OMNY SURVEILLANCE OH MY

New York City's Expanding Transit Surveillance Apparatus

OCTOBER 1, 2019

STOP
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

INTRODUCTION

On May 31, 2019, the Metropolitan Transportation Authority ("MTA") rolled out the new fare collection system "One Metro New York," or "OMNY."[1] Currently a pilot project, OMNY is proposed as the exclusive payment system for the MTA system, including New York City's subway and buses, the Long Island Rail Road, and Metro-North.[2] OMNY is built, hosted, and managed by a for-profit corporation named "Cubic", which previously contracted with London for its transit payment platform.[3]

OMNY is an electronic payment system that uses radio signal transceivers in phones, smart devices, and credit and debit cards to process riders' fares directly at subway turnstiles or bus entries. But this new, wireless payment platform also allows the MTA, and potentially third parties, to collect an alarming amount of information about transit users. OMNY will allow the MTA to track when and where specific transit users enter the system, for example, to take the subway, train, or bus. Combined with a weak Privacy Policy, available only through the OMNY website, and existing MTA surveillance tools, OMNY provides the MTA with unprecedented surveillance capacity.

In this paper, we explore the MTA's data collection and protection plans for OMNY. Regrettably, given the lack of publicly available information to date, this paper is necessarily only a starting point in a much larger, ongoing research task. Tellingly, when questioned about OMNY's privacy impact, MTA officials refused to answer critical questions about how much of this fundamental responsibility they have delegated to Cubic.[4]

Given how often government agencies, including the New York Police Department ("NYPD"), have abused surveillance data to target ethnic and religious minorities and how for-profit corporations face overwhelming pressure to monetize user data, OMNY has the potential to expose millions of transit users to troubling repercussions. This paper explores (i) how OMNY operates, (ii) the data collected by OMNY and the OMNY Privacy Policy, and (iii) the potential abuse of the data by the MTA, Cubic, or law enforcement agencies.

---

[1] *See* MTA press release titled "MTA Launches Public Pilot For OMNY Contactless Fare Payment System – First New Payment System In 25 Years", 3/5/2019, available online at: http://www.mta.info/press-release/mta-headquarters/mta-launches-public-pilot-omny-contactless-fare-payment-system-%E2%80%93

[2] https://ny.curbed.com/2019/5/22/18617849/nyc-subway-mta-omny-contactless-payment-system

[3] Cubic press release titled "Cubic Wins Contract from New York MTA to Replace Iconic MetroCard System with World-Class New Fare Payment System", 10/25/2017, available online at: https://www.cubic.com/news-events/news/cubic-wins-contract-new-york-mta-replace-iconic-metrocard-system-world-class-new, noting that Cubic will be responsible for hosting the platform.

[4] "MTA's New Fare Payment OMNY Launches Friday Amid Questions About Data Security & Durability," 5/30/2019, available online at: https://gothamist.com/2019/05/30/mta_omny_subway_contactless.php, noting that "Cubic and the MTA didn't reply to questions about how it plans to protect user data collected through OMNY." (emphasis added);

I. OMNY

OMNY facilitates the payment of transit fares through the use of contactless credit and debit cards, or digital wallets installed on smart devices (such as Apple Pay or Google Pay).[5] By 2023, the system will also support payment by special OMNY cards, at which point the current MetroCard fare collection system will be phased out.[6]

OMNY allows riders to pay their fare by "tapping" their preferred payment method against a contactless card reader at a subway turnstile or bus entry. That "tap" automatically transmits data from the payment card to the reader and then to a remote data center for authentication and storage. Based on just the OMNY features the MTA has publicly touted, including the ability for individuals to access their account and trip history online, it is evident that at least payment card and location data will be collected at each point of use and stored in a database. Neither the MTA nor Cubic have been forthcoming about what additional data, beyond what is accessible to users, will also be collected, stored, and associated with a rider's account or profile.

While riders can currently decline to use OMNY by continuing to rely on the MetroCard fare collection system, this option will be phased out by 2023, thereby making it increasingly difficult to avoid tracked payment methods. The MTA promises that an "OMNY card" will eventually be available for purchase using cash, however the MTA and Cubic are expected to encourage riders to use the contactless fare payment, which will more easily facilitate tracking riders and provide greater opportunity to monetize rider data.

