SJSU SAN JOSÉ STATE UNIVERSITY

MTI MINETA TRANSPORTATION INSTITUTE

Personal Data Protection as a Driver for Improved Cybersecurity Practices in U.S. Public Transit

Project 2113-WP2
December 2021

Katie Seckman, Harlan Belcher, Scott Belcher, JD, MPP, and Brandon Thomas

A key responsibility for any organization beyond safely delivering a high-quality service or product is the protection of the personal information and identifiers of the people associated with the organization. For public transit providers, most of the personal information they collect or retain for business purposes is from employees, and with ever-increasing detail and specificity, on customers.

Efforts to modernize public transit and provide better, more efficient services to passengers are facilitated in part by the collection of information about who, when, where, and how transit services are being used across cities. Expanding data collection, however, increases the importance of having robust and secure data management and privacy practices in place—something lacking in many U.S. transit agencies.[1] An uptick in cyberattacks, including ransomware attacks, against public transit agencies further underscores the importance and increasing responsibility transit agencies have to prioritize the protection of any personal data they collect, retain, or distribute.

> *I asked how he figured out how to hack the world's most protected networks. "It's easy," he told me. "They never anticipated they would be attacked."*[2]
>
> **-Nicole Perlroth (*New York Times*) speaking to Argentine hacker, Alfredo Ortega**

Ultimately, transit agencies will be held to account just as any other business will be—regardless of industry—for the security of the data they collect, process, and leverage for service delivery or other purposes. A failure to protect personal data in the process not only has a direct impact on the data owner, but it can also have a material impact on an agency's operations, finances, compliance status, and reputation. Fortunately, with the institution of comprehensive enterprise risk management plans, agencies can establish and mature cybersecurity policies and practices that will allow them to both collect data to inform business improvements and protect the personal information of their customers and employees.

Increasing Data Collection Capabilities in Public Transit

The opportunity to collect and process data from vehicles and customers in public transit has never been greater. Technology developments in fare management, GPS vehicle tracking, route mapping, and other mobile applications all offer new data collection tools that can help inform business operations, specifically creating a better understanding of the agency's customers, and facilitating more effective service delivery. After, or as part of the data collection process, the data's full utility can only be realized once it has been engineered (the process of turning myriad pieces of data into useable information) and subsequently analyzed (the process of interpreting the data once it is put in a useable format). With appropriate data management and security plans

in place—most likely with assistance from third-party vendors and technicians—transit agencies can leverage data collection to the benefit of their customers, business operations, and in support of overall service delivery.

Among these new data gathering opportunities is information that—in the wrong hands—could be used to the detriment of an individual or group of people. The theft and sale of personally identifiable information (PII) has a robust marketplace, often referred to as the dark web, and can be quite lucrative. Gaining access to sensitive PII or a collection of data points that, when linked, provide a detailed profile of an individual can facilitate everything from fraudulent purchases to identity theft to illegal monitoring.

Personally Identifiable Information (PII)

The definition of what constitutes personal data in the United States varies almost as much as the types of data points. Most common among them, however, is the definition provided by the U.S. National Institute of Standards and Technology (NIST) at the U.S. Department of Commerce.

Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means.[3]

Subsequent definitions from NIST and other data privacy bodies generally include additional examples of PII, such as name, home address, social security number, email address, geolocation data, biometric records, internet browsing history, purchase history, and fingerprints—to name but a few.

Fare Payment

The shift in fare payment systems from tokens and tickets to digital wallets and contactless credit cards creates a windfall of useful data for agencies and their fare payment vendors, but also ups the ante in terms of data protection and the types of PII that can be exposed in a system breach. The nonprofit advocacy group Surveillance Technology Oversight Project and the TransitCenter, an organization focused on making public transit more "just and environmentally sustainable"[4] have both weighed in on the data privacy risks of new "open-loop" payment systems that connect the identity of the transit customer with the specifics of their travels in real time.[5]

The convenience of these new open-loop payment systems is unmistakable, and consumers are growing increasingly accustomed to a simple tap of their phone or credit card to make a purchase. It only makes sense that this convenient and time-saving payment system—already being used by major transit providers in New York, Boston, Houston, and Washington, DC—would see greater uptake by transit agencies around the country. Agency privacy policies and cybersecurity practices must keep pace. Keeping pace in this instance, however, does not mean that a transit agency is doing well in its information security practices relative to other transit agencies (where there is a lot of room for improvement across the board). It means reaching a level of maturity on par with the threat landscape, which, in the realm of open-loop payments, is industry agnostic.

