Law §87 [2] [g] applied to FOIL Requests 3,4, 5 and

---

<sup>9</sup> A chart showing the NYCLU's record requests and DOCCS's invocation of exemptions is at Exhibit 8.

6, instead simply parroting the words of the statute rather than identifying which portions of the requested records were subject to the interagency materials exemption. *Id.*

52. Regarding FOIL Request 3, DOCCS merely recited the statutory language of proprietary information/trade secrets exemption under Public Officers Law §87 [2] [d], again without explaining its reasons for claiming that exemption or describing which portion(s) of the responsive records were subject to this exemption. *Id.*

53. With regard to section 7 of the FOIL Request, DOCCS offered a certification pursuant to Public Officers Law §89 [3] that “a diligent search was conducted and no responsive records could be located” relating to DOCCS’s consideration of the accuracy of face recognition technology across racial demographics. *Id.* Based on this response, a very strong, and troubling, inference can be drawn that DOCCS gave no consideration whatsoever to racial accuracy issues and collateral consequences worked on those incarcerated and their family members and friends attempting to visit DOCCS’s facilities -- either prior to, or after, DOCCS’s adoption of face recognition technology as part of the “visitation screening” process.

54. DOCCS’s refusal to release any records keeps valuable records shrouded by a cloak of secrecy that undermines the purposes that FOIL serves: namely, fostering transparency and accountability between the government and the public. As utilization of face recognition technology continues to have high reported error rates, continues to be biased against people of color and continues to demonstrate deep-seated automation biases in those who deploy this technology, the public’s right to access contemporaneous records of utilization by New York State’s carceral system has never been more paramount.

55. Petitioner timely commenced this Article 78 proceeding, within four months of the DOCCS’s final determination of Petitioner’s Appeal, *see* CPLR § 217, to force Respondents to

comply with their obligations under FOIL and to provide Petitioner with records responsive to the NYCLU's FOIL Request.

### **CAUSE OF ACTION**

#### **ARTICLE 78 REVIEW OF WRONGFUL DENIAL OF FOIL REQUEST**

56. Petitioner repeats and realleges each and every allegation contained in the preceding paragraphs as if fully set forth herein.

57. Article 78 is the appropriate method of review of final agency determinations concerning FOIL requests.

58. Petitioner has a legal right under FOIL to gain access to the public records sought in the NYCLU's FOIL Request.

59. FOIL recognizes the public's right to access and review government documents, and agency records are presumed to be public and subject to disclosure under FOIL.

60. Respondents did not provide any responsive records and have failed to properly invoke exemptions under FOIL.

61. Respondents have not met their burden to provide specific and particularized justifications for withholding the requested records.

62. None of the exemptions from FOIL that have been cited by Respondents, nor any other FOIL exemptions, apply to the material Petitioner has requested.

63. Petitioner has exhausted its administrative remedies and has no other remedy at law.

64. Petitioner has not made a prior application for the relief requested herein.

65. Because Respondents have no reasonable basis for withholding the records requested by the NYCLU in its FOIL Request dated September 23, 2020, Petitioner is entitled to the records which are the subject of this action.

**CLAIM FOR RELIEF**

Petitioner respectfully requests that this Court enter judgment, pursuant to CPLR § 7806, on its behalf:

- a. directing Respondents New York State Department of Commission on Corrections and Community Supervision (“DOCCS”) and DOCCS Acting Commissioner Anthony J. Annucci to comply with their duty under New York’s Freedom of Information Law (“FOIL”) to provide Petitioner access to the records requested by Petitioner in its FOIL request dated September 23, 2020;
- b. ordering, in the alternative, an *in camera* review of the records requested by Petitioner in the event this would better inform the Court as to their contents;
- c. awarding Petitioner its reasonable attorneys’ fees and litigation costs pursuant to Public Officers Law § 89 [4] [c]; and
- d. granting Petitioner such other and further relief as this Court deems necessary and equitable.

Dated: June 30, 2021  
New York, New York

Respectfully Submitted,



BETH HAROULES  
LISA J. LAPLACE  
New York Civil Liberties Union Foundation  
125 Broad Street, 19th Floor  
New York, N.Y. 10004  
Tel: (212) 607-3300  
bharoules@nyclu.org  
llaplace@nyclu.org

*Counsel for Petitioner the New York Civil  
Liberties Union*

**VERIFICATION**

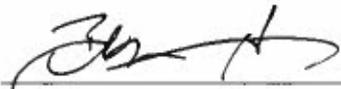
STATE OF NEW YORK    )  
  ) SS:  
COUNTY OF NEW YORK )

Lisa J. Laplace, being duly sworn, deposes and states under penalty of perjury:

1. I am a Senior Staff Attorney at the New York Civil Liberties Union Foundation and represent the Petitioner in these proceedings.
2. I make this verification pursuant to C.P.L.R. § 3020.
3. I have read the attached Verified Petition and know its contents.
4. I affirm that the exhibits to the Verified Petition are true and correct copies of the documents submitted as exhibits.
5. The statements in the Verified Petition are true to my knowledge, or upon information and belief. As to those statements that are based upon information and belief, I believe those statements to be true.

  
\_\_\_\_\_  
Lisa J. Laplace

Sworn to and subscribed before me  
this 29th day of June, 2021

  
\_\_\_\_\_  
Notary Public  
**BETH HAROULES**  
Notary Public, State of New York  
No. 02HA4890282  
Qualified in New York County  
Commission Expires March 30, 2025