TransitCenter

Do Not Track

A guide to data privacy for new transit fare media

transitcenter.org

TransitCenter

TransitCenter
One Whitehall Street
17th Floor
New York, NY 10004

TransitCenter works to improve public transit in ways that make cities more just, environmentally sustainable, and economically vibrant. We believe that fresh thinking can change the transportation landscape and improve the overall livability of cities. We commission and conduct research, convene events, and produce publications that inform and improve public transit and urban transportation. For more information, please visit www.transitcenter.org.

Publication Date: March 2021

@transitctr
@TransitCenter
@transitcenter_

TransitCenter

Do Not Track

A guide to data privacy for new transit fare media

Acknowledgments

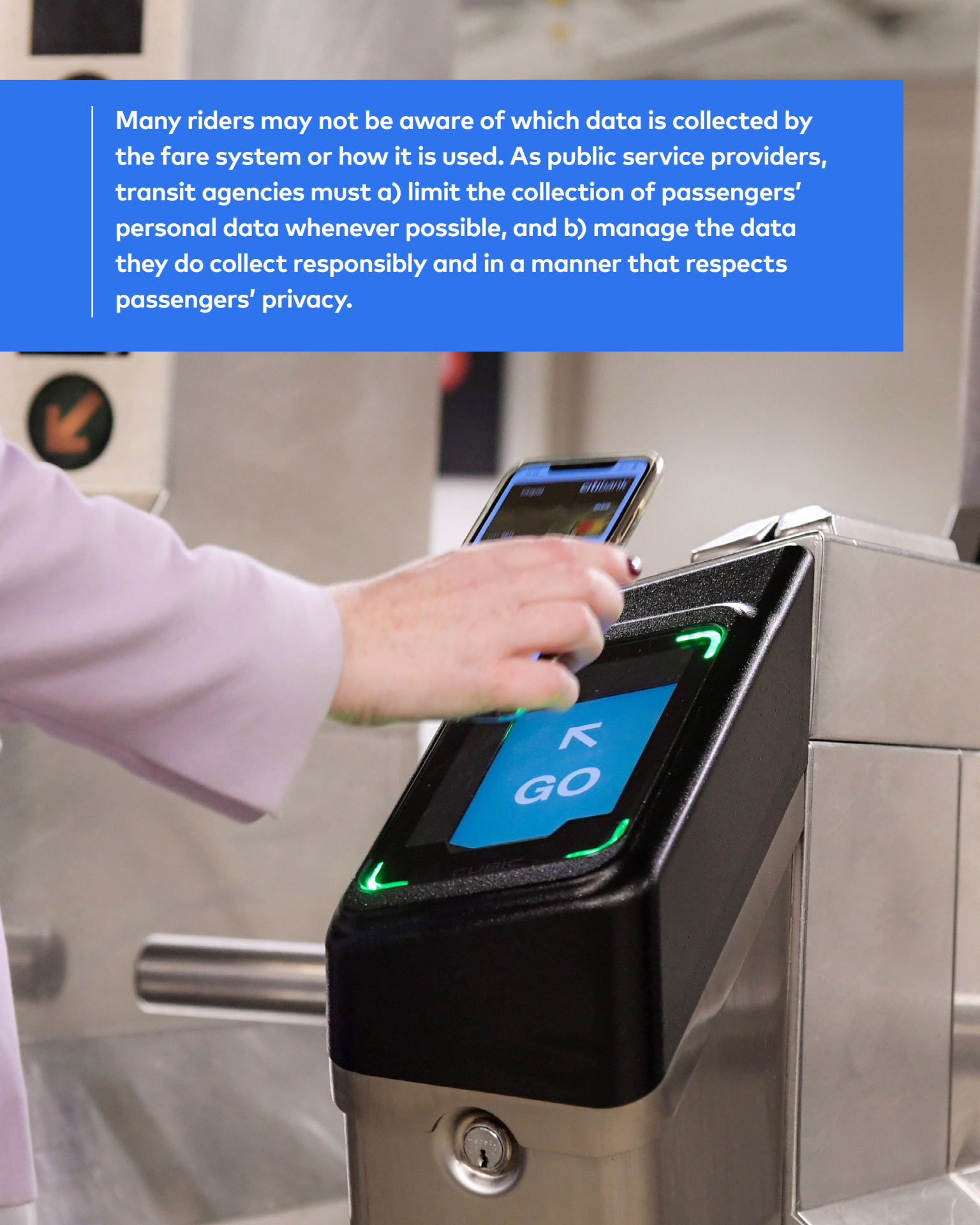
This report was authored by Tom Pera with contributions from Ben Fried, Stephanie Lotshaw, Chris Van Eyken, and Hayley Richardson of TransitCenter. The authors thank TransitCenter's David Bragdon, Tabitha Decker, Steven Higashide, and Kapish Singla; Surveillance Technology Oversight Project's Albert Fox Cahn; Electronic Frontier Foundation's nash Sheard, Jamie Lee Williams, Lee Tien, and Bennett Cyphers; WSP's David Ory; Secure Technology Alliance's Randy Vanderhoof; and Greg Newmark of Kansas State University for their valuable ideas and feedback on this report. Any errors are TransitCenter's alone.

