U.S. Department of Transportation

Privacy Impact Assessment

National Highway Traffic Safety Administration (NHTSA)

Office of Odometer Fraud Investigation (OFI)

SPIN

Responsible Official

David Sparks
Office Director
Office of Odometer Fraud Investigation (NEF300)
David.Sparks@dot.gov

Reviewing Official

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer
privacy@dot.gov

Executive Summary

The National Highway Traffic Safety Administration (NHTSA), within the Department of Transportation (DOT), carries out various motor vehicle and highway safety programs, including the investigations of possible odometer tampering on motor vehicles.

SPIN is a file system to gather information to be used in allegations of odometer fraud. It is maintained by the Office of Odometer Fraud Investigation (OFI) for use in criminal investigations and to support criminal prosecutions by the United States Department of Justice (DOJ).

This Privacy Impact Assessment (PIA) was completed in accordance with the E-Government Act of 2002 because SPIN maintains Personally Identifiable Information (PII) from members of the public. The information collected in the system includes information about suspects, defendants, witnesses, informants, motor vehicles, automobile dealers, victims and other related data obtained through Federal grand jury subpoenas.

What is a Privacy Impact Assessment?

The Privacy Act of 1974 articulates concepts for how the federal government should treat individuals and their information and imposes duties upon federal agencies regarding the collection, use, dissemination, and maintenance of personally identifiable information (PII). The E-Government Act of 2002, Section 208, establishes the requirement for agencies to conduct privacy impact assessments (PIAs) for electronic information systems and collections. The assessment is a practical method for evaluating privacy in information systems and collections, and documented assurance that privacy issues have been identified and adequately addressed. The PIA is an analysis of how information is handled to—i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system; and iii) examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[1]

Conducting a PIA ensures compliance with laws and regulations governing privacy and demonstrates the DOT's commitment to protect the privacy of any personal information we collect, store, retrieve, use and share. It is a comprehensive analysis of how the DOT's electronic information systems and collections handle personally identifiable information (PII). The goals accomplished in completing a PIA include:

[1]Office of Management and Budget's (OMB) definition of the PIA taken from guidance on implementing the privacy provisions of the E-Government Act of 2002 (see OMB memo of M-03-22 dated September 26, 2003).

- *Making informed policy and system design or procurement decisions. These decisions must be based on an understanding of privacy risk, and of options available for mitigating that risk;*
- *Accountability for privacy issues;*
- *Analyzing both technical and legal compliance with applicable privacy law and regulations, as well as accepted privacy policy; and*
- *Providing documentation on the flow of personal information and information requirements within DOT systems.*

Upon reviewing the PIA, you should have a broad understanding of the risks and potential effects associated with the Department activities, processes, and systems described and approaches taken to mitigate any potential privacy risks.

Introduction & System Overview

The Motor Vehicle Information and Cost Savings Act (the Act), as amended (49 U.S.C. 327), and its implementing regulations (49 C.F.R. Part 580), prescribes that a motor vehicle's odometer reading may be required to be disclosed in writing or electronically at the time of transfer (49 U.S.C. 32705), prohibits odometer tampering (49 U.S.C. 32703), and imposes civil and criminal penalties (49 U.S.C. 32709). Additionally, the Secretary of the Department of Transportation has delegated this authority to NHTSA. The statute and NHTSA's implementing regulations (49 C.F.R. Subtitle B Chapter V Part 580) authorize inspections and investigations (49 U.S.C. 32706). Qualified NHTSA employees may be deputized by the U.S. Marshals Service to safely and thoroughly investigate provisions of the Act that carry criminal penalties. These deputations convey law enforcement authorities such as the ability to seek and execute arrest and search warrants, serve legal documents, and carry firearms. Civil and/or criminal investigations of odometer fraud schemes may be referred to the U.S. Department of Justice for prosecution.

To facilitate NHTSA's enforcement activities, the Office of Odometer Fraud Investigation (OFI) developed SPIN. SPIN is a comprehensive, secure, web and incident-based case and document management system capable of managing the OFI workflow to include time tracking, supporting records, document management, and providing data analytics on odometer fraud investigations. The principal function of SPIN is case management. Even when ODI's mission strives to integrate criminal investigations in partnership with other criminal justice entities according to federal law[2], SPIN is only accessed by OFI personnel.