To date, the MTA and Cubic have provided limited information about the forthcoming OMNY cards. Unknowns include when the cards will become available, whether they will be purchasable at vending machines in each subway station as MetroCards are or only at limited locations, and what fees will be associated with them. In Chicago, Cubic built and deployed a similar transit payment card in 2013 with high fees, some of which were eventually lessened after considerable backlash.[7] Such fees constitute a privacy tax.

OMNY uses Near Field Communications ("NFC") technology to allow contactless payment. While "NFC based systems are generally more secure" than swiping a credit card, researchers have been able to successfully attack contactless NFC payment cards and mobile wallets, including Google Pay and Apple Pay, "with minimal difficulty and delay in transaction time."[8] It is not even necessary for the attacker to directly touch the victim or their payment

---

[5] *See* "About OMNY" webpage, available online at: https://omny.info/about-omny

[6] *See* MTA press released titled "MTA Launches Public Pilot For OMNY Contactless Fare Payment System – First New Payment System In 25 Years", 3/5/2019, available online at: http://www.mta.info/press-release/mta-headquarters/mta-launches-public-pilot-omny-contactless-fare-payment-system-%E2%80%93

[7] https://www.chicagotribune.com/news/ct-xpm-2013-05-24-ct-met-cta-ventra-debit-card-changes-20130525-story.html
See also: https://chi.streetsblog.org/2016/05/09/study-ventra-fees-cost-social-service-providers-140000-bus-rides-per-year/

[8] Giese, Dennis, et al. "Security Analysis of Near-Field Communication (NFC) Payments." arXiv preprint arXiv:1904.10623 (2019). *See also* Nicholas Akinyokun and Vanessa Teague. 2017. Security and Privacy Implications of NFC-enabled Contactless Payment Systems. In Proceedings of the 12th International Conference on

method; proximity is enough. The risk of such an attack increases in crowded places like subway stations.[9]

OMNY also offers an online account management system, known as "OMNY Account," to allow registered riders to view their travel activity and manage payment options.[10] Unregistered users may also view their travel activity using a "trip history" feature by entering their payment card details.[11] The OMNY Account and trip history feature only highlight *some* of the data collection system's tracking, data collection, and data retention capabilities as OMNY presumably collects and stores significantly more data than is visible to users through those features.

II. OMNY DATA COLLECTION AND PRIVACY POLICY

OMNY's Privacy Policy is meant to govern the collection and storage of rider data.[12] Although MTA officials have promised to keep rider data secure and safe, the Privacy Policy is deficient in several regards: (i) the Policy is only available online, even though it governs real-world usage of the system by riders who may not have access to the Policy before unknowingly sharing their data; (ii) the Policy puts no limitations on the ability of the MTA and Cubic to collect highly sensitive data about riders; (iii) the Policy permits the MTA and Cubic to store the data indefinitely; and (iv) the Policy allows a wide range of uses for the collected data, including sharing with government agencies other than the MTA.

It is concerning that data about both real-world use of OMNY—*i.e.*, paying for entry to a subway or bus—and online use of the OMNY Account[13] is collected even though the Policy is only available online and users are not presented in advance with the opportunity to review or approve it. The MTA and Cubic act on the premise that riders have accepted the Policy simply by choosing to tap their payment card at an entry point to the transportation system, whereas most riders will not realize that such a simple act is triggering massive collection, indefinite storage, and uncertain usage of their data. This disconnect is particularly puzzling as the MTA is a public- and rider-funded authority, not a free service that needs to monetize data as its only source of revenue.

The Policy indicates that OMNY collects data about the payment card used for each transaction, such as the card number and user's billing address,[14] as well as information about the

---

Availability, Reliability and Security (ARES '17). ACM, New York, NY, USA, Article 47, 10 pages. DOI: https://doi.org/10.1145/3098954.3103161

[9] *See Id*.

[10] https://omny.info/register

[11] https://omny.info/trip-history

[12] At: https://omny.info/privacy.

[13] Section 1 of the Privacy Policy provides that "We collect your credit card or other payment card information when you (i) *tap your contactless card or digital wallet* or wearable (individually and collectively, "Payment Method(s)") at an OMNY reader; (ii) *register a credit or debit card* as a Payment Method in *your OMNY Account*; or (iii) *purchase a fare product* (e.g., a monthly pass) through the *OMNY Website or other sales channels*." (Emphasis added). In other words, data associated with both real-wor;d users and online users is stored in accordance with the Privacy Policy.