Design
Cause + Matter

Published by
TransitCenter
1 Whitehall Street
New York, NY 10004

Contents

Many riders may not be aware of which data is collected by the fare system or how it is used. As public service providers, transit agencies must a) limit the collection of passengers' personal data whenever possible, and b) manage the data they do collect responsibly and in a manner that respects passengers' privacy.



Agencies that enact good privacy practices and transparently share those practices with the public will encourage adoption of new fare media by enabling riders to make informed choices.

Introduction

As digital communication technologies proliferate, people can purchase goods and services using an expanding array of payment methods: digital wallets, credit cards equipped with near-field communication (NFC), and other new methods are becoming increasingly common.[1] Public transit agencies nationwide are adapting fare collection systems to accept a wider range of these payment methods, improving the convenience of transactions for passengers. Agencies also see the potential for new payment methods—or fare media—to improve transit operations and service delivery. Possible benefits include faster bus boarding and the integration of fare policy across modes and agencies within a single metro area.

At the same time, new fare media raise legitimate individual privacy concerns. Namely, they have the potential to significantly increase the personal data generated and collected by transit agencies, as well as the private companies agencies contract or partner with. Once collected, the data can be accessed by other government entities, sold to private companies (in the case of private sector data collection), or simply be vulnerable to a data breach. Many riders may not be aware of which data is collected or how it is used. As public service providers, transit agencies must a) limit the collection of passengers' personal data whenever possible, and b) manage the data they do collect responsibly and in a manner that respects passengers' privacy. Agencies that enact good privacy practices and transparently share those practices with the public will encourage adoption of new fare media by enabling riders to make informed choices.

This policy brief explores the privacy risks of new transit fare media and recommends four methods agencies can adopt to safeguard riders' privacy and give them confidence in the fare payment system:

1. **Ensure that riders retain the ability to pay without being linked to a credit card account or other personal identifier**, and that these payment options are priced at the same rate as newer payment systems that collect and generate more data. This includes agency-issued fare cards with a stored value that can be refilled with cash at a fare card machine or third-party vendor.
2. **Make secure data management an organizational priority**. Agencies should adopt policies for secure data management, and strive to constantly improve data security the same way they actively seek to improve service and operations.

1 NFC-enabled devices process transactions through close proximity alone, enabling "contactless payment." Users can tap their device against a card reader instead of swiping or inserting their card into the reader. Most new smartphones, credit cards, and debit cards are NFC-enabled.

If a passenger uses a fare card with a unique ID, then the agency can collect data on the unique ID, the time that it was used, and the station or stop where it was used. This data is a powerful tool for transit agencies to understand trip patterns and identify where service should be allocated.

3. **Clearly and transparently communicate privacy policies**. Riders should be able to easily find out what data is collected, how that data is used, and which parties can access their data.
4. **Use data sources that protect personal privacy to improve service planning for riders**. Many transit agencies use fare payment data to track how riders are using the system. They then use this data to adjust service to best fit rider needs. Other data sources, such as automated passenger counters (APCs) and passenger surveys, may provide similar information while collecting less personal data.

Changes in Fare Payment

The major shift in the fare media landscape is from closed-loop payment systems to open-loop payment systems. Closed-loop payment systems—still the most commonly used by transit agencies—are characterized by fare media used exclusively within the transit system. Examples include physical tokens, punch cards, swipe cards, and even NFC-enabled, agency-issued tap cards. With closed-loop payment systems, the transit agency typically retains control over all data generated by passengers, because the agency controls the fare media.[2] If a passenger uses a fare card with a unique ID, then the agency can collect data on the unique ID, the time that it was used, and the station or stop where it was used. This data is a powerful tool for transit agencies to understand trip patterns and identify where service should be allocated.

Notably, some types of fare media used in closed-loop payment systems—punch cards or tokens, for example—do not provide such detailed data for transit agencies to plan service. This is because punch cards and tokens provide no personally identifying information or unique ID during the transaction process that the agency can associate with a particular user, as well as that user's travel behavior.

