STOP
SURVEILLANCE TECHNOLOGY
OVERSIGHT PROJECT

40 Rector Street, 9th Floor
New York, New York 10006
www.StopSpying.org | (212) 518-7573

MEMORANDUM

Date: July 24, 2023
To: New York State Senate Rules Committee, New York State Assembly Committee, Majority Leader Stewart-Cousins, Speaker Heastie
From: The Surveillance Technology Oversight Project ("S.T.O.P.")

Re: S.T.O.P. Memorandum in Opposition to S6656 / A2621

S.T.O.P. is a community-based civil rights group that advocates and litigates against discriminatory surveillance. Our work highlights the discriminatory impact of surveillance on Muslim Americans, immigrants, the LGBTQ+ community, Indigenous peoples, and communities of color, particularly the unique trauma of anti-Black policing.

We write to express our opposition to S6656 / A2621, which would promote invasive, insecure, and error-prone biometric technology. The bill would encourage bars, restaurants, and stores to use experimental apps to confirm customers' ages. We don't need a replacement for time-tested IDs like driver's licenses, but this bill would transform the corner store into a TSA checkpoint, using fingerprints, iris scans, and facial recognition to track customers' ages.

S6656 / A2621 promotes technology that's as creepy as it is biased. Facial recognition has been proven to be racist and error prone, often times 100 times less accurate for Black women than for white men.[1] These types of biometric technologies risk creating digital segregation, systematically excluding Black, Latinx, and Asian customers because of the color of their skin and the errors in the algorithm. But it gets even worse. These biometric systems will become a target for cybercriminals around the world, a repository of some of New Yorker's most sensitive information. When our biometric information is compromised, there's simply no going back…our identity can be compromised for the rest of our lives. And ultimately, many of these systems will make it even easier for minors to buy alcohol, cigarettes, and cannabis.

[1] Drew Harwell, *Federal Study Confirms Racial Bias of Many Facial-Recognition Systems Casts Doubt on Their Expanding Use*, WASH. POST (Dec. 19, 2019), https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/; Jesse Damiani, *New Research Reveals Facial Recognition Software Misclassifies Transgender Non-Binary People*, FORBES (Oct. 29, 2019), https://www.forbes.com/sites/jessedamiani/2019/10/29/new-research-reveals-facial-recognition-software-misclassifies-transgender-non-binary-people/?sh=497bb0b4606b.

This law expands facial recognition at a moment when our state should be outlawing it. Already, the technology has wrongfully jailed innocent Black men around the country, and its expansion into stores will only lead to more racist wrongful arrests.[2]

Even if facial recognition correctly identified every person, it would still be used in accordance with existing biases.[3] Black, brown, and undocumented New Yorkers are already over-policed and over-surveilled.[4] Expanding facial recognition into thousands of stores will magnify racist patterns of policing and lead to more arrests of Black and brown youth—who are already arrested more than twice as often as white youth.[5] One retail store, Rite Aid, has already fallen into this practice by installing facial recognition cameras in areas with large communities of color.[6] In fact, in the first major rollout of the technology, 52 out of the 65 stores targeted were in areas predominately made up of Black and Hispanic residents.[7] Following 18th century lantern laws, requiring enslaved individuals to carry lanterns after dark, and modern tactics of following Black people around stores waiting for them to steal, facial recognition is becoming the new form of discriminatory surveillance of Black people.[8] The technology can also be misused to block entry of individuals into businesses altogether on the basis of protected classifications. Jacksons Food Stores, for example, is currently facing a lawsuit for the use of facial recognition in blocking entry to customers in the name of theft prevention.[9] As a customer approaches the store, an automated voice instructs them to look up at the camera.[10] A picture is then taken and scanned in reference to those who may have been previously banned from the store before allowing them in.[11] Given the biased nature of facial recognition technology, uses such as this will only continue to criminalize minorities for actions they did not commit. This not only creates an endless cycle in which minorities are being surveilled and arrested but it also puts them at an increased risk of police violence, irrespective of whether they are correctly identified by a facial recognition system.