[14] Section 1 of the Privacy Policy provides that "Such information may include the credit or debit card primary account number and expiration date, both for the cards you tap at an OMNY reader as well as any card provisioned

"purchase" of each ride, like the location of the card reader and the time and date of a tap. Combining this information would allow the MTA, or others with whom they share the data, to map each rider's travels around New York City. Analysis over a long period of time could allow the cataloguing of each rider's habits and comparisons of the habits of riders living in different neighborhoods. As discussed in the next section, such information could easily be misused.

Furthermore, the Policy uses non-limiting language—such as, "may include, without limitation"—when detailing the data that the MTA and Cubic are permitted to collect. Accordingly, there is no clear limitation on their authority to collect and store highly sensitive rider data.

The Policy also lacks a specifically defined period of data retention. Instead, Section 4 of the Policy, titled "Retention of Your Personal Information," states only that information "is retained by us in accordance with the applicable records retention and disposition requirements of New York or federal law." The Policy itself places no explicit temporal limits on the MTA or Cubic's ability to store usage data or personal information nor does it even explain what statutory limits it might be subject to. By contrast, the Policy clearly defines the time period that riders will be able to access their own information online as 90 days.[15] Worryingly, Section 2 of the Policy contemplates that the MTA and Cubic may generate anonymized rider data, which would require large volumes of data to be useful, indicating that the MTA and Cubic will store rider data for a long period of time. Since transactions are processed in a matter of seconds, there is no need related to the service being provided for the MTA to store any rider data for any length of time.

Privacy advocates strongly discourage the practice of keeping personal information unnecessarily because of the potential for misuse, exploitation, and security breaches.[16] Storing rider data for longer than necessary to process a transaction raises the alarming possibility that the MTA and Cubic intend to contribute to the culture of government surveillance by making New Yorkers' data readily accessible with minimal usage restrictions to law enforcement and other government actors, or even to monetize it by selling it to for-profit corporations. The MTA, which essentially functions as a public utility, must operate in a different manner than companies such as Facebook and Google, where such mercenary practices are commonplace.

The Policy explicitly authorizes the MTA and Cubic to share collected information with law enforcement agencies under certain circumstances.[17] It cautions that "you should not provide personal information if you are concerned about disclosure of your information under [various

---

to a digital wallet. Additionally, we may collect the country of card issuance, the card brand (e.g., Visa, MasterCard), and/or the card type (e.g., credit, debit, pre-paid, contactless, transit benefit, etc.). For any transaction, the method by which OMNY authenticates your Payment Method varies, but may include, without limitation, your PIN, billing ZIP code or full billing address to support cardholder verification."

[15] While the data is available online for a period of 7 or 90 days (as the case may be), the OMNY system may store the data for a longer indefinite period. Section 1 of the Privacy Policy notes that "If you register for an OMNY Account, your transaction and travel history can be tracked through your OMNY Account, and you can *access* this information for a period of up to 90 days by logging into your OMNY Account." (Emphasis added).

[16] https://www.bcs.org/content-hub/the-dangers-of-data-collection/

[17] See Sections 2 and 3 of the Privacy Policy, which detail permitted uses and sharing of rider information under the Policy.

laws].” A rider may not even be notified in advance, or at all, that their personal information has been shared with law enforcement. For instance, a prosecutor would only be required to serve a subpoena for a rider’s information on the MTA, not on the rider themselves.[18] Without knowledge a government actor was seeking such data—or even a complete understanding of what kinds of data the MTA had collected and maintained—an individual would be unable to challenge the disclosure, potentially leading to criminal or civil liability.

The Policy also authorizes use of riders’ information for enhancements to OMNY and MTA products and for marketing communications. Rider information may be shared with third-party providers to enable such uses, which poses risks that the information could be misused by third parties, intercepted in transit, or breached on a third party’s system.

III. POTENTIAL FOR MISUSE OF RIDER DATA

The MTA’s collection and tracking of rider data poses both familiar and novel concerns for the public. Such a system expands the MTA and partnered law enforcement agencies’ capacity to engage in sustained suspicionless surveillance of New Yorkers. Agencies could easily transform OMNY into a perpetual log of every rider’s movements. This data could be used to monitor riders who enter a subway station following a political protest or to track which riders use the bus stop outside a mosque on Friday afternoons.

