



**Testimony by Director of Research and Policy
Cynthia Conti-Cook of the
Collaborative Research Center for Resilience**

**To the Committee on Technology of the
New York City Council
Chair Carmen de la Rosa**

**On March 2, 2026
Regarding Why New York Communities Need
Limitations on the Growth of
Biometric Collection and Recognition Technologies**

Submitted Written Testimony on March 4, 2026



The Collaborative Research Center for Resilience (CRCR) is focused on ensuring that government use of technology to access public goods, such as municipal identity or education, do not undermine democracy. We investigate and conduct community-centered action research to support key interested and affected groups who are often left in the dark (e.g., workers, impacted community members, elected officials). We do so with the intention to elevate meaningful participation in governance across areas with profound impact on our daily lives.

We testify in general support of both Introductions 428 and 213 limiting biometric recognition technology. However, we also urge the Council to expand such limitations to ban biometric collection technology in addition to recognition technology. We also encourage all reporting and use limitations to apply equally to all agencies, including police. We urge the Council to consider not just the direct harms of surveillance policing but to thoroughly also explore the foreseeable community harms, as described in further detail below. This includes the potential for taxpayers to pay three times for the harms created by new technologies: for the harm; to compensate for the harm; and for the vendors' overpriced harmful service.

In addition to the harms to individuals and communities that result from surveillance policing, we must also look ahead to the harms of surveillance pricing. While the biometric industry claims that safety and security is their mission, biometric collection infrastructure is the foundation required for surveillance pricing. Surveillance (or euphemistically “dynamic”) pricing is when the cost of goods changes based on the customer profile of each person who walks in. It predicts what they might buy again, for example if it is an allergy-safe product or favorite brand that the customer has a pattern of buying. The prices are then set according to the real-time prediction for that customer. Perhaps on a hot summer day, for example, someone who is lactose intolerant may pay a premium price for an allergy-safe ice cream.¹

Surveillance pricing relies on identification technology infrastructure—and biometric collection and recognition technologies are a key component. Identity technologies include digital drivers licenses, passports, digital wallets, and age verification technologies. The future capacity to integrate biometrics and other identity technologies with other information gathering technologies powered by AI is exactly the type of future use case industry associations brag about in front of government buyers—surveillance pricing but for police. Instead of changing a price, a police tool might have a dynamic “risk” score that lets them “click and frisk” to see more details about who that person is, where they work, and what kind of basis an officer might have to engage them.² Therefore the community harms we must consider are not just present day uses of biometrics for security but for identity technology infrastructure as a whole. Where else can we have this conversation when so many of these decisions are being made in budgets and pilot projects with little public oversight or reporting?

¹ Press Release, UFCW, UFCW Launches National Campaign to Ban Surveillance Pricing on Groceries (Feb. 12, 2026), <https://www.ufcw.org/press-releases/ban-surveillance-pricing-on-groceries/>; Jay Stanley, “*Surveillance Pricing*” Hurts Consumers, Incentivizes More Corporate Spying on Them, ACLU (Sep. 12, 2025), <https://www.aclu.org/news/privacy-technology/surveillance-pricing>.

² See The Net, <https://thecrcr.org/wp-content/uploads/MovieNight-the-Net-V20.pdf>



Community harms also include what we collectively lose—control over our creativity and cohesion. The enhanced capacity of corporations to extract fragments of our content, to collect our biological information from us—from our recordings, images, voices, and text—and create something they then sell back to us (or worse, blackmail us with) also foreseeably harms us all. Granting these systems access to our biometrics empowers AI bots with an even richer set of tools with which to continue plundering our identities, our creativity, and our community. Look what they did to the entirety of information we’ve already granted them access to over the past few decades of social media — why would we believe our biometrics will be more carefully treated than any other content that has been exploited when shared?

The AI-bot-ification of social media has made it impossible to know who is real and who is an avatar—the ingredients of each avatar being disassembled pieces of ourselves. While agentic AI is wreaking havoc on social media platforms, snatching identifying information, and blackmailing us with deep fakes, we must at the very least have a moratorium on all government procurement of biometric collection and recognition technology, a comprehensive assessment of the potential harms incoming through identity technology infrastructure in the commercial and government sectors, place more expansive limitations on insurance policies that pressure businesses to install biometric technologies and restrain biometric data collection.

There are so many ways that businesses are accessing data through sales but also through mergers and acquisitions—the prohibitions on sale of biometric data must also understand the various forms of investment, corporate maneuvering, and market capture that technology companies engage in to seize control of data assets. Public sector data is a hot commodity because it holds the keys to creating tools that governments might buy. Long-term sole-source government contracts guarantee years of predictable work and leverage over future contracts. This political economy of the technology sector cornering government marketplaces must be analyzed alongside complex forms of public procurement that also impact what companies can access sensitive personal identifying information, including biometrics, by virtue of being a public sector vendor (or parent company).

It is this level of concern we ask the City Council to consider here. We look forward to working together to understand the implications of this digital public infrastructure and protect our democracy and communities.

Collection of Biometric Data Increases Surveillance of New Yorkers

Biometric recognition and collection technology, deployed in tandem with other surveillance technology like artificial intelligence (AI), enables corporations and the government to easily track and control the behavior of Americans as they shop at the grocery store, post on social media, and other ordinary, daily real life and digital activities. The previous mayoral administration, for example, proposed using digital wallets to modify eating behavior of benefits recipients.³

³ Nicholas Liu, *How the Adams Administration is Thinking About Blockchain and Cryptocurrency*, Gotham Gazette (Mar. 17, 2023), <https://www.gothamgazette.com/city/11883-city-council-mayor-adams-blockchain-cryptocurrency/>



The proliferation of AI happening at the same time as the scaling of biometric identity technologies by small businesses and landlords should cause caution given the well publicized problems associated with their deployment, including false matches leading to wrongful arrests⁴ or unjust exclusion from businesses,⁵ the lack of reliability in its ability to accurately identify people of color,⁶ and its dubious compliance with constitutionally protected rights such as due process.⁷ Despite the uptick in the usage of these invasive technologies, Congress has not passed any legislation regulating these types of invasive technologies.⁸ Some states and cities have attempted to fill this regulation gap by passing moratoriums or bans on the use of facial recognition technology by police because of the foreseeable harms it introduces to communities.⁹