[2] Laura Moy, *Facing Injustice: How Face Recognition Technology May Increase the Incidence of Misidentifications and Wrongful Convictions*, 30 WM. & MARY BILL RTS. J. 337, 338-340 (2021); Kashmir Hill & Ryan Mac, *'Thousands of Dollars for Something I Didn't Do'*, N.Y. TIMES (Mar. 31, 2023), https://www.nytimes.com/2023/03/31/technology/facial-recognition-false-arrests.html.

[3] *See* Alex Najibi, *Racial Discrimination in Face Recognition Technology,* HARV. GRADUATE SCH. OF ARTS & SCIS: SPECIAL EDITION ON SCI. POL'Y & SOC. JUST. (Oct. 24, 2020), https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/; Tate Ryan-Mosley & Sam Richards, *Minneapolis Police Used Fake Social Media Profiles to Surveil Black People*, MIT TECH. REV. (Apr. 27, 2022), https://www.technologyreview.com/2022/04/27/1051517/minneapolis-police-racial-bias-fake-social-media-profiles-surveillance/.

[4] Tate Ryan-Mosley, *A New Map of NYC's Cameras Shows More Surveillance in Black and Brown Neighborhoods,* MIT TECH. REV. (Feb. 14, 2022), https://www.technologyreview.com/2022/02/14/1045333/map-nyc-cameras-surveillance-bias-facial-recognition/.

[5] *Juvenile Arrest Rate Trends*, OFF. OF JUV. JUST. & DELINQ. PREVENTION: STAT. BRIEFING BOOK (2020), https://www.ojjdp.gov/ojstatbb/crime/JAR_Display.asp?ID=qa05260&selOffenses=1.

[6] Jeffrey Dastin, *Rite Aid Deployed Facial Recognition Systems in Hundreds of U.S. Stores,* REUTERS (July 28, 2020), https://www.reuters.com/investigates/special-report/usa-riteaid-software/.

[7] *Id.*

[8] Najibi, *supra* note 4.

[9] Brett Dworski, *Jacksons Food Stores Facing Lawsuit over Facial Recognition Technology*, C-STORE DIVE (Jan. 6, 2023), https://www.cstoredive.com/news/jacksons-food-stores-lawsuit-facial-recognition-technology/639816/.

[10] Michael Spears, *'Look at Camera for Entry': Tacoma Convenience Store Using Facial Recognition Technology*, KIRO 7 (May 21, 2019), https://www.kiro7.com/news/south-sound-news/tacoma-convenience-store-uses-facial-recognition-technology/950979811/.

[11] Dworski, *supra* note 10.

S6656 / A2621 further allows for a one-time act of convenience to become an inescapable lifetime security concern. Unlike a password that can be updated, biometric data, including information on facial features and fingerprints, is static and cannot be changed after the fact. This not only makes the data attractive to hackers, as they can use it to access unauthorized computer systems, but it also puts consumers at risk of identity theft for the rest of their lives.[12] Compromised data may additionally prevent consumers from gaining access to services and benefits in their name because their identity cannot be verified.[13] Although S6656 / A2621 requires information collected from biometric technology to be stored in an encrypted database,[14] New York State simply does not have the oversight needed to protect consumer data.[15] Furthermore, the state agencies authorized by the bill to promulgate regulations governing the biometric information collected do not have sufficient technical expertise in cybersecurity to ensure the safety of New Yorkers' personal data.[16] Private vendors and corporations continue to maintain the upper hand as they know and store more information about consumers than ever before[17] and participate in deceptive practices that put that information at risk.[18]

S6656 / A2621 won't cut down on underage drinking and tobacco use. Facial recognition is unlikely to address the problem of underage purchases and may actually make it worse. As previously noted, facial recognition technology is extremely inaccurate and is particularly ineffective at verifying ages.[19] For example, children can unlock their parents' cell phones using facial recognition.[20] The bill itself recognizes this defect, however, it chooses to protect businesses by allowing them to use the technology as a defense for selling to minors. As a result, it is likely that minors will be able to fool automated systems into matching a parent or relative in the database and thereby gain access to alcohol or cigarettes more easily than by the use of a modern, scannable ID card.