SPIN is hosted in the U.S. Government's Amazon Web Services (AWS) environment and collects, stores, and uses information some of which includes PII, Sensitive Personally Identifiable Information (SPII), and/or law enforcement sensitive but unclassified. The OFI employees receive information from different sources such as federal and state agencies,

[2] See 49 U.S. Code § 32706.

commercial entities, and individuals in a wide variety of formats, such as paper and electronic documents, print and digital audio and images, surveillance and subject interview efforts, and computer forensics. Information may be obtained on a voluntary basis, or it may be compelled by regulatory or statutory means. The information is kept until cases are resolved because they may be used as exhibits in courts.

The PII data collected in SPIN includes:

- Individual's Information: Name, Addresses (physical, mailing, shipping, and others), phones (phone, business cell, personal cell, fax, others), email (business and personal), birth (date, place, other dates of birth), gender, race, aliases, Alien Reg. #(s), Driver's License(s) number(s)/State, (Federal Bureau of Investigation (FBI)/State Identification Definition (SID) #(s), Federal Employer ID Number (FEIN)/Tax ID, Passport(s) number(s)/Country, Social Security Number (SSN)
- Case Information: Names of the primary and secondary agents
- Seller Information: Name, address, city, state, zip code, phone number
- Buyers Information: Name, address, city, state, zip code, phone number
- Victim / Complainant Information: Name, address, city, state, zip code, phone number (Person or entity that has been harmed as a result of fraud)
- Witness Information: Name, address, city, state, zip code, phone number
- Vehicle Information: Vehicle Identification Number (VIN), make, model, year, title number, jurisdiction, ownership transfers, odometer readings, and service records.
- Commercially Available Open-Source Data: Commercially available services like, Lexis-Nexis, eBay and Carfax can provide a full array of PII like VIN numbers, historical address, phone numbers, and vehicle ownership information.

The system also stores additional information about court cases, court dates, and prosecutorial results.

The information is shared by encrypted email or carrier with the other law enforcement agencies like the U.S. Department of Justice.

Fair Information Practice Principles (FIPPs) Analysis

The DOT PIA template is based on the fair information practice principles (FIPPs). The FIPPs, rooted in the tenets of the Privacy Act, are mirrored in the laws of many U.S. states, as well as many foreign nations and international organizations. The FIPPs provide a framework that will support DOT efforts to appropriately identify and mitigate privacy risk. The FIPPs-based analysis conducted by DOT is predicated on the privacy control families articulated in the Federal Enterprise Architecture Security and Privacy Profile (FEA-SPP)

v3[3], sponsored by the National Institute of Standards and Technology (NIST), the Office of Management and Budget (OMB), and the Federal Chief Information Officers Council and the Privacy Controls articulated in Appendix J of the NIST Special Publication 800-53 Security and Privacy Controls for Federal Information Systems and Organizations[4].

Transparency

Sections 522a(e)(3) and (e)(4) of the Privacy Act and Section 208 of the E-Government Act require public notice of an organization's information practices and the privacy impact of government programs and activities. Accordingly, DOT is open and transparent about policies, procedures, and technologies that directly affect individuals and/or their personally identifiable information (PII). Additionally, the Department should not maintain any system of records the existence of which is not known to the public.

NHTSA informs the public that their PII is collected, stored, and used in several ways. NHTSA does it through this PIA, published on the DOT website, where we identify the information collection's purpose, NHTSA's authority to collect, store, and use the PII, and all uses of the PII collected, stored, and transmitted through the system.

Information about individuals in SPIN is collected from OFI's investigative activities, information supplied by other federal, state, and local agencies, publicly available information, and other means authorized by law.[5]

System contains records that are subject to the Privacy Act. NHTSA published a System of Record Notice (SORN) in the Federal Register. DOT/NHTSA 413 - Odometer Fraud Data Files System - 65 FR 19548 - April 11, 2000.

Individual Participation and Redress

DOT provides a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, and disclosure of their PII. As required by the Privacy Act, individuals should be active participants in the decision-making process regarding the collection and use of their PII and they are provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

SPIN collects, stores, and report information some of which is PII, SPII, and/or law enforcement sensitive[6] but unclassified. The OFI employees receive by email information

[3] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[4] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf
[5] 5 U.S.C. § 552a(j)
[6] Law Enforcement Sensitive Information is unclassified information originated by agencies with law enforcement missions that may be used in criminal prosecution and requires protection against unauthorized disclosure to protect sources and methods, investigative activity, evidence, or the integrity of pretrial investigative reports.

from different Federal and State agencies in a wide variety of formats, such as paper and electronic documents, print and digital images, surveillance and subject interview efforts, and computer forensics. Information may be obtained on a voluntary basis, or it may be compelled by regulatory or statutory means. This information is kept until cases are resolved because they may be used as exhibits in courts.