Law enforcement agencies use this technology to surveil and target immigrants,¹⁰ protesters,¹¹ public housing residents,¹² legal observers,¹³ and the broader community at large. However, limiting the usage of this technology only for police does not protect communities from the harms associated with surveillance

⁴ Crystal Cranmore, *Man's Wrongful Arrest Puts NYPD's Use of Facial Recognition Tech Under Scrutiny*, ABC 7 (Aug. 27, 2025), <https://abc7ny.com/post/man-falsely-jailed-nypds-facial-recognition-surveillance-tech-failed/17664671/>; *Woman Wrongly Accused of Carjacking Loses Lawsuit Against Detroit Police Who Used Facial Technology*, CBS NEWS (Sep. 4, 2025), <https://www.cbsnews.com/detroit/news/woman-wrongly-accused-carjacking-loses-lawsuit-detroit-police-used-facial-tech/>.

⁵ Jay Stanley, *Retailers Secretively Using Face Recognition to Spot "Persons of Interest" — Including For the Government*, ACLU (Jan. 20, 2026), <https://www.aclu.org/news/privacy-technology/retailers-secretively-using-face-recognition>.

⁶ U.S. COMMISSION ON CIVIL RIGHTS, *THE CIVIL RIGHTS IMPLICATIONS OF THE FEDERAL USE OF FACIAL RECOGNITION TECHNOLOGY* 3 (Sep. 2024), https://www.usccr.gov/files/2024-09/civil-rights-implications-of-frt_0.pdf.

⁷ *Civil Rights Concerns Regarding Law Enforcement Use of Face Recognition Technology*, NEW AMERICA, June 3, 2021, https://www.newamerica.org/oti/briefs/civil-rights-concerns-regarding-law-enforcement-use-of-face-recognition-technology/?utm_source=chatgpt.com.

⁸ Amy B. Cyphert, *Confronting the Challenges of Regulating Artificial Intelligence*, 20 FIU L. REV. 82, 85 (2025), <https://ecollections.law.fiu.edu/cgi/viewcontent.cgi?article=1741&context=lawreview>; Bobby Allyn, *With No Federal Facial Recognition Law, States Rush to Fill Void*, NPR (Aug. 28, 2025), <https://www.npr.org/2025/08/28/nx-s1-5519756/biometrics-facial-recognition-laws-privacy>.

⁹ Jake Laperruque, *Status of State Laws on Facial Recognition Surveillance: Continued Progress and Smart Innovations*, TECH POLICY PRESS (Jan. 6, 2025), <https://www.techpolicy.press/status-of-state-laws-on-facial-recognition-surveillance-continued-progress-and-smart-innovations/>.

¹⁰ Jude Joffe-Block, *Immigration Agents Have New Technology to Identify and Track People*, NPR (Nov. 8, 2025), <https://www.npr.org/2025/11/08/nx-s1-5585691/ice-facial-recognition-immigration-tracking-spyware>.

¹¹ Sheera Frenkel & Aaron Krolik, *How ICE Already Knows Who Minneapolis Protestors Are*, NY TIMES (Jan. 30, 2026), <https://www.nytimes.com/2026/01/30/technology/tech-ice-facial-recognition-palantir.html>.

¹² Zachary Groz, *Five Unanswered Questions About Eric Adams's Expanded Surveillance at NYC Public Housing*, NEW YORK FOCUS (Aug. 12, 2025), <https://nysfocus.com/2025/08/12/unanswered-questions-adams-surveillance-big-apple-connect>.

¹³ Alfred Ng, *DHS Accused of Using Surveillance Tech to Track Legal Observers in Maine*, POLITICO (Feb. 23, 2026), <https://www.politico.com/news/2026/02/23/dhs-accused-of-using-surveillance-tech-to-track-legal-observers-in-maine-00792722>.



technology. For example, corporations like Wegmans¹⁴ and Madison Square Garden¹⁵ employ this technology on New Yorkers as they grocery shop and attend concerts.

If corporations are permitted to collect this kind of sensitive data, law enforcement agencies can issue demands to gain access, undermining local bans on the use of facial recognition technology by police.¹⁶ It is widely reported that the Department of Homeland Security (DHS) has done just that—purchasing personal data collected by private companies, circumventing the Fourth Amendment’s requirement to get a warrant before searching private information.¹⁷ Thus, the collection of biometric data of consumers by private corporations expands the government’s ability to surveil and micro-target vulnerable communities.

Corporations can also use this data themselves to target certain consumers for higher prices¹⁸ and wrongfully refuse admission to their businesses.¹⁹ Given the federal government’s embrace and expanded use of these technologies,²⁰ it is imperative that local governments like New York City step in to protect city communities from foreseeable harm and large scale liability.

¹⁴ Tim McNicholas, *Some Wegmans Locations, Including 1 in NYC, are Now Using Facial Recognition Software on Customers. Here’s Why.*, CBS NEWS (Jan. 5, 2026), <https://www.cbsnews.com/newyork/news/wegmans-facial-recognition-software-new-york-city/>.

¹⁵ Kashmir Hill & Corey Kilgannon, *Madison Square Garden Uses Facial Recognition to Ban Its Owner’s Enemies*, NY TIMES (Dec. 22, 2022), <https://www.nytimes.com/2022/12/22/nyregion/madison-square-garden-facial-recognition.html>.

¹⁶ Paige Oamek & Andrew Giambrone, *Not Just Wegmans: More NYC Retailers Using Facial Recognition as Tech Outpaces Law*, GOTHAMIST (Jan. 12, 2026), <https://gothamist.com/news/not-just-wegmans-more-nyc-retailers-using-facial-recognition-as-tech-outpaces-law>; Sheera Frenkel, *Lawmakers Ask Tech Companies What User Data They Provided to D.H.S.*, NY TIMES (Feb. 25, 2026), <https://www.nytimes.com/2026/02/25/technology/lawmakers-tech-companies-dhs.html>.