The processing and safe-handling of customer financial information is regulated by Payment Card Industry Data-Security Standards (PCI DSS), whether the data is handled by the transit agency directly or a third-party vendor. Most transit operators contract out the handling of fare payment data to third party vendors that are generally better qualified to handle it and meet PCI compliance requirements. A failure to meet these standards can result in fines from the individual creditors (*i.e.,* Visa, Mastercard, Discover, AMEX, and JCB Int.) that comprise the PCI Security Standards Council (PCI SSC).

Open-loop Versus Closed-Loop Payment Systems in Transit

Open-loop mobile payment systems allow users to pay for goods and services at multiple vendors using a single digital wallet or credit/debit card that gets processed by the regular card payment system and shows up on the customer's monthly statement (*e.g.,* Visa, Mastercard, AMEX, Apple Pay, and Google Pay).

Closed-loop payment systems only allow for payment at a specific vendor and often involve linking a personal credit card with a vendor account (*e.g.,* reloadable transit cards issued by the transit network, Starbucks app, and gift cards).

PCI DSS compliance is comprised of 12 requirements ranging from firewall use and maintenance to data encryption to restricted data access. PCI compliance is essential for agencies and vendors and should be part of a larger enterprise risk infrastructure capability covering multiple forms of data. Weak organizational security controls—sometimes still within the basic compliance parameters of PCI DSS—can allow hackers to access valuable credit card information, something Verizon Visible, Neiman Marcus, and Volkswagen customers in the United States experienced in 2020 and 2021.[6] Meeting security standards for the protection of payment processing seems like a basic compliance requirement for most businesses, including transit vendors. Verizon's release of its 2020 Payment Security Report suggests that PCI DSS compliance among organizations is actually decreasing, an observable trend beginning in 2016. Less than 28 percent of organizations assessed in 2019 were 100% PCI compliant, according to Verizon, a drop in nearly nine percentage points from 2018 and 28 percentage points from 2016.[7] Even if an agency is outsourcing fare management and associated PII protections to vendors that are comparatively better equipped to protect the data, transit agencies should seek continued verification that their vendors are maintaining their PCI DSS compliance.

Location Data

Information on who uses public transit at a given location at a specific time is valuable data for any agency looking to refine service offerings. As with other forms of PII, the ability to construct a detailed accounting of an individual's movements over the course of multiple days or months is of interest to everyone from marketing agencies and advertisers to law enforcement and policymakers. Location data—like payment information—generates an intimate look at how people spend their time, with whom, and how they move through the world.

The Electronic Frontier Foundation (EFF) and other privacy advocates have taken issue with the detailed individual trip data being collected by local transportation planning agencies, most notably with regard to shared mobility devices like bikes and scooters.[8] EFF, the Open Technology Institute, and the Center for Democracy and Technology in 2018 and 2019 called out the Los Angeles

Department of Transportation (LADOT) for its data sharing requirements for shared mobility services that included giving LADOT access to detailed location data. EFF and others argued that LADOT did not have a comprehensive data management or privacy protection plan to adequately protect the raw trip data LADOT was requiring bike and scooter companies to provide. Uber and the American Civil Liberties Union (ACLU) subsequently sued LADOT because of the department's Mobility Data Specifications (MDS). LADOT prevailed in both cases (winning on appeal in 2020 against Uber and in a 2021 dismissal of the ACLU suit) and is now expanding its MDS to the taxi sector.[9] In addition, the Open Mobility Foundation has taken over stewardship of MDS as an industry-wide specification, promoting its use for broad application across the United States.

Although recent lawsuits have focused on mobility services, the conversations around location data collection and use—especially in concert with other types of PII—are more broadly applicable to the public transit sector and merit ongoing attention. The specific vehicle location data gleaned from cameras on the exterior of public transit vehicles (*e.g.,* license plate numbers gathered for automated enforcement purposes), for example, also has potential PII data protection implications.

