BY ELECTRONIC MAIL to BiometricRFI@ostp.eop.gov

January 14, 2022

Suresh Venkatasubramanian
Assistant Director
Office of Science and Technology Policy
White House
1600 Pennsylvania Ave NW
Washington, DC 20500

RE: Request for Information Response: Biometric Technologies

NYCLU
ACLU of New York

125 Broad St. 19th Fl.
New York NY 10004
(212) 607-3300

Donna Lieberman
Executive Director

Wendy Stryker
President

Dear Assistant Director Venkatasubramanian:

The New York Civil Liberties Union ("NYCLU") submits these comments in response to the White House Office of Science and Technology Policy's ("OSTP") Request for Information regarding Biometric Technologies (document number 2021-21975) dated October 8, 2021.

The NYCLU, the New York State affiliate of the American Civil Liberties Union, is a nonprofit, nonpartisan organization with eight regional offices and more than 200,000 members and supporters across the state. The NYCLU's mission is to defend and promote the fundamental principles, rights and values embodied in the Bill of Rights of the U.S. Constitution and the Constitution of the State of New York.

We work to expand the right to privacy, increase the control individuals have over their personal information, and ensure civil rights and liberties are enhanced rather than compromised by technological innovation. We have a long history of vigorously defending students' rights, including access to education and privacy rights, as well as protecting New Yorkers from abusive policing, including through challenging invasive and discriminatory surveillance practices. Bringing together these areas of expertise, we are the leading organization advocating for a ban on the use of biometric surveillance against public school students and have advocated against the use of biometric surveillance by New York law enforcement and other government agencies.

Biometric surveillance technologies, which include face, voice, and gait recognition, give unprecedented power to track who we are, where we go, and who we meet, enabling an invasion of privacy that reaches far beyond traditional surveillance techniques. They are highly flawed and racially biased. The use of these technologies by government agencies presents a clear danger to our civil rights and liberties and threatens to erode our fundamental rights to privacy, free speech, and equal treatment under the law. It is urgently imperative that the federal government act to stop the proliferation of biometric surveillance and ban its use.

1. The Lockport City School District's Deployment of Facial Recognition Technology

In spring 2018, the NYCLU was notified by concerned community members that the Lockport City School District ("Lockport" or the "District") purchased facial recognition technology to use in its schools, using funding from New York's Smart Schools Bond Act ("SSBA"). The SSBA, approved by voters in 2014, authorized $2 billion in general obligation bonds for schools to upgrade their infrastructure and technology to "improve learning and opportunity for students throughout" New York.[1] Many schools used these funds to improve wireless internet connectivity or purchase computers, tablets, and 3D printers for use in the classroom.

Lockport, however, spent almost all the $4 million it was awarded for "new cameras and wiring…to provide viewing and automated facial and object recognition of live and recorded surveillance video," as well as "additional surveillance servers…to provide enhanced storage of recorded video and processing."[2] The decision to implement this technology appears to have been made without sufficient public involvement as required by state law, and involved a security consultant who may have had a conflict of interest.[3]

Over the course of the next 18 months, the NYCLU repeatedly contacted the New York State Education Department ("NYSED") with concerns over issues of accuracy, bias, privacy, transparency, and data security with Lockport's system. At the NYCLU's urging, NYSED engaged with the District and required it to undertake a privacy assessment, reviewed Lockport's draft privacy policies, and prohibited Lockport from testing its face recognition system multiple times.[4]

On November 27, 2019, however, NYSED issued a determination letter granting Lockport permission to utilize its biometric surveillance system, despite unanswered questions about the system's functionality and the risks of this technology. On January 2, 2020, Lockport deployed its facial recognition system in schools, impacting more than

[1] Smart Schools Bond Act (2014), http://www.p12.nysed.gov/mgtserv/smart_schools/home.html; *see also* Smart Schools Bond Act Implementation Guidance, http://www.p12.nysed.gov/mgtserv/documents/SSBAGuidancerev_6_1_18_Final.pdf.

[2] Lockport City School District, Smart Schools Investment Plan (2016-2017), http://p1232.nysed.gov/mgtserv/documents/LOCKPORTCITYSD.pdf (last modified October 23, 2017) (emphasis added) ("Lockport SSBA Plan").