¹⁷ Anika Venkatesh & Lauren Yu, *DHS is Circumventing Constitution by Buying Data It Would Normally Need a Warrant to Access*, ACLU (Jan. 12, 2026), <https://www.aclu.org/news/privacy-technology/dhs-is-circumventing-constitution-by-buying-data-it-would-normally-need-a-warrant-to-access>.

¹⁸ FTC, FTC SURVEILLANCE PRICING 6(B) STUDY: RESEARCH SUMMARIES: A STAFF PERSPECTIVE 1, 5 (Jan. 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/p246202_surveillancepricing6bstudy_researchsummaries_redacted.pdf.

¹⁹ Kashmir Hill & Corey Kilgannon, *Madison Square Garden Uses Facial Recognition to Ban Its Owner’s Enemies*, NY TIMES (Dec. 22, 2022), <https://www.nytimes.com/2022/12/22/nyregion/madison-square-garden-facial-recognition.html>; Press Release, Federal Trade Commission, Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards (Dec. 19, 2023), <https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without>.

²⁰ See, e.g., Anthony Kimery, *Trump Administration Expands Facial Recognition While Erasing Oversight Policy*, BIOMETRICUPDATE.COM (Oct. 31, 2025), https://www.biometricupdate.com/202510/trump-administration-expands-facial-recognition-while-erasing-oversight-policy?utm_source=chatgpt.com; Matt O’Brien, et. al., *Hegseth Warns Anthropic to Let the Military Use the Company’s AI Tech As it Sees Fit, AP Sources Say*, AP (Feb. 24, 2026), <https://apnews.com/article/anthropic-hegseth-ai-pentagon-military-3d86c9296fe953ec0591fcde6a613aba>.



Biometric Collection Aids Surveillance Pricing Which Harms Consumers

The collection of consumer data and advancements in AI technology allow companies to target particular customers and charge them higher prices, a practice called surveillance pricing.²¹ For example, grocery stores who engage in surveillance pricing collect information on consumers to build individualized profiles through various means including data collected from in-store kiosks with interactive touchscreens, virtual storefronts like apps and websites, and location data from IP addresses.²²

Stores also collect biometric data on consumers while shopping in-store.²³ Grocery stores are increasingly using electronic shelf labels which enable them to change prices at any time.²⁴ These digital price tags, combined with the information collected through surveillance pricing tactics, increase the risk that stores will monitor and track shoppers as they move throughout a store, changing prices based on the information they are collecting and storing.²⁵

This also puts retail workers at risk as grocery store clerks would be the ones bearing the brunt of angry customers who notice they are being charged more than other shoppers for the same item.²⁶ Although General Business Law 349-a, the first surveillance pricing law enacted in the country, went into effect last year, it only requires businesses to disclose when their prices are set by algorithms that use the consumer's personal data, not prohibit the actual practice of surveillance pricing.²⁷

As many New Yorkers struggle to make ends meet, companies should not be permitted to surveil the shopping habits of their customers in order to charge unfair prices. The collection of biometric data on consumers when they visit stores gives companies more tools to set individualized prices and expand surveillance pricing systems.

²¹ FTC, FTC SURVEILLANCE PRICING 6(B) STUDY: RESEARCH SUMMARIES: A STAFF PERSPECTIVE 1, 5 (Jan. 2025), https://www.ftc.gov/system/files/ftc_gov/pdf/p246202_surveillancepricing6bstudy_researchsummaries_redacted.pdf.

²² *Id.* at 8–9.

²³ Liam Quigley, *NYC Wegmans Is Storing Biometric Data on Shoppers' Eyes, Voices and Faces*, GOTHAMIST (Jan. 3, 2026), <https://gothamist.com/news/nyc-wegmans-is-storing-biometric-data-on-shoppers-eyes-voices-and-faces>.

²⁴ Press Release, UFCW, UFCW Launches National Campaign to Ban Surveillance Pricing on Groceries (Feb. 12, 2026), <https://www.ufcw.org/press-releases/ban-surveillance-pricing-on-groceries/>; Jay Stanley, “Surveillance Pricing” Hurts Consumers, Incentivizes More Corporate Spying on Them, ACLU (Sep. 12, 2025), <https://www.aclu.org/news/privacy-technology/surveillance-pricing>.

²⁵ See Press Release, UFCW, UFCW Launches National Campaign to Ban Surveillance Pricing on Groceries (Feb. 12, 2026), <https://www.ufcw.org/press-releases/ban-surveillance-pricing-on-groceries/>.

²⁶ *Id.*

²⁷ Press Release, Kathy Hochul, Governor, New York, Protecting New Yorkers From Secret Online Price Hikes: Governor Hochul Announces Nation-leading Surveillance Pricing Law Now in Effect (Nov. 24, 2025), <https://www.governor.ny.gov/news/protecting-new-yorkers-secret-online-price-hikes-governor-hochul-announces-nation-leading>.



Private Biometric Collection Facilitates More Surveillance by Law Enforcement

Companies who build surveillance tools and collect data on Americans regularly sell this information to law enforcement. For example, Clearview AI built a biometric database from images of people it collected on the internet and social media profiles without permission from the websites or individuals in the photos.²⁸

Its AI system created “faceprints” of each person and allows users to search for matches when a “probe photo” runs against its database, identifying the matching faceprint and giving a link to the websites where the matching photo originated.²⁹ Clearview sold its technology, which can be utilized without a search warrant or probable cause, to law enforcement clients and Immigration and Customs Enforcement (ICE).³⁰ Law enforcement have used this technology to target immigrants, activists, and protesters, circumventing privacy and due process requirements.³¹

Clearview also sold its technology to corporations like Macy’s who allegedly used Clearview on its customers.³² When stores are permitted to collect biometric data with their security cameras, there is an increased risk that companies like Clearview could purchase access to these feeds and give this information to their law enforcement clients. This exacerbates the climate of fear for immigrants who are concerned that a trip to a grocery store like Wegmans could lead to their biometric data getting into the hands of ICE.³³ Recently, investors in Home Depot raised concerns that the company is sharing the biometric data it collects of its customers while they shop with ICE, as the agency has conducted many raids in its store parking lots, emphasizing the danger that allowing private actors to collect biometric data can open up our communities to increased policing and displacement.³⁴

