



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

2025 Memorandum

Subject: Protect Privacy and Guard Against Surveillance

A second Trump administration threatens to exploit dangerous and invasive technologies to undermine our rights and freedoms by supercharging his stated goals of mass deportations, policing, and militarization.¹ During Trump’s first administration, he instructed governors to deploy the National Guard to “dominate the streets”² and Customs and Border Protection deployed officers and drones to at least 18 cities in response to racial justice protests, including Buffalo. However, the technologies accessible and deployable far exceed the use of drones. Big Brother surveillance programs like Section 702 of the Foreign Intelligence Surveillance Act (FISA)³ and Executive Order 12333 result in mass collection of our private data. These and the government’s purchase of massive quantities of data from commercial data brokers enable the federal government to search our private communications, movements, and sensitive information without a warrant and without meaningful safeguards necessary to protect our rights. It is all too easy to foresee Trump using these overbroad and dangerous spying powers to surveil and discriminate against political opponents and people and communities in his crosshairs — protestors, communities of color, immigrants, and people seeking abortions or gender-affirming care.

Our privacy and civil liberties remain at risk unless and until the state legislature passes necessary protections to catch up with 21st century technologies. New York must pass the **Digital Fairness Act (DFA)**⁴ to provide comprehensive privacy protections, empower

¹ Project 2025 explicitly calls for even more data collection and sharing, through government entities and private data brokers alike, with the stated goal of “total information-sharing in the context of both federal law enforcement and immigration enforcement,” particularly to obtain information about immigrants in sanctuary jurisdictions including through direct “access to department of motor vehicles and voter registration databases.” The Heritage Foundation, *Mandate for Leadership: The Conservative Promise* (2024). Similarly, Project Esther provides a dangerous roadmap for the surveillance and punishment of any pro-Palestinian speech, targeting protestors, students and educators on campus, and free speech at large. National Task Force to Combat Antisemitism, *Project Esther: A National Strategy to Combat Antisemitism* (2024).

² *Trump suggests governors call in National Guard to ‘dominate the streets’*, REUTERS, Jun. 6, 2020, <https://www.reuters.com/article/world/trump-suggests-governors-call-in-national-guard-to-dominate-the-streets-idUSKBN23D08L/>.

³ See, e.g., Noah Chauvin & Elizabeth Goitein, *What’s Next for Reforming Section 702 of the Foreign Intelligence Surveillance Act*, Brennan Center, Feb. 2, 2024, <https://www.brennancenter.org/our-work/research-reports/whats-next-reforming-section-702-foreign-intelligence-surveillance-act> (describing Section 702 and noting that “[d]eclassified documents have revealed that officials have performed baseless backdoor searches for the private communications of racial justice protestors, members of Congress, journalists, crime victims, and political donors, among many others”).

⁴ S.2277-Kavanaugh/A-3308 Cruz in the 2023-24 legislative session.

people to have meaningful control over their data, protect against invasive or exploitative practices, and ensure algorithms do not undermine anti-discrimination laws. The Heritage Foundation's policy book also seeks to eliminate crucial anti-discrimination-related data collection under the Equal Employment Opportunity Commission, underscoring the urgent need to pass the **Bosware and Oppressive Technology Act**,⁵ which would establish worker privacy and employment protections for modern day technologies in the workplace. Lawmakers must also create **robust safeguards for Digital IDs** which began piloting in New York in 2024 and have far-reaching ramifications for how people will provide proof of identity, as well as the troubling potential for an expansion of the government's ability to monitor and track their interactions and movements.⁶

We must also restrict the use of invasive and biased law enforcement technologies. Chief among these is facial recognition, notoriously inaccurate for Black and Brown people, women and non-binary people, young people and old people. The legislature must **ban biometric surveillance**,⁷ which presents a clear danger to all New Yorkers' civil liberties and threatens to erode our fundamental rights to privacy, protest, and equal treatment. We need to **curtail technologies such as license plate readers** by significantly limiting when they can be utilized, reducing the amount of time that collected data may be retained, and ensuring no data is shared outside of New York. Lawmakers must also **regulate police drones** by prohibiting drone surveillance of protests and other activities protected by the First Amendment, require search warrants for their use in police investigations, and prohibit drones from using facial recognition software, weapons, or crowd control devices.⁸

In addition, lawmakers must update our warrant protections to be in line with technological advancements by passing the **Electronic Communications Privacy Act**⁹ and by **prohibiting the use of reverse location and keyword searches and warrants**.¹⁰ Our participation in digital life should not automatically result in the dystopian threat of pervasive police spying, and communities-at-risk from the Trump administration's threats should not be exposed to harm from their personal devices.

Finally, New York State must stop partnering with federal authorities to conduct abusive surveillance operations by terminating state and federal data sharing arrangements, and ending or sharply curtailing our participation in joint federal, state, and local task forces and fusion centers. The New York State Intelligence Center and other Crime Analysis Centers¹¹ have for too long operated and wielded their immense surveillance powers in darkness; it is time to clamp down on these thus-far unaccountable entities and create the public oversight and restrictions New Yorkers need and deserve.

⁵ S.7623-B Hoylman/A.9315-A Alvarez in the 2023-24 legislative session.

⁶ See Donna Lieberman & Cynthia Conti-Cook, *Want the Government to Track Your Every Move? Mobile ID May Be for You*, NYCLU, Aug. 2, 2024, <https://www.nyclu.org/commentary/want-the-government-to-track-your-every-move-mobile-id-may-be-for-you>.

⁷ S.1609-Hoylman/A.1891-Glick in the 2023-24 legislative session.

⁸ See NYCLU, *Prying Eyes: Government Drone Data Across New York State* (2022), <https://www.nyclu.org/report/prying-eyes-government-drone-data-across-new-york-state>.

⁹ A.1880-Dinowitz/S.2615-Parker in the 2023-24 legislative session.

¹⁰ S.217-Myrie/A.3306-Solages in the 2023-24 legislative session.

¹¹ Fusion Centers like the New York State Intelligence Center that tap into enormous surveillance databases and a vast arsenal of technologies such as license plate readers, drones, biometric surveillance, social media surveillance, and many others provide a core—and largely opaque—infrastructure for these aggressive efforts.