SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

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

# MEMORANDUM

**Date:** August 3, 2023
**To:** New York State Senate Internet and Technology Committee, New York State Assembly Consumer Affairs and Protection 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 A2357 / S4850**

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 A2357 / S4850, legislation that would destroy private internet access and erode civil liberties online. Lawmakers are right to be concerned about online scams, but this bill fails to mitigate fraud and would only harm ordinary New Yorkers.

The bill requires all "Email Service Providers" to collect sensitive identifying information about new users before permitting them to sign up for an email account,[1] without exception. This mandate would restrict email access, a service vital for employment, housing, and communication, to those able and willing to provide personal identification.

Many New Yorkers do not have a government-issued identification card due to legitimate concerns about national immigration enforcement, the cost of an ID, or because they are young enough that a government issued ID is not necessary. People without access to an ID card are often low-income, young, and people of color,[2] so A2357 / S4850 would cut these people off from vital online services. Several aspects of modern life are dependent upon email access. For example, email is typically used to set up online banking. New Yorkers cut off from email will struggle to secure employment, because many job applications require an email account. The same is true for applications for housing. New Yorkers' online communication with healthcare professionals and therapists could also be impacted by revoking email access. Gating this necessary service behind an authentication requirement would condemn large swathes of New Yorkers to second-class citizenship.

---

[1] A2357 (2023); S4850 (2023)

[2] Michael J. Hanmer and Samuel B. Novey, CTR. FOR DEMOCRACY AND CIVIC ENGAGEMENT, *Who Lacked Photo ID in 2020?* (Mar. 13, 2023), https://www.voteriders.org/wp-content/uploads/2023/04/CDCE_VoteRiders_ANES2020Report_Spring2023.pdf

By leaving the details of the authentication process up to providers, the bill also opens the possibility of biometric identification as a supplement or substitute to ID card verification. First, the mere collection of biometric data is problematic. Facial images, fingerprints, and other biometric data collected for the purpose of email account verification could later be reused by companies and governments for other purposes. Similarly, forcing email users to provide biometric data to private companies would expose New Yorkers to the risk that their biometric data is compromised.

Second, the use of biometrics for authentication is also concerning. Facial recognition systems generate incorrect matches, which would result in unnecessary police interactions.[3] In this case, incorrect matches could bar innocent New Yorkers from access to email. Because biometric systems are trained on skewed data, they often reinforce existing structural inequalities. As a result, these systems struggle to handle transgender and nonbinary individuals[4] and communities of color.[5] The same commercial facial recognition systems were shown to be wrong nearly one-third of the time for women classified as darker-skinned, but less than 1% for lighter-skinned men.[6] Thus, these communities are especially likely to be incorrectly barred from access to email. The fear of such mismatches would also discourage email use among these marginalized populations that are already unfairly targeted by law enforcement.

Perhaps even more importantly, New Yorkers have legitimate reasons to prefer anonymity. The United States has a long tradition of anonymous speech, going back to the Federalist Papers,[7] published by Alexander Hamilton, John Jay, and James Madison before America even adopted its constitution. Anonymity protects speakers from reprisal and backlash and is essential to preserve political liberty, particularly online. For example, in 2015, the Oregon Justice Department's criminal justice division was caught surveilling users of #BlackLivesMatter, including the leader of the department's civil rights division.[8] In cases like this, anonymity would have guarded against government data collection.

---

[3] *See* Clare Garvie, GEO. L. CTR. ON PRIVACY AND TECH., *Garbage In, Garbage Out: Face Recognition on Flawed Data* (May 16, 2019), https://www.flawedfacedata.com.

[4] Rachel Mentz, *AI Software Defines People as Male or Female. That's a Problem*, CNN BUSINESS, Nov. 21, 2019, https://www.cnn.com/2019/11/21/tech/ai-gender-recognition-problem/index.html.

[5] *See, e.g.,* PATRICK GROTHER ET AL., FACE RECOGNITION VENDOR TEST PART 3: DEMOGRAPHIC EFFECTS 2 (Dec. 2019).