[3] Lockport City School District, August 17, 2016 Proceedings of the Board of Education, https://www.nyclu.org/sites/default/files/field_documents/lockport_board_meeting.pdf. Despite the lack of comment at the hearing, the District certified on its application that it had engaged all four categories of stakeholders – parents, teachers, students, and community members. *See* Lockport SSBA Plan, at 1. In addition, the president of the Lockport Education Association stated that teachers were not consulted in a discussion of how to use the funding, as was required. *See* Tim Fenster, *Trying for More Secure Schools: Lockport district turning to facial recognition software*, Lockport Union-Sun & Journal, Mar. 4, 2018, http://www.lockportjournal.com/news/local_news/trying-for-more-secure-schools-lockport-district-turning-to-facial/article_f1cc9cfa-0898-5da0-ac5d-d600df21bed7.html.

[4] *Shultz v. NYSED*, Index No. 904134-20, Docket Entry 73, Amended Petition, New York Supreme Court, Albany County 2020; *see also* Davey Alba, *The First Public Schools in the US Will Start Using Facial Recognition Next Week*, May 30, 2019, Buzzfeed News, https://www.buzzfeednews.com/article/daveyalba/lockport-schools-facial-recognition-pilot-aegis.

4,000 students.[5] This was short lived as the COVID-19 pandemic forced Lockport to close schools in March 2020.

In June 2020, the NYCLU, on behalf of four parents, sued NYSED over its approval of Lockport's system, alleging that the agency's decision violated state privacy laws intended to protect student data.[6] Shortly thereafter, the New York State Legislature passed A6787/S5140, the first statewide bill in the country prohibiting the use of biometric identifying technology in schools.[7] The bill was signed in December 2020, enacting section §106-b of the New York State Technology Law, which prohibits the purchase or use of biometric identifying technology[8] in all public and nonpublic elementary and secondary schools until the Department of Information Technology, in partnership with NYSED, issues a report on the risks and benefits of this technology in schools. The moratorium is in effect until July 2022 or until the Commissioner of Education authorizes the use of biometric identifying technology following the report – whichever comes later.[9] This law was a direct response to Lockport's purchase and concerns over the racial disparities in identification of people of color, risks of data breaches, and access to the highly sensitive data produced by the system.

Currently, the moratorium remains in place and Lockport's system remains deactivated. It does not appear that the Department of Information Technology or NYSED has initiated the study required by the law. Additionally, the state committee tasked with reviewing school district funding proposals, the Smart Schools Review Board (the "Review Board"), has approved multiple school districts' grant applications that include biometric identifying technology. We believe this is due to an ignorance of the law, misunderstanding of the technology, and relentless pressure on school districts by for-profit entities attempting to sell these products.

On February 24, 2021, it was reported that the Smart Schools Review Board approved $21.2 million of SSBA funds for "high tech security" projects,[10] including seven school district plans for surveillance technologies which include facial recognition capabilities or other "self-learning analytics."[11] On August 12, 2021, the Review Board approved another school district proposal explicitly including "self-learning video

[5] *January 2020 AEGIS Security System Update*, https://www.smore.com/utzgy.

[6] *Shultz et al v. New York State Education Department*, https://www.nyclu.org/en/cases/shultz-et-al-v-new-york-state-education-department.

[7] A6787 (Wallace)/S5140 (Kavanagh), https://www.nysenate.gov/legislation/bills/2019/a6787.

[8] Biometric identifying technology is "any tool" that uses "an automated or semi-automated process that assists in verifying a person's identity based on a person's biometric information." N.Y. Tech Law §106-b(1)(a).

[9] N.Y. Tech Law §§106-b(2)(a), (3)(a).

[10] *Governor Cuomo Announces $59.9 Million For School Technology Upgrades Through the Smart Schools Bond Act*, February 24, 2021, https://www.wnypapers.com/news/article/current/2021/02/24/145481/59.9-million-for-school-technology-upgrades-through-smart-schools-bond-act.