Facial Recognition

Video surveillance on public transit is by no means new. Agencies rely on video footage from their vehicles and at stations to monitor customer and employee safety, for incident response, and as evidence in legal proceedings (*e.g.,* accidents, physical altercations and as evidence in crimes). Widely available facial recognition software allows for the augmentation of such surveillance. The use of facial recognition software to ascertain someone's identity in real time or via photo or video is increasingly making an appearance in public transit systems around the globe. China actively allows users to pay for public transit through scans of their face, and the Moscow and Seoul metro systems currently have ongoing pilot programs. Leadership of the Bay Area Rapid Transit (BART) system in California expressed an interest in 2018 in exploring the potential use of facial recognition technologies to help address security concerns, which prompted an outcry from privacy advocates.

How facial recognition is used by public and private entities, most notably law enforcement, and the well-documented shortcomings of the technology in accurately identifying an individual create several reasons why transit agencies should pursue such potential data collection with extreme caution.[10] Biometric data, especially when combined with other personal data points, constitutes PII and introduces additional levels of complexity to data management. Still photographs, for example, are not PII on their own. When run through facial recognition technology software, however, those photos become biometric data.[11]

A patchwork of state and local laws governs the collection and use of biometric data, something with which any agency considering facial recognition needs to be well versed. Maine, California, Virginia, Washington, San Francisco, and Portland are some of the states and cities that are specifically banning or severely limiting the use of facial recognition technologies by government agencies. Only five states—Georgia, Kansas, Michigan, Missouri, and South Dakota—do not have existing or pending legislation aimed at regulating biometric information privacy.[12] There are efforts at the federal level to limit public spending on biometric surveillance tools, including facial recognition, but they have yet to gain the necessary bipartisan support to advance.

Employee Records

A failure to adequately secure employee data and records places large troves of PII at risk of exploitation by nefarious actors. The global transit industry has experienced a 186% year-over-year increase in weekly ransomware attacks since June 2020, according to Check Point Research.[13] Employee social security numbers, bank information, and passport numbers are among the data that the Forward Air Corporation failed to secure in a December 2020 breach of its systems, much like the ransomware attack experienced by Vancouver's TransLink in the same month. Colorado-based short line rail operator OmniTrax also experienced a system breach after hackers targeted its parent company, the Broe Group. Audio equipment manufacturer Bose, Indianapolis-based Eskenazi Health, and fashion company Guess are among the many companies in 2021 dispatching notifications to current and former employees that sensitive employee PII was stolen during system breaches and posted on the dark web for purchase—and these are not even the attacks that grabbed headlines in 2021. The latest reported breach in the transit sector occurred in late October 2021 when hackers accessed the sensitive personal data of 25,000 past and present employees at the Toronto Transit Commission.[14]

RANSOMWARE ATTACK
TransLink, Vancouver, Canada
December 2020

A ransomware attack hit TransLink, which shut down some modes of payment for customers, including any non-cash form of payment at ticketing kiosks and left the transit agency without the capability to track their buses via GPS well into 2021. Based on the ransom letter received via TransLink's printers, the perpetrator was identified as the Egregor ransomware gang, a group known to sometimes publish stolen information even after a ransom payment. TransLink did not pay the $7.5M ransom because of this risk.

The hackers accessed sensitive personal data on some current and former employees, as well as some employees' spouses. Information included:

- Banking information
- Social insurance numbers
- Other personal identifiers related to payroll and benefits administration
- Scans of personal checks written to purchase taxi passes for individuals using the Access Transit Program—TransLink's disability support services. Family or care providers often write these checks on behalf of Access users.

The drive accessed in the breach contained personal information of current, past, and retired employees of TransLink, Coast Mountain Bus Company, BC Rapid Transit Company, West Coast express, and the Transit Police. Litigation against TransLink by current and former employees is ongoing.