Collection of Biometric Data Accelerates Development of Harmful Agentic AI Systems

AI companies are now developing and employing agentic AI tools—and access to biometric identifying data is a key component to how they plan to operate. Unlike generative AI, which uses data sets to create text, images, and video, agentic AI systems are semi or fully autonomous, making decisions and performing tasks with little to no human input or supervision.³⁵ As more companies develop this kind of technology,

²⁸ Luke O’Brien, *The Shocking Far-Right Agenda Behind the Facial Recognition Tech Used by ICE and the FBI*, MOTHER JONES (May & June 2025), <https://www.motherjones.com/politics/2025/04/clearview-ai-immigration-ice-fbi-surveillance-facial-recognition-hoan-ton-that-hal-lambert-trump/>

²⁹ *Id.*

³⁰ *Id.*

³¹ *Id.*

³² *Id.*

³³ Liam Quigley, *NYC Wegmans Is Storing Biometric Data on Shoppers’ Eyes, Voices and Faces*, GOTHAMIST (Jan. 3, 2026), <https://gothamist.com/news/nyc-wegmans-is-storing-biometric-data-on-shoppers-eyes-voices-and-faces>.

³⁴ Arriana McLymore & Ross Kerber, *Amid ICE Raids, Some Home Depot Investors Want to Know How Law Enforcement Uses its Surveillance Data*, REUTERS (Jan. 16, 2026), <https://www.reuters.com/sustainability/boards-policy-regulation/amid-ice-raids-some-home-depot-investors-want-know-how-law-enforcement-uses-its-2026-01-16/>.

³⁵ Beth Stackpole, *Agentic AI, Explained*, IDEAS MADE TO MATTER (Feb. 18, 2026), <https://mitsloan.mit.edu/ideas->



their desire to collect more biometric data will grow as biometric data enables the agents to operate more efficiently.³⁶ Government regulation is needed to counteract this push for more data collection as the harms of agentic AI are already materializing.

For example, banks use AI agents to decide whether to approve or deny a consumer's application for a mortgage.³⁷ These AI agents rely on information outside traditional sources like credit reporting agencies.³⁸ They also base their decisions on data collected from an individual's "digital footprint" to determine an applicant's creditworthiness, much of it collected without the user's awareness.³⁹ AI agents also rely on historical data to make lending decisions which replicate patterns of systemic discrimination and bias, harming Black and Latino applicants.⁴⁰

The rapid development of agentic AI also poses a real threat to displace entry-level jobs.⁴¹ Regulators have struggled to reel in abuses of these kinds of technologies, allowing proliferation with limited guardrails and supervision.⁴² As companies integrate biometric ID collection into these systems, the risk that our biology and identities will become vulnerable to the chaos and unpredictability of agentic AI will grow.

Similarly, people exploit these vulnerabilities by snatching our loved one's likenesses and manufacturing a crisis we respond to out of fear and without thinking. Rather than regulating and preventing the proliferation of chaotic AI and create responsibility within technology companies to prevent AI bots from plundering our information, the biometric industry irresponsibly urges us to upload even more sensitive data to our digital twins.

Lawmakers, trying to catch up when they do attempt to regulate, tend to focus on the current usages of these technologies and miss the trends on how these technologies are developing and the potential future harms associated with evolving technology. For example, AI agents are already reinforcing discriminatory practices and threatening the livelihoods of many Americans with or without access to our biometric data. If we allow companies to collect the biometric data of their customers, we permit them to use this data in

[made-to-matter/agentic-ai-explained.](#)

³⁶ Mohamed Lazzouni, *The Role of Biometric Identity in the Age of Agentic AI*, FORBES (Nov. 21, 2025), <https://www.forbes.com/councils/forbestechcouncil/2025/11/21/the-role-of-biometric-identity-in-the-age-of-agentic-ai/>.

³⁷ Korin Munsterman, *When Algorithms Judge Your Credit: Understanding AI Bias in Lending Decisions*, 17 UNT DALLAS ACCESSIBLE L. (2025), <https://www.accessiblelaw.untDallas.edu/post/when-algorithms-judge-your-credit-understanding-ai-bias-in-lending-decisions>.

³⁸ *Id.*

³⁹ *Id.*

⁴⁰ *Id.*; Will Douglas Heaven, *Bias Isn't the Only Problem with Credit Scores – And No, AI Can't Help*, MIT TECHNOLOGY REVIEW (June 17, 2021), <https://www.technologyreview.com/2021/06/17/1026519/racial-bias-noisy-data-credit-scores-mortgage-loans-fairness-machine-learning/>.

⁴¹ Ezra Klein, *How Fast Will A.I. Agents Rip Through the Economy?*, NY TIMES (Feb. 24, 2026), <https://www.nytimes.com/2026/02/24/opinion/ezra-klein-podcast-jack-clark.html>.

⁴² Tom Wheeler, *The Three Challenges of AI Regulation*, BROOKINGS (June 15, 2023), <https://www.brookings.edu/articles/the-three-challenges-of-ai-regulation/>.



conjunction with other unregulated technologies like digital drivers' licenses and digital wallets, making us even more vulnerable to the harms associated with them. It is critical that the City considers these technologies as interconnected systems, not technologies used in isolation, to ensure that the regulation sufficiently captures both current uses and future developments in the deployment of surveillance technology.

The City Council Must Address the Real Harms of Surveillance Technology

Given the extensive harms inherent in the use of biometric collection and recognition technologies, it is critical that the Council take action to protect New Yorkers. We support the Council's desire to combat biometric recognition technology in places of public accommodation, but we also encourage the adoption of stronger measures that directly address communities' core concerns around privacy and surveillance by prohibiting data collection in addition to limiting how data is used.