The danger of this data is only amplified when combined with the information from other perpetual tracking systems, such as the automated license plate readers that permeate New York City, tracking nearly every car on the road. Not only could agencies use this information to profile and track systemically-over-surveilled communities, but individual employees could use this data to track estranged family members and neighbors.

IV. DISPROPORTIONATE IMPACT CONCERNS

For years, government enforcement agencies in New York City—including NYPD and ICE—have actively collected and used surveillance data in the course of their operations, and have regularly done so in violation of individuals’ constitutional rights.

As discussed in the 2012 Supreme Court ruling *United States v. Jones*, any form of real-time location tracking may violate the Fourth Amendment. However, the NYPD’s Domain Awareness System (“DAS”) currently uses cameras, license plate readers, and radiological sensors to create a real-time surveillance map of New York City.[19] The system was created by a public-private partnership between the NYPD and Microsoft in 2012.[20] The NYPD uses this

[18] See FRCP 45 (b).
[19] *See* ADAM MARTIN, *NYPD, Microsoft Hope to Make a Mint off New Surveillance System*, THE ATLANTIC, Aug. 8, 2012, https://www.theatlantic.com/national/archive/2012/08/nypd-microsoft-hope-make-mint-new-surveillance-system/324924/.
[20] The Domain Awareness System collects the license plate data scanned by the approximately 500 license plate readers operated by the NYPD and combines it with footage from cameras and other surveillance devices around the city. The NYPD holds on to the license plate data for at least five years regardless of whether a car triggers any suspicion. *See* MARIKO HIROSE, *Documents Uncover NYPD’s Vast License Plate Reader Database*, ACLU, Jan. 25,

database to track suspects, and newly released documents reveal that ICE creates watch-lists using DAS data to track undocumented immigrants.[21] Despite its promise of being a "sanctuary city," New York's information collection and sharing already puts undocumented New Yorkers at risk.[22]

A 2015 agreement between the NYPD and Vigilant Solutions further augmented the department's tracking capabilities. This agreement provided the NYPD access to the company's nationwide database of over two billion license plates[23] and increases the DAS database by one million data points per day.[24] Vigilant Solutions' "stakeout" feature allows the NYPD to surveil everything from political rallies to abortion clinics to church services.[25] Its artificial intelligence tool purportedly enables the NYPD to "learn" a person's daily routine.[26]

As early as 2012, the NYPD shared surveillance footage with IBM so that IBM could develop facial recognition technology that allowed the NYPD to search camera footage for images of people by hair color, facial hair, and skin tone. The capability was available to the NYPD as early as 2012.[27]

OMNY has the potential to make a bad situation worse. Currently, the NYPD shares data with ICE both directly and indirectly through private, state, and federal intermediaries.[28] Because ICE does not report when local data sharing enables detention operations, it is difficult to know how many New Yorkers have been deported as a result of the information sharing that already exists.[29] Transit history data would enable ICE to locate immigrant community members by allowing the agency to track their daily movements. Further, identity-based surveillance using OMNY could compromise a rider's right to anonymous public speech and association.

Additionally, the NYPD's long history of racial discrimination and other forms of bias has led it to regularly focus its enforcement efforts on individuals belonging to minority or improvised groups, compounding the harmful effects of constitutional violations. Throughout the 2000s, the NYPD implemented the discriminatory "stop-and-frisk" program that increased stops

---

2016, https://www.aclu.org/blog/privacy-technology/location-tracking/documents-uncover-nypds-vast-license-plate-reader-database?redirect=blog/speak-freely/documents-uncover-nypds-vast-license-plate-reader-database.

[21] *See* ZACH WHITTAKER, *ICE Has a Huge License Plate Database Targetting Immigrants, Documents Reveal*, TECH CRUNCH, March 13, 2019, https://techcrunch.com/2019/03/13/ice-license-plates-immigrants/.

[22] *See* LIZ ROBBINS, *"In a 'Sanctuary City,' Immigrants Are Still at Risk"*, N.Y. TIMES, Feb. 27, 2018, https://www.nytimes.com/2018/02/27/nyregion/sanctuary-cities-immigrants-ice.html.

[23] *See* ROCCO PARASCONDOLA, *Exclusive: NYPD will be able to track fugitives who drive past license plate readers across the U.S.*, N.Y. DAILY NEWS, Mar. 02, 2015, https://www.nydailynews.com/new-york/nypd-track-fugitives-drive-license-plate-readers-article-1.2133879.