Transit agencies—like any employer—must ensure that their employees can be confident that their personal information is secure. The types of PII an employer maintains on their employees can include everything from basic identity and banking information to healthcare records (especially if the company requires medical exams or drug/alcohol testing) and biometric information. A failure to protect this information not only violates trust between the employer and its employees but also opens the employee up to potential harm (*e.g.,* identify theft) and the company up to lawsuits (as TransLink is currently facing). For agencies with a union-represented workforce, the protection of employee PII could face additional scrutiny during collective bargaining.

Patchwork of Data Privacy and Security Regulations

The regulatory environment in the United States governing the protection and use of PII by public and private entities and an individual's right to control by whom and how their personal data is used is a patchwork at best. There are 17 countries with comprehensive national data protection laws in place—the United States is not among them.[15] As more countries enact laws governing the data of their residents, U.S. entities are going to face an increasingly complex process of navigating extra-territorial and data export requirements. In short, most countries with laws like the European Union's General Data Protection Regulation (GDPR)—a groundbreaking 2018 consumer data privacy and security law—require that their residents' data be processed in a GDPR-compliant manner (read strict data protections) and that the data can only be exported to locations with similarly robust data protection rules.

Data privacy regulation at the federal level in the United States is generally limited to a few key pieces of legislation—healthcare information via the Health Insurance Portability and Accountability Act (HIPAA), consumer financial products via the Gramm-Leach-Bliley Act (GLBA), efforts to protect children under 13 using the internet via the Children's Online Privacy Protection Rule (COPPA), and a handful of other narrow regulations. Otherwise, as cited previously in this White Paper, most digital privacy rights are being crafted at the state level, with California's Consumer Privacy Act (CCPA) as the leading model (see the Privacy Glossary in the Appendix for more details on CCPA). This increases the importance for transit agencies to have a clear picture of the types of data they and their vendors collect, process, and retain, what protections are in place, and the ability to comply with local and state rules potentially governing

HIPAA and Paratransit Services

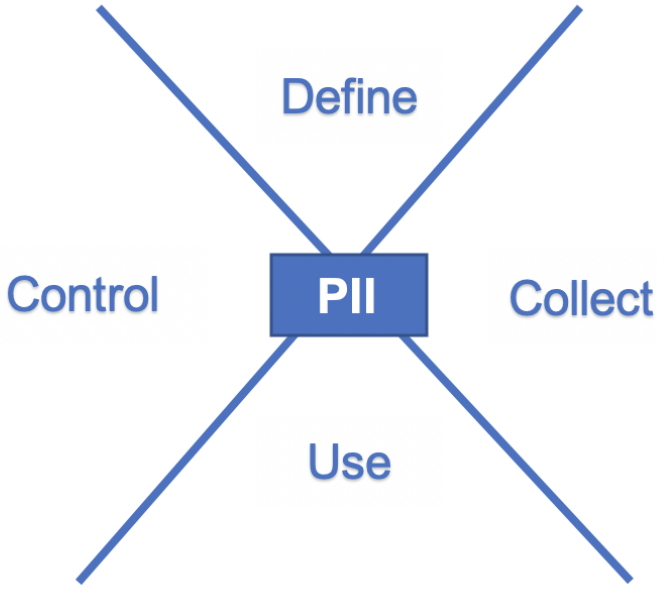
Agencies that provide paratransit services often collect PII on customers through the application and verification process. Medical documents and attestations, identity and location information, and requests for specific transit services are among the sensitive data agencies often retain or share with vendor partners enabling coordination and delivery of services.

The applicability of the Health Insurance Portability and Accountability Act's (HIPAA) privacy and security rules to transit providers is an ongoing legal debate, with a 2014 Legal Research Digest study finding that these rules generally do not apply to transit.[16] Researchers and industry experts do agree, however, that a failure to protect such data will most likely open a transit agency up to legal challenges regardless of HIPAA applicability or the presence state statutes governing health information.

this information (especially if data is stored outside the state in which it is being collected, via a vendor relationship, for example).