2 The agency, of course, might still contract with a private company to install and operate the fare payment system; however, the agency can still dictate the terms of how data is managed in its contract with the third party.

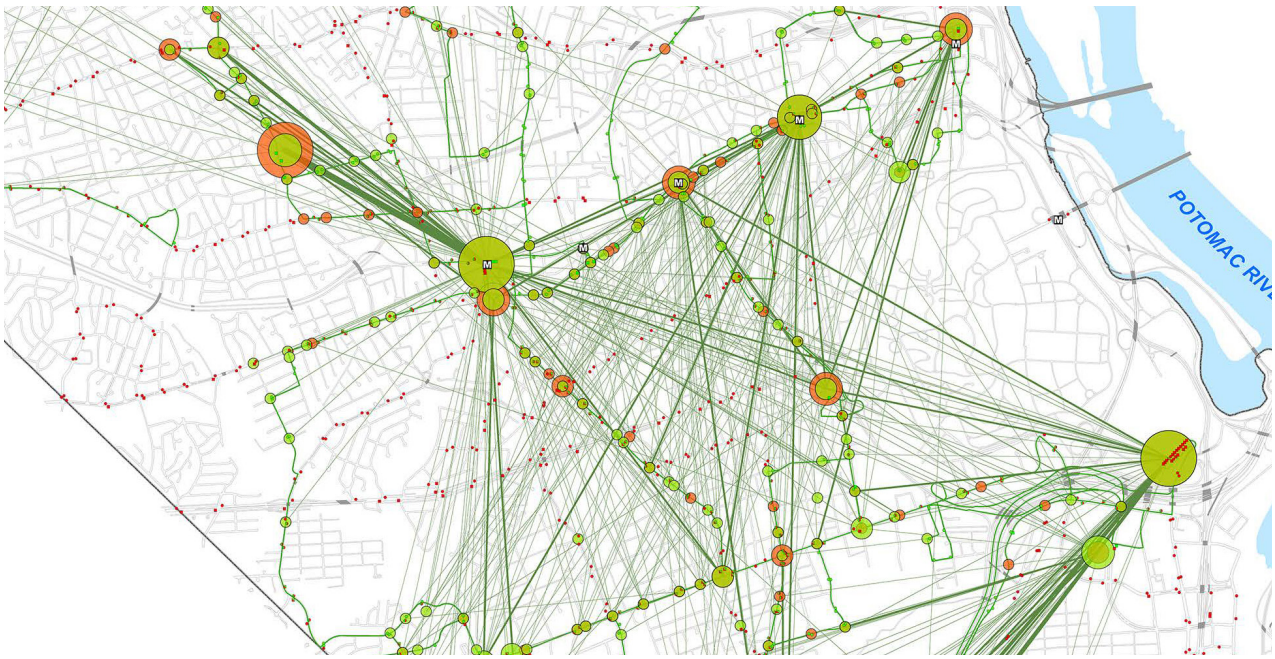


Fig. 1
Example of origin-destination map

The shift to open-loop payment systems creates new privacy challenges as personal data on transit use is collected by private companies managing the NFC-enabled payment devices.

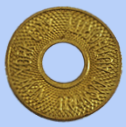
Closed-loop media	
	Magnetic stripe cards (MetroCard)
	Tokens
	NFC-enabled tap cards issued by the agency (OMNY card, Ventra card)
	Proprietary transit agency smartphone app
Open-loop media	
	Digital wallets (PayPal, Apple Pay, Google Wallet)
	NFC-enabled debit and credit cards issued by a bank (Chase Visa, Capital One Mastercard)

Fig. 2
Types of closed-loop payment media vs types of open-loop payment media

The agency can see that *a token was used* but not who used it.

Open-loop payment systems differ from closed-loop payment systems in that they integrate third-party payment methods, such as NFC-enabled credit cards and digital wallets. These systems can markedly improve convenience for passengers. With open-loop payment, as long as transit users have a credit card or smartphone on hand, they don't have to worry about purchasing a separate fare card or making sure the card has funds before boarding. These payment systems also can produce dramatic time savings, especially on buses: The MTA estimates that NFC-enabled devices reduce the transaction processing time from about 2.4 seconds swiping a MetroCard to 500 milliseconds, or approximately one minute saved for every 30 passengers who board the bus.[3] For a route like the B6 in Brooklyn with an average daily ridership of 34,000 passengers, this could add up to almost 18 hours of bus service saved per day, which the agency can then reinvest in additional service on the route.