[24] *See id.*

[25] *See id.*

[26] *See id.*

[27] https://theintercept.com/2018/09/06/nypd-surveillance-camera-skin-tone-search/

[28] *See* ROCCO PARASCONDOLA, *Exclusive: NYPD will be able to track fugitives who drive past license plate readers across the U.S.*, N.Y. DAILY NEWS, Mar. 02, 2015, https://www.nydailynews.com/new-york/nypd-track-fugitives-drive-license-plate-readers-article-1.2133879.

[29] See felipe de la hoz, "New York, a Sanctuary State, Provides Criminal Justice Data to ICE", documented, May 8, 2019, https://documentedny.com/2019/05/08/new-york-a-sanctuary-state-provides-criminal-justice-data-to-ice/.

by more than five-fold and almost exclusively targeted New Yorkers of color.[30] In addition, a bombshell 2011 AP report found significant evidence[31] that the NYPD had conducted widespread religious profiling of Muslim New Yorkers.[32] The NYPD deployed informants and undercover personnel without warrants to investigate Muslims in mosques, coffee shops, and even their homes for merely practicing their faith.[33] Disturbingly, the 2016 Office of the Inspector General for the NYPD ("OIG") found that over 95% of NYPD investigations targeted Muslim New Yorkers and their allies.[34]

In June 2019, another OIG report revealed the NYPD's systematic failure to investigate thousands of biased policing complaints over the prior five years.[35] The report found that the NYPD's investigations were so inadequate that the department failed to substantiate even a single complaint.[36] Additionally, the report found that the NYPD simply does not investigate the use of racial slurs and other offensive language by its officers, despite rules clearly marking that behavior as "biased policing."

Given the NYPD's history of discrimination, gaining access to OMNY—yet another round-the-clock tracking tool—would undoubtedly mean that New Yorkers of color, immigrants, and other minority groups would be disproportionately targeted.

V. CONCLUSION

OMNY has the potential to increase the convenience of some transit users' commutes, but it comes at a steep privacy price. Contactless payment systems may be viable in the future, but OMNY lacks the privacy and security guarantees to be expanded across the MTA system. If MTA officials disregard these concerns and continue to push this problematic platform, they must, at an absolute minimum, implement technical and legal protections to ensure that OMNY does not transform into a transit tracking system, monitoring where New Yorkers go and even whom we travel with. A simple bus or subway ride shouldn't cost us our civil rights.

---

[30] N.Y.C. Local Law No. 71 § 1 (2013), https://www1.nyc.gov/assets/cchr/downloads/pdf/amendments/Int_1080_2013_bias_profiling.pdf; in 2013, a federal judge held that NYPD's policies and practices on "stop, question, and frisk" violated the Fourth and Fourteenth Amendments, primarily because the Court found that those policies and practices resulted in the disproportionate and discriminatory stopping of hundreds of thousands of Black and Latino people. The Court issued an order specifying remedies and appointed a federal monitor to oversee implementation of the Court orders and the parties' agreements. The Court also required that NYPD "begin tracking and investigating civilian complaints related to racial profiling and other allegations of bias" committed by officers. *See generally Floyd v. City of N.Y.*, 959 F. Supp. 2d 540 (S.D.N.Y. 2013).

[31] For an in-depth review of Muslim surveillance by the NYPD, *see Raza v. City of New York*, 998 F. Supp. 2d 70 (E.D.N.Y. 2013).

[32] *See Handschu v. Police Dep't of N.Y.*, 219 F. Supp. 3d 388 (S.D.N.Y, 2016).

[33] *See id.*

[34] *See* OIG-NYPD, *An Investigation of NYPD's Compliance with Rules Governing Investigations of Political Activity*, at: https://www1.nyc.gov/assets/oignypd/downloads/pdf/oig_intel_report_823_final_for_release.pdf).

[35] *See* OIG-NYPD, *Complaints of Biased Policing in New York City: An Assessment of NYPD's Investigations, Policies, and Training*, at: https://cbsnewyork.files.wordpress.com/2019/06/19biasrpt06-26-2019.pdf.

[36] Based on an analysis of 888 biased policing allegations filed between late 2014 and early 2017.

Surveillance Technology Oversight Project, Inc.

40 Rector Street
9th Floor
New York, NY, 10006

www.STOPSpying.org

STOP
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT