Public Transit and PII: A Case for Improved Cyber Practices

MDOT April 2022 Tech Talk

Kathryn Seckman, Grayline Group

MTI MINETA TRANSPORTATION INSTITUTE

GRAYLINE®

Personally Identifiable Information (PII)

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.

-NIST Glossary

Name
Home Address
SSN

Email Address
Geolocation Data
Biometric Records

Internet Browsing History
Fingerprints

GRAYLINE®

Surge in Data Collection Opportunities

Fare Management
-Open-loop system

Medical Data
-Paratransit Services

Location Data
-GPS vehicle tracking
-Route mapping

Facial Recognition
-Fare Payment
-Safety

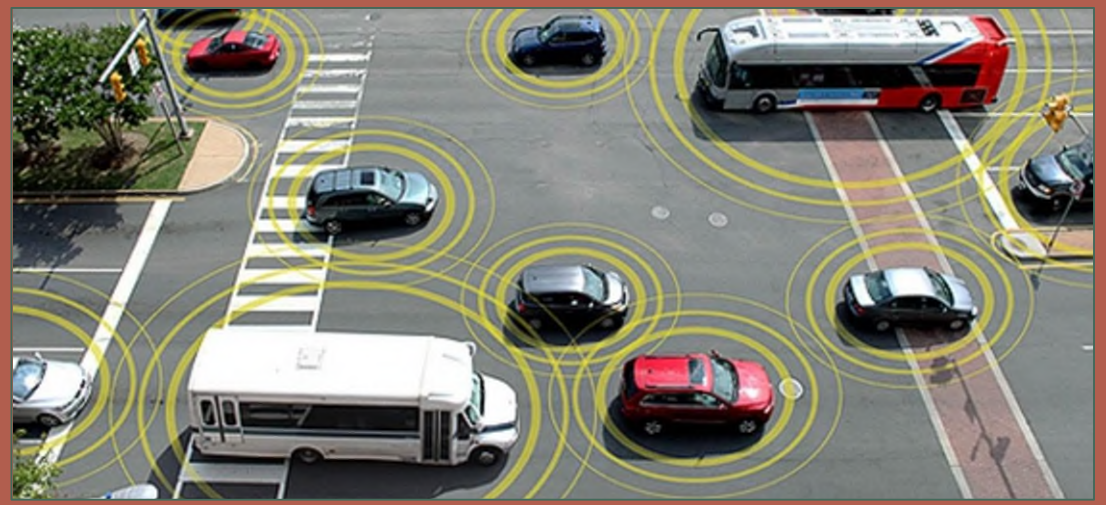
Employee Records
-SSNs, bank info, etc.
-Health plan details
-Drug/alcohol test results

Modernization of Public Transit Includes Benefits from Data Collection

IMPROVED SERVICE DELIVERY, INCLUDING EQUITY

OPERATIONAL EFFICIENCIES

OPPORTUNITIES TO LEVERAGE THIRD-PARTY EXPERTISE



GRAYLINE®

CYBERSECURITY

Honolulu Transit Putting Services Back Online After Hack

Printed ransom note asked TransLink for $7.5 million in December cyberattack

Hackers disrupt payroll for thousands of employers — including hospitals

January 15, 2022 · 5:00 AM ET

NYC officials call for investigation after data of 820,000 students compromised in hack

Transportation

A hard drive with 'vital information' on SEPTA's ransomware attack has been missing for months

Researchers hack Apple Pay, Visa 'Express Transit' mode

RIPTA under fire: Why would a public transit authority have healthcare data?

Best Practices to Protect PII

- Define PII for your organization; identify existing data
- Review PII collection, use, and use/risk calculus
- Document and share the organization's privacy policies
- Ensure data access controls are in place
- Define expectations for third-party management of transit data
- If you can't secure it, don't collect it.

Cybersecurity Resources

- Cybersecurity & Infrastructure Security Agency (CISA)
- NIST Cybersecurity Framework
- FTA Cybersecurity Resources for Transit Agencies
- TSA Surface Transportation Cybersecurity Toolkit
- American Public Transportation Association (APTA)

Additional reading on PII and Transit: **Mineta Transportation Institute,** Personal Data Protection as a Driver for Improved Cybersecurity Practices in U.S. Public Transit, December 2021

Privacy Best Practices and Governance

04-27-2022

Troy Rogers

Federal Transit Administration

U.S. Department of Transportation
Federal Transit Administration

Privacy Best Practices

Safeguard your Personally Identifiable Information (PII)

Safeguarding Personally Identifiable Information (PII) in paper and electronic form during your everyday work activities is paramount to the success of the agencies mission. Employees, contractors, consultants, and detailees are required by law to properly collect, access, use, share, and dispose of PII in order to protect the privacy of individuals doing business with agency.