[11] *See, e.g.*, Otselic Valley Central School District (requesting funding for, among other things, a license for Avigilon ACC7 software which explicitly includes "facial recognition technology") http://p1232.nysed.gov/mgtserv/documents/Georgetown-SouthOtselicCSD-Application1.pdf; *see also*, proposals from Binghamton, Canaseraga, Carmel, East Syracuse Minoa, Stillwater, and Sullivan West.

analytics" and biometric identifying capabilities.[12] These projects include camera, software, and analytics products from a vendor called Avigilon, including systems known as Avigilon Control Center ("ACC") 6 and 7.[13] ACC 7 explicitly includes "facial recognition technology" to "identify[] people of interest based on secure watch list(s)."[14] ACC 6 includes an "Appearance Search" feature which is described as "a sophisticated deep learning AI search engine for video" that uses "face analytics" including "the unique characteristics of a person's face… to understand that it is searching for the same person, even if items such as their clothing change over time."[15,16] Fulfillment of these proposals is a clear violation of New York law.[17]

1.1 Implications of Facial Recognition Technology in School Settings

Lockport is one of the first public school districts in the country to implement biometric identifying technology in a school setting[18] and, after wasting years of taxpayer money and human capital on a system it cannot use, it should be a cautionary tale for other districts intent on using similar technologies. The use of facial recognition and other biometric surveillance technologies in schools presents a number of potential harms to students and we urge OSTP to consider these carefully in its review of biometric surveillance.

First, there are well-documented issues with the accuracy and bias of facial recognition technology, particularly when used to identify women and people of color.[19]

[12] Brighton Central School District (requesting funding for a license for Avigilon ACC6 software and "self-learning video analytics."), http://p1232.nysed.gov/mgtserv/documents/BrightonCSDCouncilRock.pdf.
[13] Avigilon Control Center 6 (ACC 6) software "combines an intuitive interface with advanced search functions called Avigilon Appearance Search." Appearance Search technology "is a sophisticated AI search engine for video data that incorporates the characteristics of a person's face." Avigilon describes their ACC 6 software as "self-learning video analytics." Avigilon Control Center 7 (ACC 7) incorporates "AI-powered facial recognition technology to detect people of interest based on one or more secure watch lists" and has "next-generation analytics and self-learning video analytics," https://www.avigilon.com/support/software/acc7/avigilon-acc7-datasheet-en.pdf.
[14] *See Avigilon Control Center 7 Software*, https://www.avigilon.com/products/acc/7.
[15] https://www.avigilon.com/products/ai-video-analytics/appearance-search.
[16] It also appears that ACC 6 will be discontinued so these Districts may need to update to ACC 7 which explicitly includes facial recognition technology, https://assets.avigilon.com/file_library/pdf/acc6/ACC_6_EOL_Notice.pdf.
[17] In addition to biometric identifying technology, the NYCLU is also concerned about the use of online surveillance systems for school-issued devices. As you may know, GoGuardian and other similar products purport to monitor all online student activity "under the guise of student safety" yet these products raise concerns regarding student and family privacy and racial bias inherent in such surveillance programs. *See* letter from Senators Elizabeth Warren, Edward J. Markey, and Richard Blumenthal, Sept. 29, 2021, https://www.warren.senate.gov/imo/media/doc/2021.09.29%20Shinde%20-%20EdTech%20letter.pdf.
[18] Davey Alba, *Facial Recognition Moves Into a New Front: Schools*, THE NEW YORK TIMES, Feb. 6, 2020, https://www.nytimes.com/2020/02/06/business/facial-recognition-schools.html.
[19] *See, e.g.,* Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, PROCEEDINGS OF MACHINE LEARNING RESEARCH (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf; Patrick Grother, Mei Ngan & Kayee Hanaoka, *Face recognition vendor test part 3: demographic effects* NIST IR 8280 (2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf; and Cynthia M. Cook et al., *Demographic Effects in Facial Recognition and their Dependence on Image Acquisition: An Evaluation of Eleven*

As with any artificial intelligence, biometric surveillance carries the biases of the people who design it and the information used to train it. In the system purchased by Lockport, for example, Black women are 16 times more likely to be misidentified than white men.[20]

In all facial recognition systems, the databases to which the images are paired can be unreliable—they are not required to be vetted for quality and they are not created with any requirement of due process—and because they are provided by law enforcement, often disproportionately include young men of color.[21] This creates an unfair and undue risk of false identification for students of color, who are already more likely to be unfairly targeted by the criminal justice and school discipline systems, fueling the school-to-prison pipeline.