3 Kabak, B. (2019, June 21). *Second Ave. Sagas Podcast, Episode 5: OMNY with the MTA's Al Putre.* Second Ave. Sagas. http://secondavenuesagas.com/2019/06/21/second-ave-sagas-podcast-episode-5-omny-with-the-mtas-al-putre/

The Two Branches of Transit Data Collection

The shift to open-loop payment systems creates new privacy challenges as personal data on transit use is collected by private companies managing the NFC-enabled payment devices. But while open-loop payment is relatively new in public transit, privacy concerns related to how agencies collect and track passenger data predate it. Existing payment methods like magnetic stripe cards already generate personal data that agencies collect during transactions. Thus, the issue of privacy in transit has two branches:

1. Public sector collection of personal data, which has been possible since the first electronic, reusable fare cards debuted.
2. Private sector collection of data, which is emerging from the introduction of open-loop payment systems and increased reliance on private companies for operations support.

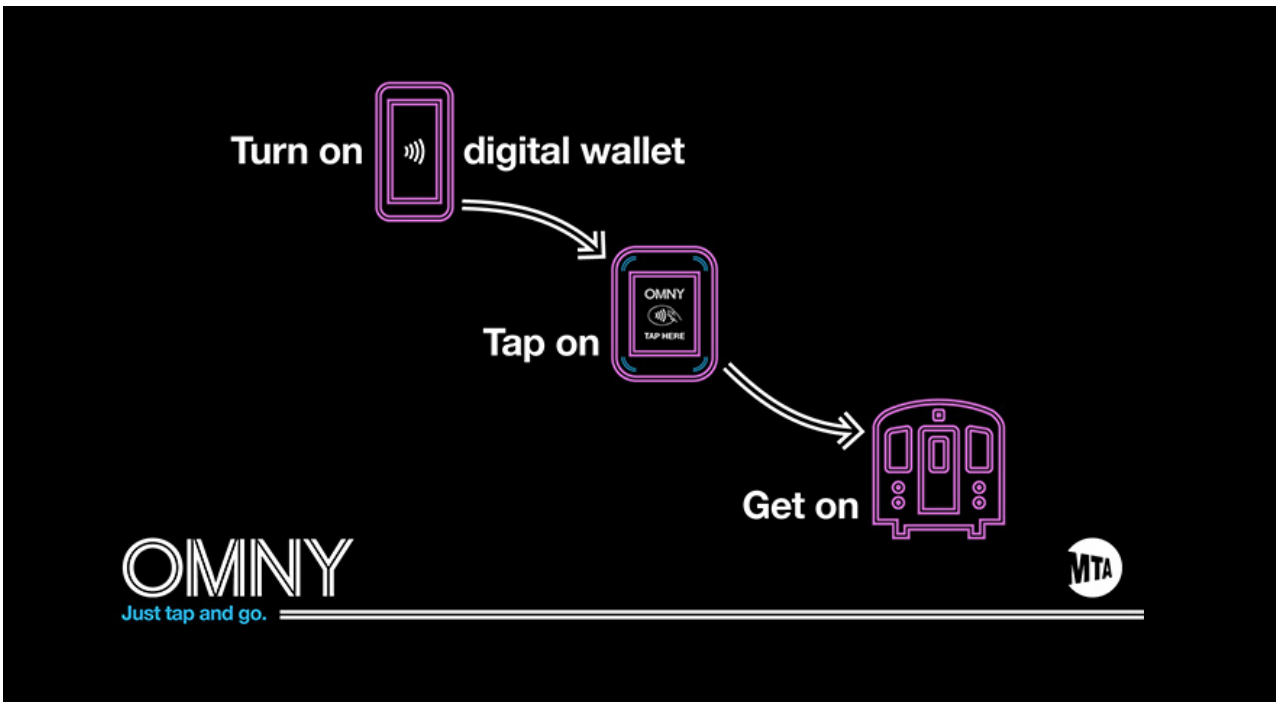
Despite frequent overlap, these two branches pose separate challenges and require different solutions.

Managing Public Sector Personal Data Collection

Concerns related to public sector collection of passenger data are associated with broader and well-known privacy concerns regarding government surveillance and social control. Privacy advocates argue that the government's collection of personal data is a method for promoting conformist behavior, as individuals fear scrutiny, judgment, and retribution for acting outside accepted norms. While these concerns have often focused more on internet activity, mobility data is also particularly sensitive and deeply revealing about an individual's activities. The United States Supreme Court writes that time-stamped location data "provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[4]

For transit agencies, there is a strong public interest in using mobility data to understand how passengers use the transit system, which informs decisions about how to allocate service. Privacy issues arise, though, when other government entities can access the data that

4 Williams, J., Cyphers, B., & Sheard, N. (2019, April 3). *Urgent Concerns Regarding the Lack of Privacy Protections for Sensitive Personal Data Collected Via LADOT's Mobility Data Specification.* Electronic Frontier Foundation, 3. https://www.eff.org/document/eff-oti-letter-urgent-concerns-regarding-lack-privacy-protections-sensitive-personal-data



transit agencies collect. In New York, for instance, organizations like the Surveillance Technology Oversight Project (STOP) highlight the risk of allowing MTA travel data to be accessed by NYPD and, in turn, Immigration and Customs Enforcement (ICE): "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 [the fare payment system] OMNY could compromise a rider's right to anonymous public speech and association."[5]

This tracking is already possible with the MTA's MetroCard system, but the MTA estimates that the process of retrieving personal information can take up to two weeks. With OMNY, the process is near-instantaneous, introducing the possibility of real-time social controls.[6]

The impulse to use transit to restrict people's movement and limit collective expression is well-documented in the U.S. and abroad. During Hong Kong's 2019 pro-democracy demonstrations, the Mass Transit Railway (MTR) closed metro stations in close proximity to where protestors were gathering, and protestors began paying for transit trips with cash for fear of the government tracing their involvement using transit data.[7] Closer to home, multiple cities shut down transit access to areas where people exercised First Amendment rights during 2020's Black Lives Matter protests.[8] While those limitations were imposed without access to personal travel data from open-loop systems, that transit access was curtailed in order to restrict movement is concerning. Transit agencies and regulators should take steps to prevent data from open-loop systems leading to more intrusive surveillance and control of individual travel.

How can travel data from new fare payment systems serve the public's interest in responsive transit planning while preventing that data from being misused by other government agencies? Ultimately, better federal regulation of data privacy similar to the European Union's General Data Protection Regulation (GDPR) is needed to ensure that transit data is used only for transit-related purposes.[9] Until that time, however, transit agencies must recognize their role in generating and collecting personal mobility data, as well as how that data might be abused. This responsibility extends to the more recent development of open-loop payment systems, through which private companies will gain greater access to transit users' personal mobility data.

5 Surveillance Technology Oversight Project. (2019, October 1). *OMNY Surveillance Oh My: New York City's Expanding Transit Surveillance Apparatus*. Urban Justice Center, 6.

6 Metropolitan Transportation Authority, Cubic. Presentation at TransitCenter.

7 Hui, M. (2019, June 13). *Why Hong Kong's protesters were afraid to use their metro cards*. Quartz. https://qz.com/1642441/extradition-law-why-hong-kong-protesters-didnt-use-own-metro-cards/

8 MilNeil, C. (2020, June 4). *How T Closures Escalated Post-Protest Tensions*. StreetsblogMASS. https://mass.streetsblog.org/2020/06/04/how-t-closures-escalated-post-protest-tensions/

9 California's California Consumer Privacy Act (CCPA) is a statewide privacy law similar to the GDPR. State legislation can serve as an important stopgap measure, but federal policy ensures consistent application, particularly for agencies with service areas that span multiple states.

10 Fitzsimmons, E. (2019, July 30). *So Long, Swiping. The 'Tap-and-Go' Subway is Here*. The New York Times. https://www.nytimes.com/2019/07/30/nyregion/metrocard-mta-subway-discontinued.html

11 OMNY is expected to be available on all buses throughout the system as early as 2021.

12 As of writing, the *only* way to use the OMNY system is with open-loop payment devices, such as NFC-enabled credit cards and smartphones, because physical OMNY cards are not yet available. Once the agency issues its own passes, the physical OMNY cards will function similarly to the existing MetroCards with regard to data collection.

Case Study

MTA and OMNY

The MTA is currently transitioning to an open-loop payment system (OMNY) from a closed-loop payment system (MetroCard). Both systems were developed by Cubic, which the MTA contracted with to launch MetroCard in 1993.[10] Both MetroCard and OMNY function as *gated systems* that require passengers to swipe or tap into the system using a payment device. To board a bus, passengers can swipe their MetroCard or pay with cash by dropping exact change into the farebox.[11] But to access the subway system, users must have a MetroCard, which are available for purchase at ticketing machines and kiosks using cash or bank cards. If a passenger purchases a MetroCard using cash, then no personal data is collected. The agency can track the MetroCard's movements throughout the system using the card's unique ID, but cannot see who used it. If the passenger purchases a MetroCard using a credit or debit card, however, then the agency can associate the MetroCard's movements with a specific individual: the original purchaser.