What is Personally Identifiable Information (PII)

PII is any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to an individual. Some PII is not sensitive, such as that found on a business card. Other PII is Sensitive PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive PII requires stricter handling guidelines. Examples of Sensitive PII include: Social Security number (SSN), driver's license number, financial information, citizenship or immigration status, or medical information, in conjunction with the identity of an individual. In addition, the context of the PII may determine its sensitivity, such as a list of employees with poor performance ratings.

Privacy Best Practices

Safeguard your Personally Identifiable Information (PII)

- Ensure that you have appropriate policies and procedures in place.
- Limit access to only those that have a need to know (ACLs)
- Ensure your system has encryption in place ; in transit and at rest (FIPS 140-2 compliant)
- Have approved Privacy Threshold Analysis (PTA) in place
    - Required for all systems to identify if the system maintains PII
- Have approved System of Records Notice (SORN) in place (if required)
    - A SORN is required under the Privacy Act when federal agencies store and retrieve information by name or a personal identifier from paper records or electronic systems under their control.
- Have approved Privacy Impact Assessment (PIA) in place (if required)
    - The Privacy Impact Assessment (PIA) is a decision tool to identify and mitigate privacy risks that notifies the public what Personally Identifiable Information (PII) DHS is collecting, why the PII is being collected and how the PII will be collected, used, accessed, shared, safeguarded and stored.

Privacy Best Practices

Safeguard your Personally Identifiable Information (PII)

- If you must email PII (not recommended), save it to document and password-protect or encrypt it. Send the encrypted document as an email attachment and provide the password to the recipient in a separate email or by phone; then delete the document from your laptop.
- Do not post PII on the intranet, the Internet (including social networking sites), shared drives, or multi-access calendars that can be accessed by individuals who do not have a "need to know."
- Secure physical PII in a locked desk drawer, file cabinet, or similar when not in use. Documents must not be accessible to casual visitors, passersby, or other individuals within the office without a "need to know." Avoid faxing PII, if at all possible.
- Destroy documents containing PII when no longer needed, consistent with applicable records disposition schedules. Shred paper containing PII; do not recycle or place in garbage containers. Be especially alert during office moves and times of transition when large numbers of records are at risk.
- Report Privacy Incidents
    - You must report all privacy incidents/breach, whether suspected or confirmed, to your supervisor immediately. If your supervisor is unavailable, or if there is a potential conflict of interest, report the incident to your Program Manager, Help Desk, component privacy officer or privacy point of contact.
    - Most importantly report any type of breach to FTA