We urge the Council to approach surveillance technology with the goal of *preventing* the collection of New Yorkers' personal data, rather than solely regulating how their data is being used. While regulations on the use of personal data are valuable, they are also limited in how much protection they provide. The collection and storage of personal data, regardless of intended purpose, creates significant risks to privacy and security. Personal data is always vulnerable to data breaches or leaks once harvested—a danger heightened by the uniqueness of biometric data.⁴³ Additionally, the very real economic value of such data provides powerful incentives for corporations to sell data even when such sales are illegal. This incentive is further strengthened by the difficulty of tracking illicit disclosures, the existence of loopholes that allow the sale of aggregated or supposedly “anonymized” data,⁴⁴ and weak financial penalties that pale in comparison to the profits offered by the data-mining industry. Even if companies are unwilling to take the risk of directly selling data, other legal workarounds threaten the security of personal data, such as transfers through corporate mergers and acquisitions.⁴⁵

In the Netherlands, for example, a legislative task force is considering blocking a merger between a Dutch identity technology vendor that operates its national ID system and an American company. The concerned

⁴³ Report of the New York City Council Committee on Consumer Affairs and Business Licensing on Int. 1170-2018, (Dec. 10, 2020), <https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3704369&GUID=070402C0-43F0-47AE-AA6E-DEF06CDF702A&Options=Advanced&Search> [accessible as a PDF by clicking hyperlink “Committee Report 12/10/20”]

⁴⁴ Public Interest Advocacy Centre, *Consumers Anonymous? The Privacy Risks of De-Identified and Aggregated Consumer Data*, (Oct. 6, 2011), https://www.piac.ca/wp-content/uploads/2014/11/piac_consumers_anonymous_paper_final_6oct2011.pdf (explaining methods of re-identification from aggregated or de-identified data)

⁴⁵ Daniel Ilan, *Privacy in M&A Transactions: Personal Data Transfer and Post Closing Liabilities*, HARVARD LAW SCHOOL FORUM ON CORPORATE GOVERNANCE, (Nov. 10, 2016), <https://corpgov.law.harvard.edu/2016/11/10/privacy-in-ma-transactions-personal-data-transfer-and-post-closing-liabilities/> (discussing liabilities involving personal data during the mergers and acquisitions process).



members of the legislature wonder whether the merger is a national security threat by virtue of how much power the vendor holding the entirety of the Dutch civic infrastructure has.⁴⁶

Beyond the technical challenges of regulating how personal data is handled, an approach to surveillance that only regulates corporations *after* they collect people's data misses the core problem of surveillance: *people do not want to be the source of information when it is foreseeably going to make them more vulnerable in the future.* Only by ending the collection of sensitive biometric and personal data is it possible to address the real harms of surveillance technology on the people of New York.

New Yorkers Do Not Want to be Surveilled

Time and again, the people of New York City have made clear that they value their privacy and do not want to be surveilled by *anyone*. Beginning with executive orders in 1989 and 2003, New Yorkers demonstrated their commitment to ensuring that their private data is not shared with federal immigration authorities.⁴⁷ These orders have been reinforced by the City Council five separate times over the last 15 years.

In 2011, the Council restricted the Department of Corrections from cooperating with federal immigration detainees.⁴⁸ In 2013, the Council implemented similar limitations on cooperating with immigration detainees for the NYPD.⁴⁹ In 2014, the Council further restricted the NYPD's involvement with federal immigration officials as soon as it was apparent that it could do so lawfully.⁵⁰ Finally, in 2017 the Council passed two more bills limiting cooperation with federal immigration officials: the first restricted all government agencies from spending resources to assist immigration policing;⁵¹ the second significantly limited access to city property by all types of federal policing agencies.⁵² Each of these efforts was designed to ensure that personal information was not being transmitted or shared with federal authorities.

New Yorkers' desire for privacy extends beyond immigration policing, as similar laws have expressed communities' desire not to be surveilled by local government or private businesses either. New Yorkers

⁴⁶ Masha Borak, *US Bid for Dutch Digital ID Infrastructure Company Raises National Security Fears*, Biometric Update (Jan. 26, 2026), <https://www.biometricupdate.com/202601/us-bid-for-dutch-digital-id-infrastructure-company-raises-national-security-fears> (showcasing the risk of sensitive data being acquired by foreign corporations).

⁴⁷ NEW YORK CITY DEPARTMENT OF INVESTIGATION, DOI Investigation into the NYPD's Compliance with Local Laws Restricting City Assistance with Immigration Enforcement, Release #49-2025, (Dec. 3, 2025), <https://www.nyc.gov/assets/doi/reports/pdf/2025/49NYPD.SancLawsRelease.Rpt.12.03.2025.pdf>

⁴⁸ Local Law 2011/062, <https://intro.nyc/local-laws/2011-62>; see also N.Y. City Admin. Code § 9-131 (as amended)

⁴⁹ Local Law 2013/021, <https://intro.nyc/local-laws/2013-21>; see also N.Y. City Admin. Code § 14-154 (as amended)

⁵⁰ Local Law 2014/059, <https://intro.nyc/local-laws/2014-59>; New York City Council, Press Release, *Council to Vote on Legislation Banning Warrantless ICE Detainers* (Oct. 22, 2014), <https://council.nyc.gov/press/2014/10/22/314/>

⁵¹ <https://intro.nyc/local-laws/2017-228>

⁵² Local Law 2017/246, <https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3022111&GUID=2471E159-AF64-4416-801A-91321D8D281E&Options=ID|Text|&Search=> [accessible as a PDF by clicking hyperlink "Local Law 246"]; see also N.Y. City Admin. Code § 4-210



have taken stands against municipal agencies through the adoption of municipal data privacy legislation enacted in 2017,⁵³ against local law enforcement through the 2020 POST Act and its 2025 expansion,⁵⁴ and against their landlords through the 2021 Tenant Data Privacy Act.⁵⁵ At the state level, New Yorkers also expressed concern about the way private businesses handle and use their data by enacting the SHIELD⁵⁶ and the New York Algorithmic Pricing Act.⁵⁷ New Yorkers' willingness to fight for each of these bills year after year sends a clear message: *stop stealing our data*.