The same will be true of OMNY once physical cards are available. The agency can track the personal information of OMNY cards that were purchased with credit or debit cards but cannot do so if the OMNY card was purchased with cash. One difference between MetroCard and OMNY—between closed-loop and open-loop—is that in closed-loop systems the private companies providing credit card services only process transactions when the MetroCard is purchased or refilled, which may only happen once per month and in fewer locations. OMNY, meanwhile, processes a transaction each time a passenger uses an open-loop payment device to tap into the system, consequently creating many more data points for private companies.[12]

Managing Private Sector Data Collection

Transit data collected through fare payments can contribute to a larger card-data economy, through which private companies can create incredibly detailed profiles of individuals' personal lives, behaviors, and preferences—all through consumers' purchasing histories. Tech journalist Geoffrey Fowler tracked his purchase of a single banana at Target and found that "six types of businesses could mine and share elements of [his] purchase, multiplied untold times by other companies they might have passed it to."[13] While transit agencies cannot be held responsible for the lack of federal regulation that permits this ready exchange of personal data between private companies, they need to understand the role that their fare payment systems play in the monetization and exchange of their riders' data.

It is helpful to understand what data is generated during each fare payment transaction and who exactly is able to capture this data. Payments expert Stephen Cho describes the "four-party payment systems" regime that is dominant in the United States.[14] These four parties are: 1) the cardholder, 2) the merchant, 3) the card issuer, and 4) the merchant acquirer. In transit, parties 1 and 2 are nearly always the passenger and the transit agency, respectively. The card issuer is the financial institution or bank that has issued the credit or debit card. And the merchant acquirer is "a financial institution that enrolls merchants into programs that accepts cards." When a passenger (party

13 Fowler, G. (2019, August 26). *The spy in your wallet: Credit cards have a privacy problem*. The Washington Post. https://www.washingtonpost.com/technology/2019/08/26/spy-your-wallet-credit-cards-have-privacy-problem/

14 Cho, S. (2015, April 9). *Deciphering the payments stack*. Medium. https://medium.com/@stephenjcho/deciphering-the-payments-stack-efbcb9c8eac4

Public transit is one of many pieces in the broader data privacy and card-economy puzzle. Yet transit agencies are in a uniquely difficult position among government entities in that they straddle a line between public service and profit-oriented business.

1) accesses the transit system using an open-loop payment device, each of the other parties collects data on that transaction.

Once the private companies have collected the data, United States privacy law—in particular, the Gramm-Leach-Bliley Act—imposes few restrictions on how they analyze, share, sell, or otherwise use it. The American Civil Liberties Union (ACLU) warns that "companies could be collecting a vast amount of detail about our lives: how much we spend on travel, restaurants, political or religious donations, liquor stores, sex shops, and on and on," adding, "that kind of information is more powerful and revealing when combined with other data."[15] Open-loop payment systems potentially offer private companies more detail on not just "how much we spend on travel," but when and where we travel, as well.[16]

As with concerns about the public sector and social controls, private companies can use this information to direct consumer spending, target and prey on certain demographic groups, and monetize one's life in a manner that they are not complicit with. ABC News has reported that, in at least one instance, a credit card company used "behavioral scoring" to lower a man's credit limit "because *other shoppers* at certain stores he patronized had proven to have poor credit records."[17] Similarly, the marketing firm Affinitiv Inc. "develops scores by crunching data on things such as previous car purchases, whether a household has a teenager, where else a person has shopped and zip codes, which can be used as a proxy for income."[18] This type of consumer scoring—by credit card companies or by other firms that have purchased card data—can clearly lead to a disparate racial impact when factors like zip codes and income are considered.

Public transit is one of many pieces in the broader data privacy and card-economy puzzle. Yet transit agencies are in a uniquely difficult position among government entities in that they straddle a line between public service and profit-oriented business: few other government agencies interact with the public so frequently. If someone has a negative experience at the DMV, the inconvenience is relatively small because it will be months or years before they next need to visit the DMV. For people who rely on public transit, though, transit is a daily necessity. Transit agencies are motivated to provide the best experience for their passengers because they take pride in good service, and also because they must compete with other modes for their passengers' patronage. Pressure to modernize payment systems derives from the imperative to improve the passenger experience, but in the process agencies must respect passenger privacy.

15 Stanley, J. (2019, August 13). *Why Don't We Have More Privacy When We Use A Credit Card? ACLU Speech, Privacy, and Technology Project.* https://www.aclu.org/blog/privacy-technology/consumer-privacy/why-dont-we-have-more-privacy-when-we-use-credit-card

16 Presently, open-loop systems in Chicago and New York City only process that a transaction occurred and the transaction's time. Private companies are not able to view any location data: in other words, where exactly the transaction took place. However, it is unclear if the technology prevents the exchange of the location data or if agency policy prevents the exchange. If the latter is true, then this policy should be codified and communicated to prevent a future policy change.