Privacy Act requests for access to an individual's record must be in writing (either handwritten or typed). However, information relevant to criminal investigations is protected by the Freedom of Information Act (FOIA)[7] and is not required to disclose any information to the public, victims, witnesses, potential suspects, and other individuals involved in criminal investigations.

Additional information and guidance regarding the Freedom of Information Act and Privacy Act program may be found on the FOIA | NHTSA website. Privacy Act requests also may be addressed to:

NHTSA
Executive Secretariat
1200 New Jersey Avenue, SE
West Building, 41-304
Washington, D.C. 20590

Fax: (202) 493-2929
FOIA Requester Service Center: (202) 366-2870
email: NHTSAFOIAPublicLiaison@dot.gov

For more information related to PII collected under the FOIA, please see U.S. Department of Transportation's Freedom of Information Act and Privacy Act system of records notice. 84 Fed. Reg. 4605 (February 15, 2019) (https://www.govinfo.gov/content/pkg/FR-2019-02-15/pdf/2019-02356.pdf).

Purpose Specification

DOT should (i) identify the legal bases that authorize a particular PII collection, activity, or technology that impacts privacy; and (ii) specify the purpose(s) for which it collects, uses, maintains, or disseminates PII. The PII contained in PTB is utilized for transit subsidy usage reconciliation, reporting for the agency, monitoring, and tracking participant usage.

The primary purpose of the Office of Odometer Fraud Investigation is to conduct administrative, civil, and criminal investigations concerning odometer fraud. Violations of the statutes and regulations governing odometers are committed by individuals. The collected information is about the perpetrators, witnesses, and victims related to the odometer fraud investigations.

[7] 5 U.S.C. § 552b(7)

The Motor Vehicle Information and Cost Savings Act (the Act), as amended (49 U.S.C. 327), and its implementing regulations (49 C.F.R. Part 580), prescribes that a motor vehicle's odometer reading may be required to be disclosed in writing or electronically at the time of transfer (49 U.S.C. 32705), prohibits odometer tampering (49 U.S.C. 32703), and imposes civil and criminal penalties (49 U.S.C. 32709). Additionally, the Secretary of Transportation has delegated this authority to NHTSA. The statute and NHTSA's implementing regulations (49 C.F.R. Subtitle B Chapter V Part 580) and authorize inspections and investigations (49 U.S.C. 32706).

Data Minimization & Retention

DOT should collect, use, and retain only PII that is relevant and necessary for the specified purpose for which it was originally collected.

NHTSA collects and uses only minimum data elements necessary to investigate possible odometer fraud.

NHTSA retains most records in SPIN for a maximum period of 15 years, or when the records are no longer needed for the odometer fraud investigation purposes in accordance with the with approved National Archives and Records Administration (NARA) record schedule DAA-0416-2015-0001[8]. However, whenever there is federal criminal prosecution, record retention is coordinated with DOJ.

On rare occasions hard copy documents are received and stored in secured cabinets in a secured area, in OFI offices. The records retention schedule also applies to the hard copies and electronic records.

Use Limitation

DOT shall limit the scope of its PII use to ensure that the Department does not use PII in any manner that is not specified in notices, incompatible with the specified purposes for which the information was collected, or for any purpose not otherwise permitted by law.

The Office of Odometer Fraud Investigation collects, stores, uses, and retains in SPIN only the data elements that are relevant and necessary for the purposes of investigating possible odometer fraud from victims, witnesses, and potential suspects. The system stores information necessary to uniquely identify these individuals and document their role as it relates to an investigation.

[8] https://www.archives.gov/files/records-mgmt/rcs/schedules/departments/department-of-transportation/rg-0416/DA-0416-2015-0001_sf115.pdf

The PII in SPIN is not shared publicly. The information is only shared with other law enforcement agencies like the U.S. Department of Justice, or when required by Federal law.

Data Quality and Integrity

In accordance with Section 552a(e)(2) of the Privacy Act of 1974, DOT should ensure that any PII collected and maintained by the organization is accurate, relevant, timely, and complete for the purpose for which it is to be used, as specified in the Department's public notice(s).

OFI has quality control (QC) processes in place to monitor and review the data it obtains for its investigations. QC activities are required to ensure each record has accurately captured the data and the data entry and coding are consistent across all records in the system.