Second, these systems infringe on the privacy rights of students, parents, and staff. Student images are a protected part of a student's biometric record, included in the definition of "personally identifiable information" under the Family Educational Rights and Privacy Act and New York's student data privacy law, Education Law §2-d.[22] Once an individual's photo is uploaded to a school facial recognition system, the system will track that person's movements around the school and with whom they interacted. These systems can turn students' and staff members' every step into evidence of an infraction or crime, can trace a student's use of sensitive services such as the nurse's or counselor's office, and can be used to criminalize ordinary child behavior and personal interactions, potentially violating the First Amendment right to association. These systems can even be used with immigration enforcement databases, meaning students could be targeted by immigration authorities simply for coming to school—putting themselves and their families at risk of deportation.

Third, the use of this technology raises concerns about data maintenance and retention. For example, how long the associated data will be retained, how securely it will be stored, who will pay for the upkeep of additional data storage, who will have access to it and how it may be shared, including any connection to law enforcement databases. While there is good reason to maintain most education records for the student's entire school career, surveillance records should be retained for the shortest possible time.

Fourth, these systems, like all databases, are vulnerable to hacking.[23] But unlike passwords or credit card numbers, a person's biometric information is highly sensitive and

Commercial Systems, 1 IEEE TRANSACTIONS ON BIOMETRICS, BEHAVIOR, AND IDENTITY SCIENCE 32–41 (2019).

[20] *Shultz v. NYSED*, Index No. 904134-20, New York Supreme Court, Albany County, Schwarz Aff. Ex. 12, https://www.nyclu.org/sites/default/files/field_documents/schwarz_affidavit.pdf.

[21] Sidney Fussell, *School Districts can Hardly Wait to Start Tracking Kids with Police State-Style Face Recognition*, Gizmodo, May 21, 2018, https://gizmodo.com/school-districts-can-hardly-wait-to-start-tracking-kids-1826197713.

[22] "Biometric record, as used in the definition of personally identifiable information, means a record of one or more measurable biological or behavioral characteristics that can be used for automated recognition of an individual. Examples include fingerprints; retina and iris patterns; voiceprints; DNA sequence; facial characteristics; and handwriting." 34 C.F.R. § 99.3.

[23] In February 2018, CCTV systems were hacked at four schools in the UK and aired online in real time. ACLU of Arkansas Warns Schools of Privacy Risks of Biometric Surveillance Systems, Mar. 16, 2018, https://www.acluarkansas.org/en/press-releases/aclu-arkansas-warns-schools-privacy-risks-biometric-surveillance-systems.

cannot be changed if there is a security breach. Storing massive amounts of this data collected from children, parents, and school employees raises the risk that personally identifiable information may be hacked, stolen, or sold.[24]

Fifth, these systems can cost millions of dollars, taking vital funding away from instruction. "Ed Tech," including school surveillance, has become a lucrative industry for private vendors and security consultants who see the deep pockets of public funding and may take advantage of schools' well-intended efforts to protect students.

Sixth, these systems negatively impact school climate. Students should feel welcomed and supported in schools—not made to feel like suspects who must be surveilled throughout the school building.

Finally, these systems, particularly Lockport's, have been implemented without full transparency and input from critical stakeholders. Private vendors are incentivized to conceal system information to protect proprietary interests. Students, families, teachers, and other community members must be consulted as to whether the use of biometric identifying technology should be used in a school and should be engaged in a frank discussion of the potential harms and benefits.

1.2 Recommendations Concerning Biometric Technologies in School Settings

Lockport's use of facial recognition technology highlights the immediate need for protections at the federal level. There is currently no federal guidance or restrictions on the use of facial recognition and other biometric surveillance technologies in schools. As highlighted above, these systems pose real risks to students and are inappropriate for use in an educational context. The OSTP should work with the United States Department of Education to issue guidance advising schools that facial recognition and other biometric identifying technologies should not be utilized in school settings and that no federal education funding should be utilized for purchasing such systems. Above all, the OSTP should emphasize that schools and districts have an obligation to protect student privacy and ensure that schools are welcoming places for all children to learn and thrive, not for them to be surveilled.