17 Stanley, J. (2019, August 13). *Why Don't We Have More Privacy When We Use A Credit Card?* ACLU Speech, Privacy, and Technology Project, emphasis in original.

18 Safdar, K. (2018, November 1). *On Hold for 45 Minutes? It Might Be Your Secret Customer Score.* The Wall Street Journal. https://www.wsj.com/articles/on-hold-for-45-minutes-it-might-be-your-secret-customer-score-1541084656

Transit agencies can limit the data made available to other government entities (and themselves) through policy that limits how long data can be retained, after which it is deleted permanently.

Protecting Passenger Data: Collection and Anonymization

Several strategies are available to transit agencies as they seek to better protect passenger data: 1) eliminating "privacy taxes" and empowering passengers to make an informed choice when choosing their fare media; 2) anonymizing and aggregating the data that *is* collected; "3) transparently and clearly communicate fare data privacy practices; 4) designing fare payment systems that collect less personal data in the first place.

Eliminating Privacy Taxes

Cash is the most secure and private fare payment medium, either when used to board the bus or when purchasing and refilling an agency-issued fare card. It is much more difficult to connect a specific fare card's movement to an individual passenger when the passenger originally paid for the card using cash.[19]

Because paying fares with currency can slow down service and increase fare collection costs compared to other payment methods, some agencies introduce incentives to pay with cards. For instance, free transfers may not be available when riders pay with currency. Advocates refer to a penalty for paying with cash as a "privacy tax."

Agencies making the switch to open-loop payment should strive to eliminate privacy taxes. Refilling a card with cash should entitle riders to the same fare value as using credit. And agencies need to ensure that a cash payment option remains accessible throughout the system as open-loop payment systems are introduced. Encouragingly, the MTA has promised to expand its network of sales partners to make agency-issued OMNY cards available for cash purchase in neighborhood stores throughout the city.[20]

Managing Data Securely

Privacy advocates like the Electronic Frontier Foundation (EFF) and STOP have outlined ways agencies can manage data more responsibly. One is simply by developing "clear policies on use, retention, deletion, and access/sharing."[21] Advocates believe that data collected for the purpose of providing transit service—be it for customer service like when a transit user loses their monthly pass, or for planning bus routes based on ridership patterns—should be used *only* for that purpose. It is unfortunately unclear what transit agencies can do to prevent other

19 Again, this is because in order to process the credit or debit card transaction, the agency collects the personal information associated with that card.

20 Metropolitan Transportation Authority, Cubic. Presentation at TransitCenter.

21 Williams, J., Cyphers, B., & Sheard, N. (2019, April 3). *Urgent Concerns Regarding the Lack of Privacy Protections for Sensitive Personal Data Collected Via LADOT's Mobility Data Specification.* Electronic Frontier Foundation, 2.

government entities from accessing the data for non-transit purposes.

Agencies can, however, commit to not sharing data with any private companies.[22] Transit agencies can also limit the data made available to other government entities (and themselves) through policy that limits how long data can be retained, after which it is deleted permanently. STOP points out that OMNY's privacy policy "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."[23] Even for service planning purposes, transit agencies have little reason to store granular transit data much longer than one year.

Anonymizing and aggregating data is a promising strategy for agencies that want to use—and even share—transit data for transportation planning purposes. Researchers at the Metropolitan Transportation Commission (MTC) in San Francisco sought to create a "data product" from fare payment transaction data that could be shared between the San Francisco Bay Area's 20 separate transit providers and even with interested private sector companies. For the MTC, "the highest value aspect of the Clipper [fare card] transaction data is individual trajectories through the transportation network."[24] In other words, MTC planners wanted to understand individual riders' origin-destination data over time.

MTC's anonymizing scheme:

- Separated all personally identifiable information from the database
- Replaced fare cards' unique ID with a "pseudo-random identification field that persists for one…day"
- Selected a sample of 50 percent of unique cards for each day
- For each day of the week, randomly selected only three of the four or five possible days in which that weekday had occurred that month
- Replaced each date with a unique, random number
- Truncated each timestamp to the nearest 10 minutes

However, when soliciting feedback on the final product from internal and external users, MTC staff found that the anonymization scheme had limited the datasets' usability for planning purposes. In particular, planners wanted to see trends over more than just 24 hours or on days that saw special events, data points that were lost in the anonymization process. If more attention is paid to data privacy in fare payment, further research could continue to refine the anonymization process while maintaining more of the usability found in the original data set.