[6] Joy Buolamwini, Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Proceeds of Machine Learning Research*, vol. 81, 1-15, 2018 p. 1.

[7] *See, e.g.,* THE FEDERALIST No. 1 (Alexander Hamilton).

[8] *See* Denis C. Theriault, *Black Lives Matter: Oregon Justice Department Searched Social Media Hashtags*, OREGONIAN, Nov. 10, 2015, https://www.oregonlive.com/politics/2015/11/black_lives_matter_oregon_just.html.

The proposed legislation would also limit whistleblower anonymity, making New Yorkers more vulnerable to other forms of corporate fraud and abuse. Employee whistleblowing is the most effective way to identify fraud, outperforming audits.[9] Two-thirds of whistleblowers experience retaliation, which can pose lifelong personal and professional consequences.[10] By eliminating email anonymity, this legislation would make it much easier for corporations and government agencies to retaliate against whistleblowers, greatly discouraging them from coming forward in the first place.

This legislation's harms are not limited to high-profile cases of activism. Ending access to anonymous online speech would impact every New Yorker. Anonymous email enables undocumented New Yorkers to communicate honestly about work conditions and legal issues without the fear of employer or government retaliation. For Muslim New Yorkers and others disproportionately impacted by police surveillance, anonymity guards against government overreach and protects personal privacy.[11] For people seeking abortion care or gender-affirming care, anonymous email is an important tool for securing medical care and communicating about their medical needs. Finally, anonymous email is also a safeguard for those who are common targets of police misconduct, such as New Yorkers engaged in sex work.[12]

While legislators are justifiably interested in building a better internet,[13] this legislation will do little to address internet fraud. This bill only regulates email inside of New York, but internet fraud typically originates outside the state or abroad.[14] Requiring New Yorkers to surrender their personal information would do nothing to stop misleading email sent from outside of the state. Even worse, this legislation may actually increase online fraud by exposing New Yorkers to a greater risk of identity theft after a provider data breach.

Instead of limiting New Yorkers' access to anonymous communication online, we recommend legislation that would promote cybersecurity education and fraud awareness, particularly among

---

[9] *See* Tanya M. Marcum & Jacob Young, *Blowing the Whistle in the Digital Age: Are You Really Anonymous? The Perils and Pitfalls of Anonymity in Whistleblowing Law*, 17 DePaul Bus. & Comm. L.J. 1, 2 (2019).

[10] *See Id.* at 3-4.

[11] *See* Mazin Sidahmed, *NYPD's Muslim Surveillance Violated Regulations as Recently as 2015: Report*, THE GUARDIAN, Aug. 24, 2016, https://www.theguardian.com/us-news/2016/aug/24/nypd-muslims-surveillance-violations.

[12] *See* Joshua Kaplan & Joaquin Sapien, *NYPD Cops Cash in on Sex Trade Arrests With Little Evidence, While Black and Brown New Yorkers Pay the Price*, PROPUBLICA, Dec. 7, 2020, https://www.propublica.org/article/nypd-cops-cash-in-on-sex-trade-arrests-with-little-evidence-while-black-and-brown-new-yorkers-pay-the-price.

[13] *See* Clyde Vanel, *KTS Email Bill (Know the Sender)*, YOUTUBE (Jan. 11, 2022), https://www.youtube.com/watch?app=desktop&v=pOs8Zv1Zyag.

[14] *See* Yudhijit Bhattacharjee, *Who's Making All Those Scam Calls?* N.Y. TIMES, Apr. 21, 2021, https://www.nytimes.com/2021/01/27/magazine/scam-call-centers.html.

SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

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

communities most at risk of internet-based fraud. We should not allow online scammers to take advantage of our community, but A2357 / S4850 will not further that goal. Protecting New Yorkers online does not need to come at the cost of their civil liberties. Thank you for your consideration of our concerns.

Sincerely,

Surveillance Technology Oversight Project