As the U.S. Government pays increasing attention to the cyber vulnerabilities at public and private companies alike, the authors expect more federal and state guidance—if not laws—to pass in the coming years. The Transportation Security Administration in October 2021 issued a directive specifically outlining new cybersecurity mandates for railroad and rail transit systems in an effort to shore up the security of critical transportation infrastructure across the country. The authors expect these same provisions to be rolled out to large transit providers in short order. Among the new mandates are requirements that companies designate and name a cybersecurity point person at their organization, that any cyber incidents be reported to the Department of Homeland Security in a timely manner, and that the organization have an incident response plan in place.[17] In addition, the Biden Administration is expected to take a more active role in establishing federal policy in this area, as evidenced by the July 2021 *Executive Order on Promoting Competition in the American Economy,* in which the Administration encouraged the Federal Trade Commission to establish rules that regulate "unfair date collection and surveillance practices that may damage competition, consumer autonomy, and consumer privacy."[18]

Taking Steps to Protect PII



Transit agencies need to have a comprehensive understanding of the PII they have within their data ecosystem—including data collected from transit users by third-party vendors. How this information is collected, used, stored, and shared needs to be assessed, included in policies and procedures, and accounted for in regular security reviews.

The ability to protect sensitive personal information collected by transit agencies and their vendors starts with the overall enterprise risk and security practices of the organizations. There are multiple resources available to transit providers to help them on this journey, including from the Cybersecurity and Infrastructure Security Agency (CISA) and the American Public Transportation Association (APTA).[19] As a component of enterprise risk management policies and practices, transit agencies and their vendors need to ensure that PII is adequately accounted for and managed within their respective systems. Some important steps in protecting PII include:

1. Define PII for your organization and identify existing data that falls within these parameters already collected and stored by the organization

2. Review the types of information being collected, how it is used, and whether the use case is worth the risk of storing the data

3. Articulate the organization's privacy policies in accordance with local, state, and federal laws, business needs, legal ramifications, and customer data privacy interests

4. Ensure proper controls are in place, per agency cybersecurity policies and protocols, to limit internal and external access to PII

5. If data is managed by a vendor, include data collection, use, and storage requirements in proposal requests and contracts—spell out the expectation that agency vendors must protect transit customer data

6. Ultimately, if the agency does not yet have the cybersecurity capabilities to reliably secure specific data flows, consider forgoing collection until such time that securing it is possible.

Endnotes

1. https://transweb.sjsu.edu/sites/default/files/1939-Belcher-Transit-Industry-Cyber-Preparedness.pdf

2. Perlroth, Nicole. (2021) This is How They Tell Me The World Ends. Pg. 260. Bloomsbury Publishing.

3. https://csrc.nist.gov/glossary/term/PII

4. https://transitcenter.org/about/

5. https://static1.squarespace.com/static/5c1bfc7eee175995a4ceb638/t/5d921e21407e522fcfb42ac0/1569857057595/OMNY+Surveillance+Oh+My.pdf

   https://transitcenter.org/publication/do-not-track-a-guide-to-data-privacy-for-new-transit-fare-media/

6. https://www.cpomagazine.com/cyber-security/attack-on-verizon-visible-confirmed-to-be-a-credential-stuffing-campaign-hacked-accounts-charged-for-thousands-of-dollars-in-purchases/

   https://www.nbcnews.com/tech/security/vw-says-data-breach-vendor-impacted-33-million-people-north-america-rcna1180

   https://www.theverge.com/2021/9/30/22703171/neiman-marcus-hacked-security-credit-cards

7. https://enterprise.verizon.com/business/resources/reports/2020-payment-security-report.pdfx

8. https://www.eff.org/deeplinks/2020/03/unchecked-smart-cities-are-surveillance-cities-what-we-need-are-smart-enough

   https://www.eff.org/deeplinks/2019/04/los-angeles-department-transportations-ride-tracking-pilot-out-control

9. https://cities-today.com/us-court-dismisses-lawsuit-against-las-mobility-data-sharing-requirement/

10. https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/

    https://www.nytimes.com/2019/01/24/technology/amazon-facial-technology-study.html

11. https://www.jdsupra.com/legalnews/biometric-and-facial-recognition-1371482/

12. https://www.foley.com/en/insights/publications/2021/06/developments-biometric-information-privacy-laws

https://www.vice.com/en/article/wjvxxb/san-francisco-bans-facial-recognition-use-by-police-and-the-government