Business Value and Innovation

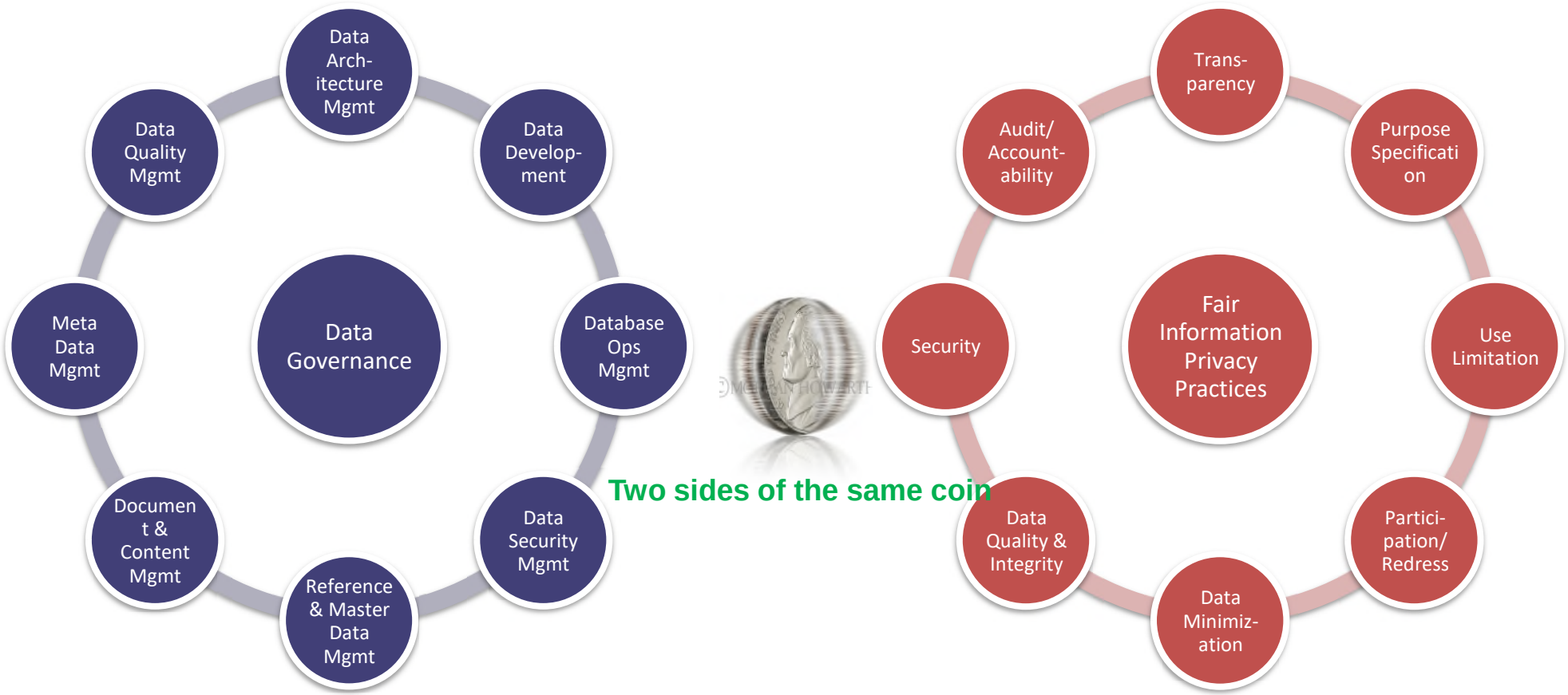
Value	Description
Improved customer service	Decisions based on information supports client responsiveness and enhances support for program activities
Stronger corporate governance	Well-managed data provides management with a comprehensive cohesive view of an organization's activity
Poor quality data costs more	Correcting data and decisions based (rework costs) on poor data increase as you move through data lifecycle
Faster identification and response to change	Promote proactive change management based on actual vs. perceived need
Improved accountability	As stakeholder awareness improves, policy owners can hold them accountable for their responsibilities and enforce compliance.

Information is the organization's most important resource

OCIO

2

Privacy and Data Management



Source: *Data Management Association (DAMA)*
Data Management Body of Knowledge (DMBOK)

Program Drivers

- What are my rights?
- Is this the data we really need?
- How is it protected from misuse?
- Am I Required to Provide?
- Why do you need?