[12] *See Is Your Identity at Risk from Biometric Data Collection?*, BEYONDTRUST (Mar. 21, 2019), https://www.beyondtrust.com/blog/entry/is-your-identity-at-risk-from-biometric-data-collection.

[13] *See* Amos Toh & Lena Simet, *Facial Recognition Problems Denying US Workers Unemployment Lifeline*, HUM. RTS. WATCH (June 25, 2021) https://www.hrw.org/news/2021/06/25/facial-recognition-problems-denying-us-workers-unemployment-lifeline (a woman's unemployment claim was denied as facial recognition could not verify her identity and flagged her application as fraud).

[14] S6656 (2023); A2621 (2023).

[15] *See* Juan Miguel & Daniel Schwarz, *NY Is Ignoring the Ban on Facial Recognition in Schools*, NYCLU (June 28, 2022), https://www.nyclu.org/en/news/ny-ignoring-ban-facial-recognition-schools.

[16] *See* S6656 (2023); A2621 (2023).

[17] *Total Data Volume Worldwide 2010-2025*, STATISTA (last visited July 24, 2023), https://www.statista.com/statistics/871513/worldwide-data-created/; Michael Cooney, *Cisco Predicts Nearly 5 Zettabytes of IP Traffic Per Year by 2022*, NETWORK WORLD (Nov. 28, 2018), https://www.networkworld.com/article/3323063/cisco-predicts-nearly-5-zettabytes-of-ip-traffic-per-year-by-2022.html.

[18] *See* Jonathan Grieg, *Clearview AI Fined $20 million, Banned from Processing Biometric Data in Greece After GDPR Violations,* RECORD (July 13, 2022), https://therecord.media/clearview-ai-fined-20-million-banned-from-processing-biometric-data-in-greece-after-gdpr-violations/; Natasha Lomas, *Italy Fines Clearview AI €20M and Orders Data Deleted*, TECHCRUNCH (Mar. 9, 2022, 9:06 AM), https://techcrunch.com/2022/03/09/clearview-italy-gdpr/.

[19] Emma Lindmark, *The Feasibility of Face Scanning as an Age Verification Tool from a Technical- and UX-Perspective*, UPPSALA UNIVERSITY DIV. OF VISUAL INFO. & INTERACTION (2021).

[20] James Peckham, *This 10-Year-Old Unlocked His Mother's iPhone X Using Face ID,* TechRadar (Dec. 3, 2021), https://www.techradar.com/news/this-10-year-old-unlocked-his-mothers-iphone-x-using-face-id.

S6656 / A2621 is a harmful "solution" in search of a problem. Modern IDs work, but facial recognition does not. Proponents of the bill argue that individuals will have the choice to use biometrics; however, any real choice in the matter is in the hands of businesses, not consumers. Nothing in the bill prevents businesses from requiring identity verification using facial recognition in place of government-issued IDs. On the contrary, the bill allows for the results of the biometric technology to defeat physical forms of identification. This ultimately forces customers to carry the burden and face the consequences of inaccurate results and allows for scenarios in which those legally authorized to purchase alcohol and tobacco are wrongfully denied services and subject to criminalization. And, on the flipside, it protects businesses that choose to use racist and inaccurate technology when they inevitably profit from selling alcohol and tobacco products to minors.

S6656 / A2621 is an expansion of New York's surveillance toolkit that risks our sensitive data and further criminalizes marginalized communities. We ask you to oppose the bill and take a stand against facial recognition, a broken technology that threatens our privacy, security, and constitutional rights.

Thank you for your consideration of our concerns.

Sincerely,

Surveillance Technology Oversight Project