IMMIGRANT DEFENSE PROJECT

40 West 39th Street, Fifth Floor, New York, NY 10018
Tel: 212.725.6422 • Fax: 800.391.5713
www.ImmigrantDefenseProject.org

New York City Council Committee on Immigration
February 11, 2019 Hearing on Oversight--IDNYC Program
Testimony of Mizue Aizeki, Deputy Director, Immigrant Defense Project

Thank you to the Committee for holding this public hearing and for allowing the public the opportunity to address the proposal to integrate multiple functions into the IDNYC with the City. The Immigrant Defense Project (IDP) is a New York-based nonprofit that works to secure fairness and justice for all immigrants by focusing on the rights of those caught at the intersection of the criminal justice system and the immigration system. IDP fights to end the current era of unprecedented mass criminalization, detention and deportation through a multi-pronged strategy including advocacy, litigation, legal support, community partnerships, and strategic communications.

IDP is part of the NYC Municipal ID Coalition that worked in 2014 with the New York City Council and the administration for a municipal ID that would ensure equal access to services and protections for all New Yorkers. As a coalition, we were committed to ensuring that the IDNYC would offer a secure state-issued ID to New Yorkers who faced obstacles in acquiring one—namely the homeless, formerly incarcerated people, gender non-conforming people, youth and undocumented immigrants. Given that many of these New Yorkers were also subject to frequent interaction with the NYPD, the City secured a commitment from the NYPD that the IDNYC would be regarded as a valid form of ID so people would not be brought into the precinct solely because of a lack of an ID. For immigrants, not being brought to a precinct significantly limits the potential of ICE being notified of someone in police custody.[1] Privacy concerns were also a central concern. The Coalition advocated for the City to not retain any underlying documents—the result being a decision by the City to retain the documents for two years, rather than five, and to destroy the documents by December 31, 2016.[2] Fortunately, the City was able to fight off a legal challenge filed by two State Assembly members in December 2016 who argued that destroying the records would threaten national security and that the data should be made accessible under New York State's freedom of information law.[3]

Keeping New Yorkers and their personal information safe from discriminatory local and federal policing and surveillance remains a central principle to our vision for the IDNYC. For this

[1] Fingerprints taken at booking are sent to ICE, allowing ICE to make a detainer request to police to notify ICE when the person is being released from criminal custody. In some jurisdictions, ICE will request that the police hold the person for up to 48 hours after release from custody for ICE to pick them up. Given the increasing risk of deportation that immigrants face when brought into the police precinct, avoiding arrest is ever more critical. Once immigrants are funneled from the criminal legal system into ICE custody, they are often transferred to remote immigration detention centers, making their lack of access to services more severe. People in ICE detention face an incredibly difficult time fighting a pending criminal charge, reuniting with children, or fighting their deportation
[2] http://rules.cityofnewyork.us/sites/default/files/adopted_rules_pdf/amendments_to_idnyc_rule.pdf;
[3] https://www.nytimes.com/2017/04/07/nyregion/new-york-can-destroy-documents-judge-rules-in-municipal-id-case.html

reason, IDP joins our coalition members today in expressing our grave concern about the potential risks associated with the City's proposal to integrate multiple functions into the IDNYC and urge the City to halt the current proposal and pursue an alternative path.[4] The proposed integrations with public and private partners to the IDNYC—including "MTA's planned contactless fare payment system, the NYC Health + Hospitals medical records," and a financial services component—put immigrants at even greater risk of ICE surveillance and targeting.

While we acknowledge and appreciate the City's commitment to serve the needs of New Yorkers, we urge the City to pursue progressive solutions that are not connected to the IDNYC. Combining all these functions on the IDNYC increases the vulnerability of card holders to data breaches. It also increases the likelihood that they will be profiled, targeted, and surveilled based on this data. At a time when the federal government has made clear that immigrants in cities who have passed policies to protect its residents from ICE are the number one target, we cannot afford to put our communities at even greater risk.