2. Biometric Surveillance by Law Enforcement

In the absence of federal- or state-mandated guidelines or restrictions on the acquisition and use of biometric surveillance technologies, law enforcement agencies throughout New York have been free to set their own rules. Because these departments so frequently attempt to evade public demands for greater transparency and oversight, the full reach of the surveillance state is unknown. What we do know, however, is that the biometric surveillance systems currently being used by law enforcement agencies make countless people, particularly people of color, less safe. As mentioned above, facial recognition technology is notoriously inaccurate, failing to correctly match faces to a

[24] Matthew Gault, *DHS Admits Facial Recognition Photos Were Hacked, Released on Dark Web*, Vice, Sept. 24, 2020, https://www.vice.com/en/article/m7jzbb/dhs-admits-facial-recognition-photos-were-hacked-released-on-dark-web.

comparison database, especially when it comes to identifying women and people of color.[25] When these systems are used by law enforcement, the risks of misidentification cannot be overstated, especially considering the potential for lifelong consequences that can result from even a single encounter with law enforcement.[26]

Even if the accuracy of the technologies were to improve, biometric surveillance systems would continue to operate with built-in bias. This is because the databases that the technologies rely on for comparators are, themselves, typically generated by law enforcement. For example, facial recognition systems may depend on mugshot databases, which—reflecting the disproportionate rate at which communities of color are policed—have many more faces of people of color in them. The biased policing practices that continue to disproportionately target and criminalize people of color[27] will mean that these technologies will end up being used disproportionately against people of color.

While the risks of misidentification are obvious, the potential for these technologies to produce accurate identifications should also raise serious concerns in the law enforcement context. The widespread deployment of biometric surveillance systems – especially when coupled with existing surveillance infrastructures – would give law enforcement the ability to easily identify and track a person's every movement: where they go to school, which doctors they visit, which places of worship they attend, and which protests and demonstrations they decide to attend. The New York Police Department ("NYPD" or the "Department") already has more than 20,000 cameras integrated into its Domain Awareness System[28] and plans to increase that number to a staggering 50,000 cameras.[29] And the Department continues to introduce even more cameras in the form of officer body-worn cameras and unmanned drones. It also makes use of social media photographs; in August of 2020, the NYPD used facial recognition software to identify a Black Lives Matter activist during a protest against police brutality through a photo from his Instagram account.[30]

Given the NYPD's long and troubling history of engaging in surveillance tactics that have targeted political dissent, criminalized communities of color, and singled out Muslim New Yorkers for suspicionless surveillance solely on the basis of their religion,

[25] *Supra,* note 19.

[26] *See, e.g.,* Kashmir Hill, *Wrongfully Accused by an Algorithm*, The New York Times, June 24, 2020, https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html, Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, The New York Times, Dec. 29, 2020, https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html.

[27] *See, e.g.*, Annual Stop-and-Frisk Numbers, NYCLU, https://www.nyclu.org/en/stop-and-frisk-data (demonstrating that police stop, detain, frisk, and arrest Black and brown people at disproportionate rates).

[28] A Conversation with Jessica Tisch '08, HARVARD LAW TODAY (2019), https://today.law.harvard.edu/a-conversation-with-jessica-tisch-08/.

[29] Preparedness Grant Effectiveness Case Study: New York City, 27 (2021), https://www.fema.gov/sites/default/files/documents/fema_nyc-case-study_2019.pdf.

[30] George Joseph & Jake Offenhartz, *NYPD Used Facial Recognition Technology In Siege Of Black Lives Matter Activist's Apartment*, Gothamist, Aug. 14, 2020, https://gothamist.com/news/nypd-used-facial-recognition-unit-in-siege-of-black-lives-matter-activists-apartment.

the dangers that hypothetically accurate biometric surveillance technologies would pose to our most fundamental rights and liberties would be no less concerning.[31]

Through litigation, the public has learned of the highly flawed, unscientific, and even unlawful practices that pervade the NYPD's facial recognition program since its inception over ten years ago. A 2019 report from the Georgetown Law Center on Privacy and Technology revealed that the NYPD engaged in such dubious tactics as uploading photographs of celebrity lookalikes in lieu of actual suspect photos, editing suspect photographs (including through effects that substantially alter the suspect's actual appearance) in order to generate a potential match, and apprehending suspects "almost entirely on the basis of face recognition 'possible matches'" without taking additional investigative steps to establish probable cause.[32]