13. https://blog.checkpoint.com/2021/06/14/ransomware-attacks-continue-to-surge-hitting-a-93-increase-year-over-year/

14. https://techcrunch.com/2021/11/10/toronto-cyberattack-employee-data/

15. https://securityscorecard.com/blog/countries-with-gdpr-like-data-privacy-laws

16. https://www.apta.com/wp-content/uploads/Resources/mc/legal/previous/2017legal/synopsis/Documents/Legal%20Research%20Digest%2046.pdf

17. https://www.washingtonpost.com/national-security/rail-cybersecurity-dhs-regulations/2021/10/06/b3db07da-2620-11ec-8831-a31e7b3de188_story.html

18. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/

19. https://www.apta.com/research-technical-resources/safety-security/cybersecurity-resources/

Appendix: Privacy Glossary

Biometric Information Privacy Act (BIPA): Passed by the Illinois General Assembly in 2008, BIPA led the way in promoting consumer data protection by requiring companies that collect or store biometric information or identifiers to inform individuals that such information was being collected, why, and secure a written release from that individual to do so. The disclosure of biometric information without consent is also prohibited. Class action litigation based on the 2008 law increased in recent years, including a February 2021 settlement against Facebook for $650 million.

California Consumer Privacy Act (CCPA): A California law modeled on Europe's GDPR that gives consumers in California the right to control the personal information businesses collect and retain on them, and how such data is used. Under CCPA, which went into effect on January 1, 2020, businesses must give consumers details on their respective privacy practices and comply with consumer requests for details on the types of personal information the business collects, what they do with the data, and abide by consumer requests to opt-out of their sale of their personal information and/or have their personal data deleted. A California ballot initiative passed in November 2020, the **California Privacy Rights Act (CPRA),** amends and expands the CCPA and will not go into effect until July 1, 2023.

General Data Protection Regulation (GDPR): A robust regulation in European Union law governing the data privacy and security of EU citizens with the purpose of giving data subjects greater control over how their personal information is collected, processed, and erased. Any company—regardless of their physical location—processing the personal data of EU citizens or residents must comply with GDPR. Failure to do such results in stiff fines. GDPR affords EU data subjects substantial privacy rights and serves as a framework for other global privacy compliance regulations. GDPR is considered one of the strictest data privacy laws in the world.

Gramm-Leach Bliley Act (GLBA): Also known as the Financial Modernization Act of 1999, the GLBA requires companies that offer consumer financial products or services such as loans, insurance, and investment advice to outline for customers how they manage, share, and protect customers' information. Customers must be given the opportunity to opt-out of having their personal data shared with third parties. The rule covers most personal information and transactional data, including credit reports, bank account numbers, social security numbers, etc.

Health Insurance Portability and Accountability Act (HIPAA): Enacted in 1996, HIPAA is a federal law that created regulatory standards for the use and disclosure of protected health information (PHI). The HIPAA Privacy Rule sets the standards for how entities who use PHI (*e.g.,* healthcare providers, health plans, etc.) handle such information and gives individuals rights to understand and control how their PHI is used. The HIPAA Security Rule protects a specific subset of PHI covered by the Privacy Rule, specifically related to electronic protected health information (e-PHI).

Acknowledgement

The authors thank Lisa Rose, for editorial services, as well as MTI staff, including Executive Director Karen Philbrick, PhD; Deputy Executive Director Hilary Nixon, PhD; Graphic Designer Alverina Eka Weinardy; and Communications and Operations Manager Irma Garcia.

About the Principal Investigator

Scott Belcher is the President and CEO of SFB Consulting, LLC, where he specializes in transportation, transportation technology, the internet of things, smart cities, and the environment. Mr. Belcher serves on a number of public and private advisory boards. Mr. Belcher holds a JD from the University of Virginia, a Masters of Public Policy degree from Georgetown University, and a Bachelor of Arts degree from the University of Redlands in Redlands, California.

This report can be accessed at transweb.sjsu.edu/research/2113WP2

MTI is a University Transportation Center sponsored by the U.S. Department of Transportation's Office of the Assistant Secretary for Research and Technology and by Caltrans. The Institute is located within San José State University's Lucas Graduate School of Business.