For the coalition's overall concerns related to the proposed integrations, please see our December 26, 2018 letter and January 11, 2019 memo with follow up questions to the City.[5]

My comments today focus on the privacy and surveillance risks of the proposed integrations—assessments made in consultation with data security experts. Forest Gregg of DataMade, a civic technology company based in Chicago, is one of the experts who helped ensure maximum privacy protections for the municipal ID program in Chicago. Rocio Baeza, the CEO and Founder of CyberSecurityBase, specializes in helping tech companies with information security. I also consulted with Dr. Tom Fisher with Privacy International, a London-based nonprofit that has expertise in global security issues, and Jason M. Schultz, Director of NYU's Technology Law & Policy Clinic, who focus includes practical frameworks and policy options to help traditional areas of law such as privacy, consumer protection, and civil rights adapt in light of new technologies and the challenges they pose.

Risks from Data-mining and Metadata – When Data Gets Into the Wrong Hands:

Five days after the inauguration on January 20, 2017, the Trump administration laid out its mass deportation agenda in an Executive Order, "Enhancing Public Safety in the Interior of the United States."[6] This has included an escalation of Immigration and Customs Enforcement (ICE) community arrests and raids, with a stated focus on the targeting of "sanctuary jurisdictions" such as New York City—those with policies limiting collusion between local law enforcement

[4] These integrations with public and private partners include "MTA's planned contactless fare payment system, the NYC Health + Hospitals medical records," and a financial services component. The City of New York, Request for Information (RFI) IDNYC Dual Interface Card Payments Initiaitve, IDNYC, Human Resources Administration, Issue Date: Wednesday, May 30, 2018

[5] The NYC Municipal ID Coalition letter to Mayor Bill de Blasio and follow up memo to MOIA Commissioner Bitta Mostofi, Collette Samman, IDNYC Executive Director, HRA, and J. Phillip Thompson, Deputy Mayor for Strategy Policy Initiatives were submitted along with the testimony of Deyaniro del Rio, Co-Director, New Economy Project

[6] Enhancing Public Safety in the Interior of the United States. https://www.whitehouse.gov/presidential-actions/executive-order-enhancing-public-safety-interior-united-states/

ICE. Indeed, IDP has documented a 1700% increase in ICE operations at New York courthouses during the Trump administration.[7]

We also learned in early 2017 that ICE, through a contract with data-mining firm, Palantir, has a web-based system that allows "ICE agents to access a vast 'ecosystem' of data" that facilitates ICE targeting of immigrants for deportation.[8] This system allows ICE to quickly search multiple databases to build profiles on people they want to target for deportation. This includes databases of federal and local law enforcement agencies, as well as any other information they can get access to—data gathered and sold by private companies, location data, social media content and contacts, financial information, health information, and more.

We are deeply concerned that the potential integrations to the IDNYC put immigrants at even greater risk of ICE surveillance, as the data collected through multiple points associated with the ID can become a very useful tool for creating profiles about people or groups of people. According to Privacy International, "Smartcard metadata are usually sufficient to identify an individual with a high degree of precision. Behavioral patterns, physical movements, and purchasing habits can then all be inferred and attributed to the identified individual(s). Should these data become accessible to a third party...they can be used to track and persecute vulnerable groups."[9]

According to the privacy experts that we consulted, combining an ID with multiple functions exposes people to significant privacy and surveillance risks, including:

- **Tying ID to healthcare and financial data**: There is big money made from collecting and selling data. For example, MasterCard has widely noted this is a growing revenue source for the company, selling data to retailers, banks, governments, and Google.[10] Data brokers also make substantial profits by combining personal information, such as healthcare data with financial data, and selling to insurance companies who may deny coverage or increase health insurance rates based on that information.[11] The FBI has warned health care facilities about the potential for cyber attacks to gather medical data—as the sale of this type of personal data is extremely profitable.[12]
- **Tying ID to location data:** In other cities where contactless transit systems are in place, police and federal intelligence agencies have regularly accessed collected data. A position paper on the Australian transit system states: "In almost every jurisdiction where smartcard ticketing has been implemented, police and intelligence agencies are able to access travel information on smartcards for the investigation or prevention of crime. In

---

[7] Immigrant Defense Project, *The Courthouse Trap: How ICE Operations Impacted New York Courts in 2018,* https://www.immigrantdefenseproject.org/ice-courts/