Investigative reporters have uncovered even more failures by the NYPD to safeguard sensitive information and ensure officer adherence to even minimal standards on the use of biometric surveillance systems. It was revealed that the NYPD was including mugshots of juveniles and other sealed arrest records in its facial recognition database.[33] And despite the NYPD's explicit rejection, citing concerns about security and the potential for abuse, of software developed by Clearview AI that scrapes billions of photographs from social media platforms and other public sources, it has been reported that dozens of "rogue" officers have continued to use the software in more than 11,000 searches.[34] The reporting noted that "[i]t is not clear if the NYPD officers will face any disciplinary action for using the app,"[35] raising doubts about the willingness of the Department to enforce even its own rules and raising concerns about their ability to safeguard sensitive biometric information going forward. The NYPD is far from the only agency deserving of closer scrutiny; at least 61 law enforcement agencies across New York State (*see figure 1*) have secretly used Clearview AI's software, which includes biometric data on virtually everyone who has ever uploaded photos to Facebook, Instagram, Twitter, Venmo, or other social media platforms.[36]

[31] A few examples of the many cases the NYCLU has litigated involving NYPD surveillance abuses include *Handschu v. Special Services Division* (challenging surveillance of political activists), *Raza v. City of New York* (challenging the NYPD's Muslim Surveillance Program), and *Millions March NYC v. NYPD* (challenging the NYPD's refusal to respond to a Freedom of Information Law request seeking information about whether the NYPD is using invasive technology to infringe on the protest rights of Black Lives Matter advocates).

[32] Clare Garvie, Georgetown Law Center on Privacy & Technology, Garbage In, Garbage Out: Face Recognition on Flawed Data, (2019), https://www.flawedfacedata.com/.

[33] Joseph Goldstein & Ali Watkins, *She Was Arrested at 14. Then Her Photo Went to a Facial Recognition Database*, THE NEW YORK TIMES, Aug. 1, 2019, https://www.nytimes.com/2019/08/01/nyregion/nypd-facial-recognition-children-teenagers.html.

[34] *See, e.g.,* Craig McCarthy, *Rogue NYPD Cops are Using Facial Recognition App Clearview*, N.Y. POST, Jan. 23, 2020, https://nypost.com/2020/01/23/rogue-nypd-cops-are-using-sketchy-facial-recognition-app-clearview/; Ryan Mac, Caroline Haskins & Logan McDonald, *Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA*, BuzzFeed News, Feb. 27, 2020, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement.

[35] *Id.*

[36] *See, e.g.,* Ryan Mac et al., *How A Facial Recognition Tool Found Its Way Into Hundreds Of US Police Departments, Schools, And Taxpayer-Funded Organizations*, BuzzFeed News, April 6, 2021, https://www.buzzfeednews.com/article/ryanmac/clearview-ai-local-police-facial-recognition; and Kashmir

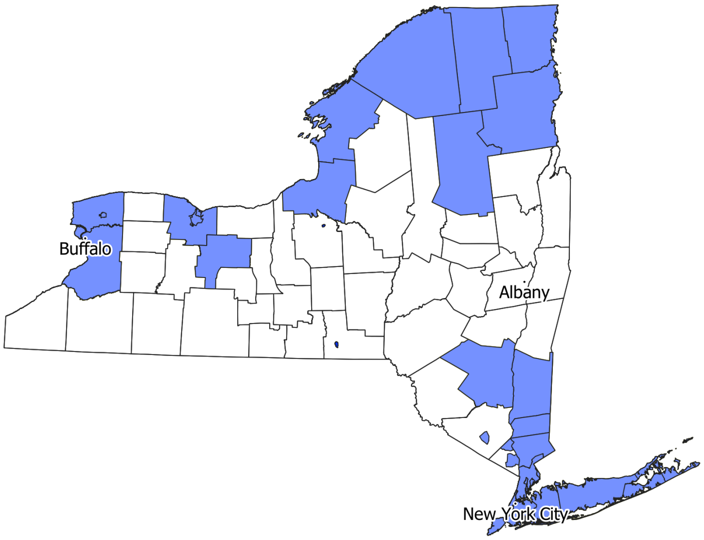

Fig 1: New York law enforcement agencies that have used Clearview AI.

