ACLU of New York

Legislative Affairs
One Whitehall Street
New York, NY 10004
212-607-3300
www.nyclu.org

Testimony of Daniel Schwarz

On Behalf of the New York Civil Liberties Union

Before the New York City Council Committee on Technology

Regarding a Study on a Digital Identification Program Pilot

September 24, 2021

The New York Civil Liberties Union ("NYCLU") respectfully submits the following testimony regarding the proposed legislation to create a study and report on a digital identification program pilot. The NYCLU, the New York affiliate of the American Civil Liberties Union, is a not-for-profit, non-partisan organization with eight offices throughout the state and more than 180,000 members and supporters. The NYCLU's mission is to defend and promote the fundamental principles, rights, and values embodied in the Bill of Rights, the U.S. Constitution, and the Constitution of the State of New York. The NYCLU works to expand the right to privacy, increase the control individuals have over their personal information, and ensure civil liberties are enhanced rather than compromised by technological innovation.

While a carefully implemented and nuanced digital identification system may prove worthwhile and beneficial, if done improperly it could have far-reaching ramifications, entrench injustice, erode privacy rights, and threaten our civil rights and liberties. Intro. 2305 risks the latter by creating a pathway for new tracking capabilities without setting the necessary guardrails and oversight.

We have significant concerns about the digital identification program pilot study, as laid out in Intro. 2305, and oppose the legislation in its current form. As currently drafted, a mayor-designated city agency would work in partnership with a financial institution on a digital ID feasibility study and report. Mandating a fin-tech vendor to be the sole partner is problematic at best. To succeed, the focus must be squarely on equity and privacy, not a company's bottom line. Appropriate partners would be experts in cryptography and cyber-security, open-source technology, immigrants' rights, civil rights, and accessibility; and, most importantly, representatives from the communities most affected by such a program, especially those receiving public assistance.

Further, any digital identification program must be entirely voluntary, require opt-in consent, offer granular control over one's data, and ensure strong privacy protections – guaranteed both by legal and technical safeguards.

But the technology is not ready yet: open standards[1] development is still in process and the City should not fall for proprietary tech developed behind closed doors, forcing costly vendor lock-ins – as experienced in the past. Transparent and auditable open standards are the only meaningful path to ensure trust and security.

Unfortunately, throughout the pandemic, opaque, exploitative, and discriminatory technologies were deployed for digital identity verification. 21 states have procured a facial recognition tool for unemployment insurance processing.[2] The New York Department of Labor is one of them, thereby creating new barriers for people to receive their benefits by requiring the provision of their biometric data to third-party companies and risking misidentification through a technology that has repeatedly been shown to have significantly higher error rates for women and people of color. It is incumbent on the Council to not repeat these mistakes and ensure such technologies have no place in our city.

As the *Identity Crisis* report[3] in the appendix further details, we strongly urge to not move forward with any digital ID system unless the following key principles are adhered to:

- *Community Inclusion*. Impacted people need to have a seat at the table from the start. Communities most affected and those receiving public assistance must be represented and meaningfully involved. Consult with experts in digital identification, cryptography and cyber-security, open-source technology, immigrant's rights, civil rights, and accessibility.
- *Equitable Tech*. Ensure technologies serve people and communities in need, not companies' shareholders.
- *Voluntary and Opt-In Consent*. Any digital ID program must be fully voluntary and require opt-in consent. The use of digital IDs should never become mandatory or be required to access certain services.

---

[1] *See*, e.g.: Verifiable Credentials Data Model 1.0, WORLD WIDE WEB CONSORTIUM (W3C) (2019), https://www.w3.org/TR/vc-data-model/ (last visited Sep 23, 2021).

[2] *See*, e.g.: Dave Gershgorn, *21 States Are Now Vetting Unemployment Claims With a 'Risky' Facial Recognition System*, ONEZERO (2021), https://onezero.medium.com/21-states-are-now-vetting-unemployment-claims-with-a-risky-facial-recognition-system-85c9ad882b60 (last visited Sep 23, 2021); and Michele Gilman & Mary Madden, *Digital Barriers to Economic Justice in the Wake of COVID-19*, DATA & SOCIETY (2021), https://datasociety.net/library/digital-barriers-to-economic-justice-in-the-wake-of-covid-19/ (last visited Sep 23, 2021).

[3] Jay Stanley, *Identity Crisis: What Digital Driver's Licenses Could Mean for Privacy, Equity, and Freedom*, AMERICAN CIVIL LIBERTIES UNION (2021), https://www.aclu.org/report/identity-crisis-what-digital-drivers-licenses-could-mean-privacy-equity-and-freedom (last visited Sep 23, 2021).

- *Encryption and Security Standards*. The system must be built with the strongest possible encryption and security standards.
- *No Police Officer Access to Phones*. System should be designed that ID owners never need to hand over their device to a verifier.
- *Unlinkable Presentations*. The system should be designed to prevent any creation of records of where and when an ID was presented.
- *Granular control over data released*. The system must be designed to give people comprehensive controls over what data is released. It should also allow for broad categories to be disclosed and therefore follow data minimization principles (e.g., over 21; over 65; NYC resident).
- *Restrictions on ID Demands*. The system should not create additional ID checks where none was needed before.
- *Open Source and Open Standards*. Avoid proprietary solutions, vendor lock-ins, and long-term dependencies. Adopt initiatives like "Public Money, Public Code," which requires publicly financed software developed for public use to share its source code. Standard, interoperable protocols are also more secure and better tested.
- *Ban Discriminatory Technologies*. Enact bans on technologies that show discriminatory impact or threaten people's fundamental rights.
- *Auditing and Reviewing Mechanisms*. All systems should be subject to independent, transparent review to ensure – and to assure the public – that such technologies are being used appropriately and treating personal information with the care required.

In conclusion, the NYCLU thanks the Committee for the opportunity to provide testimony. We urge the Committee not to rush the digital ID infrastructure prematurely. Without the necessary precautions, it would supercharge surveillance and lock people out from much needed city services. Any steps towards a digital identity system must center equity and privacy protections from the very beginning – and for this it matters who sits at the table and what values undergird the endeavor.