Despite these repeated attempts from New Yorkers to secure their personal and private data, their desire for privacy has been undermined by key limitations in law and administration. For instance, the New York City administrative code's regulations on municipal agency data sharing allow the police to collect, receive, or disclose data virtually at will.⁵⁸ Other municipal agencies are held to similarly minimal standards, as is evident through past programs like Worker Connect.⁵⁹ Current laws also only allow for a maximum of \$5,000 in damages; given the difficulty of determining if your personal information has been sold and the costs of bringing an individual suit, this does not serve to adequately disincentivize businesses from selling personal data. Moreover, biometric data is unique, meaning once it is leaked it may well never be recoverable, further showing that proactive (as opposed to a reactive) regulations are needed to meaningfully secure private data. Appealing digital theft of one's likeness, as we can tell from the ongoing weaponization of deep fakes, is too much burden to add to already burdened New Yorkers.

Beyond just the structural and technical limitations of the laws adopted by the city, compliance has also been lackluster. New York Department of Investigation reports have found that the NYPD repeatedly flouts both the POST Act⁶⁰ and limitations on cooperation with federal immigration enforcement.⁶¹ New Yorkers fought hard to get these laws passed, and they expect restraints on surveillance and data collection in

⁵³ N.Y. City Admin. Code, §23-1201 *et seq.* (L.L. 2017/247, 12/17/2017, eff. 6/15/2018; Am. L.L. 2023/061, 5/26/2023, eff. 11/22/2023)

⁵⁴ Local Law 2020/065; N.Y. City Admin. Code, § 14-188; N.Y. City Charter, § 803. *See also* New York City Council, Press Release, *City Council Passes Expanded POST Act Legislative Package to Strengthen Transparency and Oversight of NYPD Surveillance Technology* (Apr. 15, 2025) <https://council.nyc.gov/amanda-farias/2025/04/15/city-council-passes-expanded-post-act-legislative-package-to-strengthen-transparency-and-oversight-of-nypd-surveillance-technology/>

⁵⁵ N.Y. City Admin. Code, § 26-3001 *et. seq.*

⁵⁶ <https://www.nysenate.gov/legislation/bills/2019/S5575>

⁵⁷ N.Y. Gen. Bus. Law § 349-A

⁵⁸ *Supra* note 49, § 23-1202

⁵⁹ Anemona Hartocollis, *Concern for Vast Social Services Database on the City's Neediest*, NEW YORK TIMES, (Jun. 16, 2011), <https://www.nytimes.com/2011/06/17/nyregion/promise-and-concern-for-vast-social-services-database-on-citys-neediest.html?searchResultPosition=1> (examining the risks of the Worker Connect database)

⁶⁰ NEW YORK CITY DEPARTMENT OF INVESTIGATION, *An Assessment of NYPD's Compliance with the POST ACT*, Release #45-2024, (Nov. 26, 2024) <https://www.nyc.gov/assets/doi/reports/pdf/2024/49PostActRelease.Rpt.12.18.2024.pdf>

⁶¹ NEW YORK CITY DEPARTMENT OF INVESTIGATION, *DOI Investigation into the NYPD's Compliance with Local Laws Restricting City Assistance with Immigration Enforcement*, Release #49-2025, (Dec. 3, 2025), <https://www.nyc.gov/assets/doi/reports/pdf/2025/49NYPD.SancLawsRelease.Rpt.12.03.2025.pdf>



return.⁶² Instead, they have been faced with increased usage of facial recognition and other surveillance technologies in their day-to-day lives, both from law enforcement and private businesses. To honor New Yorkers' expectations, the Council should effectuate a strong and comprehensive system that cuts off the harm of surveillance at the source: the surveillance itself.

Surveillance by retail or grocery⁶³ stores, or other places of public accommodation,⁶⁴ is just as unpopular as surveillance by law enforcement.⁶⁵ And as if it were not harmful enough on its own, biometric collection and recognition technologies deployed in places of public accommodation also increases law enforcement agencies' ability to acquire sensitive data, as there are no restrictions on a private business selling or sharing biometric data with the police.⁶⁶

New Yorkers are not interested in being asked for their informed consent before being surveilled, they *do not want to be surveilled at all*. In recognition of this, the New York State Legislature has introduced numerous bills seeking to curtail the use of surveillance technology, including the New York Data Protection Act,⁶⁷ the Protecting Consumers and Jobs from Discriminatory Pricing Act,⁶⁸ and more.⁶⁹ The efforts are community- and worker-driven, reflecting the importance of surveillance technology to the people of New York.⁷⁰

Current Data Privacy Laws Do Not Adequately Protect New Yorkers

Current data privacy laws focus primarily on what happens to personal data *after* it is collected, rather than preventing people's private information from being harvested in the first place. It also centers the direct

⁶² New York City Council, Press Release, *City Council Passes Expanded POST Act Legislative Package to Strengthen Transparency and Oversight of NYPD Surveillance Technology* (Apr. 15, 2025) <https://council.nyc.gov/amanda-farias/2025/04/15/city-council-passes-expanded-post-act-legislative-package-to-strengthen-transparency-and-oversight-of-nypd-surveillance-technology/>

⁶³ Liam Quigley, *NYC Wegmans Is Storing Biometric Data on Shoppers' Eyes, Voices and Faces*, GOTHAMIST (Jan. 3, 2026), <https://gothamist.com/news/nyc-wegmans-is-storing-biometric-data-on-shoppers-eyes-voices-and-faces>

⁶⁴ Jacob Sowers, *Madison Square Garden's Use of Facial Recognition Technology to Bar Certain Lawyers Stirs Protests*, FREE SPEECH PROJECT AT GEORGETOWN UNIVERSITY, (Jul. 18, 2023), <https://freespeechproject.georgetown.edu/tracker-entries/madison-square-gardens-use-of-facial-recognition-technology-to-bar-certain-lawyers-stirs-protests/>

⁶⁵ Paige Oamek & Andrew Giambrone, *Not Just Wegmans: More NYC Retailers Using Facial Recognition as Tech Outpaces Law*, GOTHAMIST (Jan. 12, 2026), <https://gothamist.com/news/not-just-wegmans-more-nyc-retailers-using-facial-recognition-as-tech-outpaces-law>

⁶⁶ N.Y. City Admin. Code, §22-1201 *et seq.* (L.L. 2021/003, 1/10/2021, eff. 7/9/2021) (exempting biometric identifier information "shared with, sold or leased to . . . law enforcement agencies" from regulatory requirements).