[8] https://theintercept.com/2017/03/02/palantir-provides-the-engine-for-donald-trumps-deportation-machine/

[9] *The Humanitarian Metadata Problem - Doing No Harm in the Digital Era*: page 16; https://privacyinternational.org/report/2509/humanitarian-metadata-problem-doing-no-harm-digital-era

[10] https://www.forbes.com/sites/petercohan/2018/07/22/mastercard-amex-and-envestnet-profit-from-400m-business-of-selling-transaction-data/#120c3df77229

[11] https://www.newsweek.com/secretive-world-selling-data-about-you-464789

[12] https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924

the UK, police make over 3,000 requests per year for travel information from Transport for London."[13]

- **Creating multiple databases tied to the ID:** The various integrations with the IDNYC would create multiple databases with different data and potentially varying levels of security protections. For example, transit data that may be limited to ID number and travel time and location, could be coupled with the medical data which would have much more detailed personal information. It is critical to have more information regarding data protection. That information should include: what data is being stored, who (the government or a third-party provider) is storing it, how long the data will be kept, and who will have access to the data.
- **Narrowing the pool of IDNYC cardholders to those most vulnerable to surveillance**: Privacy experts also have noted that by offering and requiring services on the card that are most likely to be used by people without other options (those who rely on the City's health insurance system, who do not have a bank card, who need the IDNYC as their metro card), this will narrow the group of people who are IDNYC users in the various databases, making it easier to de-anonymize the data and to identify individuals based on the data.
- **Function creep:** According to Privacy International, function creep is one of the main dangers of an ID system—once implemented, the ID begins to be used in an increasing range of functions which not only makes the ID a source of more and more data for both the public and private sector but also potentially forces residents to get an ID as they would otherwise not be able to access services. Two notable examples of ID systems where function creep has violated rights include the national ID controversies in Ireland (the Public Services Card or PSC) and in India (Aadhaar).[14] In Ireland, the PSC ID card started off as an optional card, but became mandatory to access social welfare benefits, to apply for a passport, to take a driver's test, and more.[15] The PSC, which has come under growing scrunity, may be terminated as it maybe be in violation of the European Union's General Data Protection Regulation (GDPR).[16] In India, the Aadhaar ID card, where it is compulsory to link a unique biometric identify with bank accounts, income tax returns, and access to government benefits, has been subject to at least 21 leaks or data breaches—including the breach of personal details of over 1 billion people. The use of Aadhaar by the private sector was declared unconstitutional by the Indian Supreme Court. The court ruled, 'Allowing private entities to use Aadhaar numbers will lead to commercial exploitation of an individual's personal data without his/her consent and could lead to individual profiling'.[17]

---

[13] http://www.ttf.org.au/wp-content/uploads/2016/06/TTF-Smartcard-Ticketing-On-Public-Transport-2010.pdf; https://privacyinternational.org/blog/1596/oyster-octopus-and-metro-cards-what-happens-our-data

[14] https://www.thejournal.ie/public-services-card-oireachtas-committee-3840426-Feb2018/; https://www.sbs.com.au/news/what-is-aadhaar-india-s-controversial-billion-strong-biometric-database

[15] https://www.irishtimes.com/business/technology/wary-of-the-public-services-card-you-have-good-reason-to-be-1.3351106

[16] https://www.dublinlive.ie/news/dublin-news/public-service-cards-scrapped-14271141

[17] https://www.hindustantimes.com/india-news/right-to-privacy-a-fundamental-right-7-aadhaar-controversies-that-raised-concerns/story-UGTtXhgJDtaWrmyuli2LwO.html; https://privacyinternational.org/feature/2299/initial-analysis-indian-supreme-court-decision-aadhaar

Need for more participatory evaluation of the risks, and answers to questions:

Community involvement has been a central feature of the IDNYC, and we appreciate the City's ongoing commitment to an IDNYC that serves the best interests of New Yorkers. While we support the City's efforts to address the financial, medical, and transit needs of New Yorkers, we do not believe that integrating these functions into the IDNYC is a viable solution.