The widespread availability of biometric technologies has led to deployments across agencies and industries, which law enforcement has attempted to exploit. In one particularly alarming example, the Metropolitan Transportation Authority and the NYPD partnered with IBM to develop software to search for people by their skin color in the transit system.[37] And Amazon Ring has partnered with hundreds of law enforcement agencies, including on Long Island, to facilitate data sharing from privately installed devices to the police.[38] Some of these systems offer or plan to offer other forms of biometric recognition such as affect recognition and aggressive or suspicious behavior detection, whose outcomes are severely inaccurate and plagued by disparate impacts for Black people.[39]

Correctional facilities have also become a testing ground for biometric surveillance technologies. The New York Department of Corrections and Community Supervision

Hill, *The Secretive Company That Might End Privacy as We Know It*, THE NEW YORK TIMES, Jan. 18, 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[37] George Joseph & Kenneth Lipp, *IBM Used NYPD Surveillance Footage to Develop Technology That Lets Police Search by Skin Color*, THE INTERCEPT, Sept. 6, 2018, https://theintercept.com/2018/09/06/nypd-surveillance-camera-skin-tone-search/.

[38] Drew Harwell, *Doorbell-Camera Firm Ring Has Partnered With 400 Police Forces, Extending Surveillance Concerns*, WASHINGTON POST, Aug. 28, 2019, https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach; Catherine Thorbecke, *Long Island Police Partner with Amazon's Ring to Crack Down on Porch Pirates*, ABC NEWS, Dec. 4, 2019, https://abcnews.go.com/Technology/long-island-police-crack-porch-pirates-amazon-ring/story?id=67489715.

[39] *See* Lisa Feldman Barrett et al., *Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements:*, PSYCHOLOGICAL SCIENCE IN THE PUBLIC INTEREST (2019), https://journals.sagepub.com/eprint/SAUES8UM69EN8TSMUGF9/full; LAUREN RHUE, *Racial Influence on Automated Perceptions of Emotions* (2018), https://doi.org/10.2139/ssrn.3281765.

("DOCCS") uses facial recognition for "visitation processing," deploying it to deny visitation to family members, friends, and other loved ones who wish to visit people in DOCCS's custody.[40] DOCCS has not released any information about its utilization of facial recognition for "visitation processing," and its use has not been subject to any public oversight. Additionally, DOCCS deploys a telephone system with voice recognition technology to collect and analyze voiceprints of not only the person who is incarcerated, but other parties on the call. The vendor offers investigative support, identification capabilities, call monitoring, behavioral analysis, suspicious keyword notification, pattern analysis, and even location tracking of the called party. Yet voice recognition tools have similar racial bias as other biometric technologies; studies have shown error rates for Black speakers are twice as high compared to white speakers.[41] In March 2021, it was revealed that a vendor recorded confidential attorney-client calls and provided them to New York City district attorneys.[42] A recent audit disclosed that nearly 2,300 calls to attorneys were recorded.[43]

Law enforcement use of biometric surveillance technologies will only continue to expand absent federal oversight. The OSTP should work with the United States Department of Justice to issue clear guidance advising law enforcement agencies against the continued use of biometric surveillance technologies given the grave risks that they pose to privacy, civil liberties, and racial justice.

3. Conclusion

The ever-expanding deployments of biometric surveillance and the immense risks associated underscore the immediate need for a ban on biometric surveillance by government, in particular in schools, by law enforcement, and in other areas where our fundamental rights are at stake.

Sincerely,

Stefanie D. Coyle
Deputy Director
Education Policy Center

Daniel Schwarz
Privacy & Technology Strategist
Policy Department

[40] Beth Haroules & Lisa LaPlace, *NYCLU v. DOCCS*, New York Civil Liberties Union (2021), https://www.nyclu.org/en/cases/nyclu-v-doccs.

[41] *See e.g.*, *Voicing Erasure*, ALGORITHMIC JUSTICE LEAGUE (2020), https://www.ajl.org/voicing-erasure; Allison Koenecke et al., *Racial disparities in automated speech recognition*, 117 PNAS 7684–7689 (2020).

[42] Chelsia Rose Marcius, *NYC's 5 DA offices wound up with recordings of confidential jailhouse calls between inmates and lawyers*, NYDAILYNEWS.COM, (2021) https://www.nydailynews.com/new-york/ny-jails-recordings-attorney-client-privilege-calls-20210321-tzbyxwnle5dc5jgvi5cona6wry-story.html.

[43] Noah Goldberg & John Annese, *NYC Correction contractor recorded thousands more lawyer-client jail phone calls than first reported; could jeopardize court cases*, NYDAILYNEWS.COM, (2021), https://www.nydailynews.com/new-york/nyc-crime/ny-audit-shows-doc-listened-in-on-even-more-lawyer-inmate-calls-20211230-zni5qacdhjaozok7rdmwyg2wsm-story.html.