⁶⁷ Senate Bill S4860 (establishing the New York Data Protecting Act), <https://www.nysenate.gov/legislation/bills/2025/S4860>

⁶⁸ Senate Bill S8616 (establishing the Protecting Consumers and Jobs from Discriminatory Pricing Act), <https://www.nysenate.gov/legislation/bills/2025/S8616>

⁶⁹ Senate Bill S8623, <https://www.nysenate.gov/legislation/bills/2025/S8623> (banning the use of personal data to algorithmically set prices)

⁷⁰ Johan Sheridan, *New York Democrats Want to Ban Surveillance Pricing, Digital Price Tags*, NEWS10, (Feb. 11, 2026), <https://www.news10.com/capitol/new-york-democrats-want-to-ban-surveillance-pricing-digital-price-tags/>



identification of individuals and shows little concern for the damage that data can do when aggregated. When not directly regulating the handling of personal data, local laws operate mainly to ensure that individuals are informed that they are being surveilled or through securing their consent. None of these approaches are especially effective at restraining the state and corporate surveillance making New Yorkers vulnerable to surveillance pricing and policing.

First, nothing in the current municipal laws forbids an establishment from collecting and using people's personal data for its own ends. Rather, municipal law⁷¹ only forbids establishments from selling or trading information to third parties. Concerningly, it also appears that the current law allows companies to simply *give away* personal data.⁷² As a result, establishments are free to collect and weaponize people's own data against them as much as they want, with the only caveat being that they cannot outsource such exploitation to other companies.

But with an increasing number of private businesses conducting their own surveillance,⁷³ limiting disclosures in this way hardly reduces how frequently people's data is being used against them. It also does little to guard against the risk that the data will be stolen or mishandled; the vast proliferation of people's data means that even with reasonable security measures in place⁷⁴ there is still a significant risk of disclosure or breach. It also ignores the powerful incentive of private corporations to sell the data illicitly to massive data-hungry corporations (particularly those operating in the sphere of Artificial Intelligence) who seek to develop myriad systems that turn people's own data against them.

Second, statutorily requiring the posting of notices or otherwise asking for legal consent allows corporations to take advantage of their market position in comparison to consumers, tenants, and workers.⁷⁵ New Yorkers can hardly afford—either in terms of time or money—to search high and low for the one grocery store that is not scanning them while they shop. Worse, it is likely that such a grocery store will not exist in the near future, leaving consumers and workers with no practical choice but to submit to being surveilled. This is not consent, and it is not privacy.

New Yorkers should be free to shop wherever they want without worrying about being watched; the only way to accomplish that is to prevent surveillance technology from being deployed in shops, stores, and businesses across the city. Doing so will also protect New Yorkers from being targeted by data-mining

⁷¹ N.Y. City Admin. Code § 22-1202(b)

⁷² Emile Ayoub & Elizabeth Goitein, *Closing the Data Broker Loophole*, BRENNAN CENTER FOR JUSTICE, (Feb. 13, 2024), <https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole> (explaining how companies might circumvent exchange limitations in data privacy laws)

⁷³ U.S. GOVERNMENT ACCOUNTABILITY OFFICE, *Consumer Data: Increasing Use Poses Risks to Privacy*, (Sep. 13, 2022), <https://www.gao.gov/products/gao-22-106096> (noting a massive increase in consumer surveillance in recent years)

⁷⁴ For example, those mandated under the SHIELD Act. N.Y. Gen. Bus. Law § 899-bb; *see also* Senate Bill 5575, <https://www.nysenate.gov/legislation/bills/2019/S5575>

⁷⁵ Claire Park, *How "Notice and Consent" Fails to Protect Our Privacy*, OPEN TECHNOLOGY INSTITUTE, (Mar. 23, 2020), <https://www.newamerica.org/oti/blog/how-notice-and-consent-fails-to-protect-our-privacy/#:~:text=Put%20simply%2C%20notice%20and%20consent,and%20utilizing%20their%20personal%20data>.



companies seeking to extract personal information so that they can sell it back to the city⁷⁶ and profit twice from the same invasion of privacy.

Third, current privacy laws are difficult to enforce in comparison to a simple ban on biometric collection and surveillance technology. Instead of attempting to track and monitor every sale and transfer of data, it has been long understood that minimizing the amount of data collected is the best and easiest way to protect personal privacy.⁷⁷ Adopting a prevention-based approach is thus not only more faithful to what people want, but it is also likely to be cheaper, easier to administer, and more effective.

The Legislation Does Not Adequately Address the Harms of Data Surveillance and AI

Though the legislation prohibits the current use of biometric data recognition technology, it does not adequately address the inherent harms of biometric data collection or target the harms that will arise from future developments of these technologies. By only seeking to prevent the harms that biometric data recognition technology perpetuates now, we fail to see and address the full scope of harm these technologies perpetuate. Incoming threats from agentic AI and identity verification technologies, such as those in the financial technology industry, the education technology industry, and more, must be addressed by this legislation to best protect the identities of New Yorkers and prevent further chaos and infringement upon the privacy rights of all New Yorkers.