We continue to ask the City for more clarity on the privacy and surveillance risks before the City continues to move forward with this proposal. Some of the questions below were raised in the January 11, 2019, memo submitted by the NYC Municipal ID Coalition to the City, and some have been added based on consultation with privacy experts. In the spirit of ongoing community collaboration, we respectfully request responses to our questions raised in the memo as well as the questions below:

- Given our knowledge about security breaches of data, such as Equifax, why is the City confident that there is adequate security in place to protect IDNYC cardholders from a breach of data at the multiple points where data will be collected (e.g., transit, health services, financial services, homeless shelters)
- What data will be collected about IDNYC cardholders' activity? (transit, health services, homeless shelters, financial services)
    - What data is being stored?
    - Who will hold the data? (The City and/or a third-party vendor?)
    - How long will it be held?
    - Who will have access to the data?
    - What protections will be in place to limit access to the data?
    - What transparency will the City offer to cardholders around how personal information including how it will be collected, stored, and used, and who might have access to it?[18]
    - The negotiated acquisition solicitation specifically states that "data collected through the financial institution cannot be shared with any entity *other than the City of New York*." Why does the City want access to this data?
- Would NYPD or other law enforcement agencies, such as ICE, be able to access the data? If so, what procedures would be required for them to do so?
- How have your agencies engaged NYPD or other law enforcement agencies in the smart chip research/planning process?, to date?
- What protections would be available to cardholders if a federal government agency demanded data/information/analysis from the City or the vendor?
- When and how would the City be made aware of any data requests made to the private vendor and whether or not they were fulfilled?
- Will the City include provisions to assure that anyone who has an IDNYC has the right to gain access to any data collected about them through the ID and then subsequently, the right to correct or delete any information they wish?
- How will the City publicize and inform cardholders about which local, state, and federal agencies have access to their data and when new agencies gain access.

[18] Example from UK: https://tfl.gov.uk/corporate/privacy-and-cookies/zip-oyster-photocard#on-this-page-8

- What mechanism will the City create to ensure the right to be notified and contest any decisions made about benefits based on data gathered through the IDNYC? For example, if their IDNYC data is used related to employment, education, access to healthcare, etc., people should have basic due process and equal protection rights to understand and challenge such decisions.

Our concerns are not unfounded or overly cautious. What we know is that data breaches and the collecting and sharing of personal data is highly profitable and a key focus of financial corporations, such as MasterCard, companies such as Facebook and Google, as well as cyber hackers. We also know that ICE is focused on gathering all forms of personal data to fuel their deportation machine and that other global efforts to expand ID systems, such as in Ireland and India, have led to serious privacy violations.

In contrast to the European Union, the United States does not have comprehensive legal protections for personal data, despite record-breaking data breaches and inadequate data-protection practices.[19] Given a political climate that is hostile to the rights of immigrants, LGBTQ people, certain political activists, people of color, and low-income people, the unnecessary collection of data of IDNYC cardholders is a grave concern.

No other municipal ID program in the U.S. has implemented the kind of technology and integration that NYC is now considering. Chicago opted for minimal data retention with their municipal ID card—in addition to not retaining any supporting documents, the system does not retain names or addresses. The transit card function to Chicago's municipal ID is completely optional, as the City offers metro cards that are not linked to the ID. Also, Chicago decided against including a financial services function to their municipal ID due to concerns about data collection as well the exorbitant fees typically charged by the financial services providers.

For these reasons, we are extremely concerned that the proposed changes to the IDNYC are an unnecessary dangerous experimentation with big data collection, and urge the City to reexamine their consideration of this proposal and instead, to pursue progressive solutions that are grounded in maximum privacy and security protections for New Yorkers.

---

[19] "In 2017, there was a disastrous breach at Equifax, Yahoo's admission that billions of its email accounts were compromised, Deep Root Analytics' accidental leak of personal details of nearly two hundred million U.S. voters, and Uber's attempt to conceal a breach that affected fifty-seven million accounts. Individuals are left stymied about what action they can take, if any, to protect their digital assets and identity." https://www.cfr.org/report/reforming-us-approach-data-protection