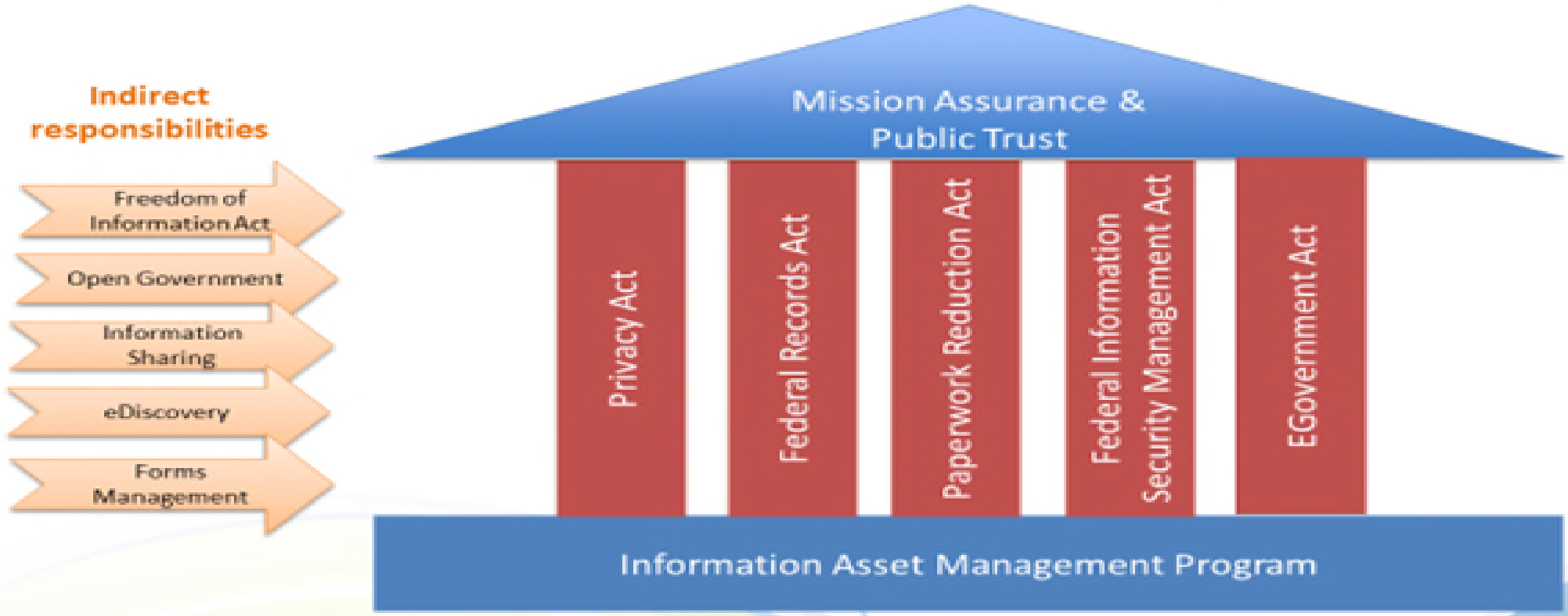
- Is the data any good?
- How will it be used?
- Can somebody else use?
- What are the legal obligations/ constraints?
- What if I don't like what you're doing?

OCIO Office of the DOT Chief Information Officer

Governance

Program Vision

Information Governance drives organizational efficiencies for lifecycle information in support of the DOT mission and enhancing public trust



OCIO

1

The Privacy Act of 1974

The Watergate Scandal and other allegations of governmental abuse led Congress to pass the Privacy Act of 1974. In 1974, Congress was concerned with curbing the illegal surveillance and investigation of individuals by federal agencies that had been exposed during the Watergate scandal. It was also concerned with potential abuses presented by the government's increasing use of computers to store and retrieve personal data by means of a universal identifier – such as an individual's social security number. The Act focuses on four basic policy objectives:

- To restrict disclosure of personally identifiable records maintained by agencies.
- To grant individuals increased rights of access to agency records maintained on themselves.
- To grant individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete.
- To establish a code of "fair information practices" that requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records.

Federal Records Act

The Federal Records Act of 1950 is a United States federal law that was enacted in 1950. It provides the legal framework for federal records management, including record creation, maintenance, and disposition.

The act, and its related regulations, require each federal agency to establish an ongoing program for record management and to cooperate with the National Archives and Records Administration (NARA).

What is National Archives and Records Administration (NARA)

The National Archives and Records Administration (NARA) is the nation's record keeper. Of all documents and materials created in the course of business conducted by the United States Federal government, only 1%-3% are so important for legal or historical reasons that they are kept by us forever.

Paperwork Reduction Act

The Paperwork Reduction Act (PRA) was enacted to minimize the paperwork burden for individuals; small businesses; educational and nonprofit institutions; Federal contractors; State, local and tribal governments; and other persons resulting from the collection of information by or for the federal government.

What requires a Paperwork Reduction Act review?

The Paperwork Reduction Act of 1995 (PRA) requires that all Federal Agencies receive approval from the Officer of Management & Budget (OMB) prior to collecting information from the public.

Federal Information Security Management Act

The Federal Information Security Management Act (FISMA) is United States legislation that defines a framework of guidelines and security standards to protect government information and operations. This risk management framework was signed into law as part of the Electronic Government Act of 2002, and later updated and amended.

The Electronic Government Act was introduced in order to improve the management of electronic government services and processes, while also managing federal spending around information security. FISMA was one of the more important regulations in the Electronic Government Act since it brought forth a method to reduce federal data security risks while emphasizing cost-effectiveness. A set of security policies were made for federal agencies to meet. FISMA requires federal agencies, and others it applies to, to develop, document and implement agency-wide information security programs. These programs should be able to protect sensitive data.

EGovernment Act

An Act to enhance the management and promotion of electronic Government services and processes by establishing a Federal Chief Information Officer within the Office of Management and Budget, and by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to Government information and services, and for other purposes.

TRANSIT.DOT.GOV