Proposed Changes to Int 0213-2026 and Int 0428-2026

Banning the Collection of Biometric Data Would Better Protect Data Privacy

We would encourage a prohibition on biometric data collection, not simply the use of biometric recognition technology. We appreciate the outright ban on the use of biometric recognition technology (“It shall be unlawful for any place or provider of public accommodation to use any biometric recognition technology to verify or identify a customer”⁷⁸), which helps further the purpose of protecting the privacy of New Yorkers. However, the bill currently allows for the the collection of biometric data via an informed consent framework, noting that “Any [commercial establishment]... that collects, retains, converts, stores, [or] shares, or otherwise obtains biometric identifier information of customers must disclose such collection, retention, conversion, storage, [or] sharing, or obtaining of biometric identifier information... by placing a clear and conspicuous sign near all... entrances... and shall be required to get the written consent of such customer in advance of any collection.”⁷⁹

⁷⁶ Pakzad, R., & Conti-Cook, C., *Key Considerations When Procuring AI in the Public Sector*, TARAAZ & THE COLLABORATIVE RESEARCH CENTER FOR RESILIENCE (CRCC), (Aug. 5, 2025), <https://taraazresearch.org/ai-procurement> (detailing the exploitation of municipal procurement processes by data companies)

⁷⁷ ELECTRONIC PRIVACY INFORMATION CENTER (EPIC), *Data Minimization*, <https://epic.org/issues/consumer-privacy/data-minimization/> (last accessed Mar. 1, 2026) (explaining the benefits of a data minimization approach)

⁷⁸ Int. No. 213, line 19-20

⁷⁹ Int. No. 213, line 9-18



A ban on the collection of biometric data at the source would help prevent future threats to data privacy, not just immediate ones. Without a ban on biometric data collection, there is an ever-present risk that either the collector of the data, or a third party with nefarious intent, could access the data without the consumers' consent. Allowing collection, even while outlawing recognition software, still sets up a system where the data might be utilized down the line, even if the collector of the data creates a policy with a "retention schedule and guidelines for the permanent destruction" of the data.⁸⁰ Including an outright prohibition on collection would help to ensure that New Yorkers are adequately protected in an ever-evolving technological field that poses continuous surveillance and privacy threats.

In addition, the bill seeks to regulate the collection of biometric data through the implementation of an informed consent scheme, specifying that businesses "shall be required to get the written consent of [customers] in advance of any [biometric data] collection."⁸¹ Implementing an informed consent program might help prevent biometric data collection on an individual level by allowing each consumer to provide consent to the collection of their data. However, the protection of data privacy is not an individual question, but one that applies to all of us. For example, biometric data has the potential to implicate family members of the individual whose data is obtained because it includes genetic identifiers.⁸² In that vein, informed consent on an individual level is ineffective to get at the underlying problem of biometric data collection and recognition technology, which is the use of data in enabling more harmful and hostile technologies in the future. Banning collection at the source would undercut these serious security risks, privacy concerns, and protect vulnerable communities by preventing community mapping.

The "informed consent" procedure in the bill also raises key concerns. There exist inherent power dynamics in situations of urgency, whether it is somebody trying to get into their building quickly or someone trying to buy groceries. Those in power (e.g., landlords, businesses, etc.) are able to exploit this urgency in order to obtain consent from those who may otherwise prefer to withhold consent. There also exists a lack of transparency around how individual biometric data will be used, making this inherently different from a situation where somebody is consenting to data sharing with full information. The inherently coercive nature of the situations where biometric data is being collected renders the "informed consent" scheme ineffective.

The Ban on the Sale of Biometric Data Should Extend to Law Enforcement Agencies

We would also encourage extending the ban on the sale of biometric data to government agencies, including police agencies.⁸³ The bill currently reads, "Nothing in this chapter shall apply to the collection, storage, sharing or use of biometric identifier information by government agencies, employees or agents."⁸⁴

⁸⁰ Int. No. 213, line 3-4

⁸¹ Int. No. 213, line 17-18

⁸² <https://www.thehortongroup.com/resources/understanding-the-risks-of-collecting-biometric-data-in-logistics-and-moving-amp-storage/>

⁸³ Int. No. 213, line 17-18

⁸⁴ Int. No. 213, line 14-18



Allowing government agencies, including police, to continue using biometric data and recognition technology only serves to further the harms outlined above. Facial recognition technology in particular poses an immediate and substantial threat if biometric data is sold to police agencies. Police departments across the country, including in New York, utilize facial recognition technology by submitting “photos of unknown individuals.”⁸⁵ The use of technology in attempting to identify suspects does not stop here, though, as police departments often use other software in conjunction with facial recognition technology to edit photos or fill in “missing pieces.”⁸⁶ This amounts to the utilization of a few pieces of biometric data to fabricate the rest, which results in large errors in outputs.⁸⁷ Using “... these techniques to identify criminal suspects, who may be deprived of their liberty and ultimately prosecuted based on the match...” should be unequivocally discouraged.⁸⁸ Including police agencies in the ban on the sale of data would serve to better protect the New York community from unfair targeting.

Remedies for Victims are Inadequate, and Government Roles with Responsibility for Decisions Related to Procurement of Technology Should Be Reported On Annually

Finally, we would encourage a more robust system for victims of biometric data collection or recognition technologies to seek remedies for violations. The bill currently prevents raising a claim against the collector of the data if the violation has been “cured” within 30 days.⁸⁹ “Curing” a data violation is a misnomer because once the data has been collected and disseminated (whether intentionally or unintentionally), the data is out of the hands of either the individual or the company that collected it, and it can be used by whoever manages to access it.⁹⁰

As such, it is imperative that the responsibility for collection, dissemination, and use of biometric data begins at the stage of procurement. The government actors responsible for each phase of the procurement decision-making process should be clearly identified and their understanding of whether a technology foreseeably increases any risk of constitutional violations must be produced in a written analysis and made publicly available. Instead of placing an undue burden on business owners who may be unable to fully protect the data they collect, transparency and accountability at the stage of procurement would better serve to protect New Yorkers from having their biometric data shared down the line.

⁸⁵ <https://www.flawedfacedata.com/>

⁸⁶ *Id.*

⁸⁷ *Id.*

⁸⁸ *Id.*

⁸⁹ Int. No. 213, line 15-22

⁹⁰ <https://jamiejbartlett.substack.com/p/what-actually-happens-to-your-stolen>



Conclusion

We testify in support of both bills limiting biometric recognition technology but urge the Council to expand such limitations to ban biometric *collection* technology in addition to *recognition* technology. We also encourage all reporting and use limitations to apply equally to all agencies, including police.

We urge the Council to consider not just the direct harms of surveillance policing but of the community harms—including the potential for taxpayers to have to pay three times for new technologies—for the harm, to compensate for the harm, and for the vendors' service.

At the very least we must have a moratorium on all government procurement of biometric collection and recognition technology, more expansive limitations on insurance policies that pressure businesses to install biometric technologies and limitations on businesses' collection of biometric data.