22 An exception to this is private companies that assist agencies with service planning, such as consultants or software providers. Still, agencies can include in contracts language that prevents from these companies from using the data except for their engagement with the agencies' service planning.

23 Surveillance Technology Oversight Project. (2019, October 1). *OMNY Surveillance Oh My: New York City's Expanding Transit Surveillance Apparatus*. Urban Justice Center.

24 Ory, D. & Granger-Bevan, S. David Ory. (2016, September 25). *A Functioning Beta Solution to the Challenge of Opening Transit Payment System Transaction Data*. Bloomberg Data for Good Exchange Conference. New York City, NY, USA. https://arxiv.org/pdf/1609.08757.pdf

Transparency and Clear Communication

Agencies should clearly communicate their fare data management practices to passengers, and explain how fare payment choices affect the collection of personal data. Good privacy practices and transparency about data management can build public trust in a new fare payment system.

Organizations typically convey this information to users by posting privacy policies posted on their websites. Unfortunately, privacy policies are often written in jargon that's hard for people to digest. The Center for Internet and Society's Jen King calls such policies "documents created by lawyers, for lawyers."[25]

Transit agencies' privacy policies are no exception. For example, based on the Flesch-Kincaid scale—a common measure of readability—OMNY's policy would score at the 15th Grade Level, meaning it's about as readable as Steven Hawking's *A Brief History of Time* or an academic paper.[26] The CTA's Ventra privacy policy is similarly complex, but the CTA provides simple summary bullets at the top of the webpage.[27] Other agencies might adopt this practice and expand it to include some of the information in this brief (e.g. which law enforcement agencies can access the data without the users' knowledge, or that filling a fare card with cash prevents personal information from being shared).

Agencies should also guide passengers to their privacy policies through marketing materials and signage throughout the system. One of the concerns about tap-and-go, NFC payment systems is that they smooth the payment process but do not give users the opportunity to understand or opt out of the privacy policy to which they've implicitly agreed when they tap into the system. Signage at entrances, in stations, and aboard vehicles can alleviate at least some of these concerns by informing passengers as to where they can access the agency's privacy policy. QR codes posted at turnstiles can link passengers to the privacy policy using the same smartphone that they are about to tap with. For agencies seeking to assure riders that they can protect personal data, honesty and openness are the best policy.

Secure Alternatives in Fare Payment

Finally, transit agencies can pursue fare payment systems that collect less passenger data by design. Proof-of-payment fare validation systems, where passengers show an inspector a receipt to demonstrate they've paid the fare, potentially generate less location-specific data than gated systems. Proof-of-payment

25 Litman-Navarro, K. (2019, June 6). *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster.* The New York Times. https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html

26 Kelly, L. (2020, November 10). The Flesch Reading Ease and Flesch-Kincaid Grade Level. The Readable Blog. https://readable.com/blog/the-flesch-reading-ease-and-flesch-kincaid-grade-level/

27 Chicago Transit Authority. (2017, December 18). *Your Privacy & Ventra.* https://www.ventrachicago.com/privacy-policy/#:~:text=You%20can%20use%20the%20Ventra,live%20in%20a%20secure%20facility.&text=The%20data%20we%20collect%20helps,services%20and%20to%20provide%20support.

Based on the Flesch-Kincaid scale—a common measure of readability—OMNY's policy would score at the 15th Grade Level, meaning it's about as readable as Steven Hawking's *A Brief History of Time* or an academic paper.

systems face separate challenges, such as the potential for unequal enforcement due to racial profiling, but offer a more secure experience when executed correctly.

Unfortunately, when agencies stop collecting this movement data with swipes and taps, they lose a valuable resource for service planning. The most difficult data to replace is origin-destination data, which is particularly important for designing service that is responsive to where passengers need to go. Surveys are a viable alternative to constructing this origin-destination data. Most agencies already conduct surveys, especially for data that is hard to collect through farebox data alone. Replacement data sources can be found for other important service planning metrics, too: Automatic Passenger Counters (APCs) can be used to calculate load on buses and trains in lieu of farebox data.

Conclusion

Open-loop payment systems offer tremendous potential in streamlining fare payments for passengers and agencies alike. And many agencies that are not yet moving to open-loop payment are nonetheless turning to third-party private companies to support their fare payment and service operations, especially through mobile applications. However, the increased involvement of third parties in fare payment underscores the need for better data collection and management policies within transit agencies. Through proactive measures, transit agencies can set the stage for protecting passenger data even as new technologies emerge.

TransitCenter

@transitctr
@TransitCenter
@transitcenter_

TransitCenter
One Whitehall Street
17th Floor
New York, NY 10004