The OFI QC process includes:

- Edit Checks- an internal program checks to assure consistent data.
- In-house Record Review – Each record is reviewed for accuracy.
- Record Review – Each record is reviewed to ensure compliance with protocols and coding conventions.
- Data Review – Each record is reviewed to ensure that it includes the required elements needed for the study (e.g., damage sketches, crash reconstruction, images, etc.)
- Data Coding – Each record is reviewed to ensure that data elements are coded correctly.
- Investigation Activities – OFI investigators perform confirm the data is correct during their investigations. Otherwise, it is corrected.
- Site Visits – OFI investigators may conduct visits to crash locations to measure scenes and vehicles and to interview individuals involved in the crash to assure accuracy and completeness.
- OFI Review – Prior to sharing data with other law enforcement agencies, OFI staff review data for consistency and completeness.

Security

DOT shall implement administrative, technical, and physical measures to protect PII collected or maintained by the Department against loss, unauthorized access, or disclosure, as required by the Privacy Act, and to ensure that organizational planning and responses to privacy incidents comply with OMB policies and guidance.

PII collected and maintained in SPIN is safeguarded in accordance with applicable rules and policies, including all applicable DOT automated systems security and access policies. NHTSA security policy and practices are based on NIST Information Risk Management and Security standards. These are supplemented by privacy-specific guidance provided in NIST

800-122 and NIST Special Publication 800-53 Revision 4, and the DOT Privacy Risk Management Policy 1351.18 and the Office of Management and Budget circular A-130, Section 8b(3), Securing Agency Information Systems. The NIST security guides and standards are used by NHTSA to, among other things; assess information confidentiality, integrity and availability risks, identify required security safeguards, and adjust the strength and rigor of those safeguards to reduce risks to appropriate acceptable levels. Under this policy NITSA has implemented appropriate Administrative, Physical and Technical safeguards to protect the confidentiality, availability and integrity of the SPIN system and information.

Under this policy, NHTSA has implemented appropriate administrative, physical, and technical safeguards to protect the confidentiality, availability and integrity of the SPIN system and information.

Further protection of PII in SPIN include:

- All NHTSA employees and contractors undergo the mandatory DOT background checks prior to being granted access to the DOT network. In addition, all SPIN users receive both general, and role-based security training on an annual basis.
- NHTSA utilizes role-based security in SPIN to restrict user access to specific applications.
- NHTSA enforces assigned authorizations in SPIN for controlling access to the system using multi-factor authentication technology.
- The SPIN system maintains an audit trail of changes made, date/time of change and the user for each database change.

All electronic communications are encrypted using Federal Information Processing Standard (FIPS) 140-2 certified in-transit and at-rest encryption modules. Remote access to SPIN IT Infrastructure is provided via the DOT Secure Remote Access solution using multi-factor authentication to ensure only authorized personnel are granted access to the system and its data. By policy and design, SPIN is not accessible from public networks.

The information is protected by limiting users' access within the system based on their user's profile to view, change, add or delete information within the system. SPIN employs a multi-factor authentication for users' access to the system. The multi-factor users' authentication process provides an additional security layered approach by requiring the user to present a combination of two credentials to verify a user's identity.

Accountability and Auditing

DOT shall implement effective governance controls, monitoring controls, risk management, and assessment controls to demonstrate that the Department is complying with all applicable privacy protection requirements and minimizing the privacy risk to individuals.

NHTSA is responsible for identifying, training, and holding operating administration personnel accountable for adhering to NHTSA privacy and security policies, and regulations. NHTSA follows the fair information practice principles (FIPPS) as best practices for the protection of information associated with the records in the SPIN Data System. In addition to these practices, policies and procedures will be consistently applied, especially as they relate to the protection, retention, and destruction of records. The NHTSA Security and Privacy Officers will conduct periodic security and privacy reviews of the SPIN Data System consistent with the Office of Management and Budget Circular A-130, Section 8b, Securing Agency Information Systems and follow the DOT Privacy Risk Management Policy 1351.18. https://www.transportation.gov/sites/dot.gov/files/docs/CIOP - Privacy Risk Management - 1351.18 - Policy - 09302014.pdf.

Responsible Official

David Sparks
System Owner
Office Director
Office of Odometer Fraud Investigation (NEF300)

Prepared by: Jose Delgado-Forastieri, NHTSA Privacy Officer

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN
Digitally signed by KARYN MARIE GORMAN
Date: 2024.11.07 09:29:11 -05'00'