U.S. Department of Transportation

Privacy Impact Assessment

Federal Motor Carrier Safety Administration (FMCSA)

FMCSA Data Repository

Responsible Official

Dan Britton
Email: dan.britton@dot.gov
Phone Number: 202-366-9980

Reviewing Official

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

Executive Summary

The U.S. Department of Transportation's (DOT) Federal Motor Carrier Administration's (FMCSA) core mission is to reduce commercial motor vehicle-related crashes, injuries, and fatalities. To further this mission, FMCSA's Office of Analysis, Research, and Technology undertakes numerous research studies to improve the safety and efficiency of commercial motor vehicle operations through technological innovation and improvement, which results in many datasets that would be of value to other researchers and the public.

The FMCSA Data Repository and website (https://fmcsadatarepository.vtti.vt.edu/), managed by the Virginia Tech Transportation Institute (VTTI), provides the public access to these datasets. The Data Repository provides the public with a centralized repository of datasets from previous FMCSA studies, as required in the policy memorandum from the Office of Science and Technology Policy "Increasing Access to the Results of Federally Funded Scientific Research" dated February 22, 2013, available at: https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/ostp_public_access_memo_2013.pdf

Public-use data which does not contain Personally Identifiable Information (PII) are also available on the Data Repository website. Complete datasets from the research studies which contain PII are maintained in a secure data enclave, which is accessible only to approved users who are authorized to access that data at the VTTI data enclave facility. The data elements of each study that qualify for this level of access are determined on a case-by-case basis and are based on the data use terms laid out in the originating study's informed consent forms (ICFs). This Privacy Impact Assessment (PIA) is published in accordance with the E-Government Act of 2002 and addresses the risks associated with maintaining and facilitating access to data in the Data Repository.

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:

- *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

FMCSA-sponsored research and technology studies often result in motor vehicle related datasets that could be used for future analyses. To support further use of these datasets, FMCSA created the Data Repository to house the data from these studies. To access this data, researchers are required to follow access and security procedures established by FMCSA. The FMCSA Data Repository, managed by VTTI, consists of a user website (https://fmcsadatarepository.vtti.vt.edu/), which hosts de-identified data, and a secured Data Enclave which hosts complete datasets from research studies which include PII.

Public-Use/De-Identified Data

At the conclusion of each FMCSA-sponsored study, the contractors who performed the study are required to create a de-identified, public-use dataset containing the data from the study. This data is posted on the Data Repository website. To gain access to this data, users create an account by registering a username and password, email address, first name, last name, and organization name. This allows VTTI to track who downloads the data.

The data may include, but is not limited to:

[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).

1. *Reduced event and baseline data:* Data on safety-critical events, with contributing characteristics such as internal/external distractions, fatigue, and whether a driver took his/her eyes off the road. Baseline data is comprised of samples of everyday driving data, randomly selected during periods that do not contain the factors being investigated.
2. *Kinematic data from the vehicle(s):* Data such as horizontal and lateral g-force, braking severity, speed, and throttle position.
3. *Actigraph data*: Data collected from a small wearable device that detects motion, light value, and, through various algorithms, evaluates sleep and activity.
4. *Psychomotor vigilance task data (PVT):* Reaction time data that determines a driver's fitness for duty.
5. *Questionnaire data:* Responses from questionnaires that were administered to obtain driver demographics or opinions.

Identifiable Data

1. *Video:* Video containing images of the participant drivers' faces.
2. *GPS:* GPS coordinates on truck locations that may allow someone to determine where the participating driver lives, works, or drives regular routes.
3. *Crash Information:* Dates, times, and locations associated with crashes.
4. *Electronic Logging Device (ELD) Information:* Dates, times, and locations associated with ELD data.

Requesting Access to Identifiable Data

Access to identifiable/sensitive data requires approval by FMCSA to ensure that it is available only to qualified researchers. To access this data, users are required to contact VTTI (using the "contact us" button on the website, which initiates an email to "DataRepository@vtti.vt.edu") and request a specific dataset

Data with PII may only be viewed in the secure data enclave located at VTTI. For access to be approved, the user must show proof of Institutional Review Board (IRB)[2] approval and sign VTTI's Data Use License (DUL) describing their need for the data with PII. The request must also be approved by FMCSA.

[2] An IRB is an appropriately constituted group that has been formally designated to review and monitor research involving human subjects. An IRB has the authority to approve, require modifications of, or disapprove research.

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 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.

Research Participants

The Data Repository houses data obtained in research and technology studies, all of which are required to obtain IRB approval before data collection begins. Part of the IRB process is developing an Informed Consent Form (ICF), which details the participants' role in the study and how their data is be protected. All ICFs discuss the possibility of PII being accessed by qualified researchers in a secure setting (i.e., the secure data enclave). Data is only collected from participants who sign these ICFs, so all data in the Data Repository has been gathered from people who have specifically consented to make their data available in this manner. More recent (i.e., after the start of the Data Repository project) ICFs specify that a public use dataset is posted online for public download. Before any data is included in the Data Repository, IRB materials are reviewed to ensure that publicizing the data is allowed.

FMCSA informs the public that their research data with PII is stored and accessible at the Data Repository's secure data enclave through this PIA. This document identifies the information collection's purpose, FMCSA's authority to collect, store, and use the PII, along with all uses of the PII stored and transmitted through the Data Repository.

[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

Researchers Registered in the Data Repository

Researchers are required to create user accounts to access the Data Repository and accessing data with PII has additional requirements. Data on these users helps FMCSA plan and manage Data Repository systems, such as making decisions regarding upgrading hardware, software, and communications technology to meet changing Internet/Intranet use requirements (see DOT/ALL 13 – Internet/Intranet Activity and Access Records). When accessing the datasets within the Data Depository, users must read and agree to a warning message that discusses the penalties of unauthorized access before logging in. The Data Repository website has a link to the DOT Privacy Policy describing DOT policies on the online collection and use of PII, as required by the E-Government Act of 2002.

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.

Research Participants

Since data is de-identified, it is impossible for participants to identify their data to ask for its removal. Furthermore, when participants signed the ICF, they agreed to allow their de-identified data to be posted online. While all data shared on the website is de-identified, any concerns by participants may be expressed by sending an email to VTTI via the “contact us” button. These concerns are reduced by ensuring the concerned participant that the data is thoroughly de-identified.

Researchers Registered in the Data Repository

Personal information collected for Data Repository user account creation is provided by the users, who are informed that this data is only kept to maintain website functionality. If users wish to delete their account, they may contact VTTI, who in return disables and deletes the requested account.

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.

Research Participants

The Data Repository provides the public with a centralized repository of datasets from previous FMCSA studies, as required in the policy memorandum from the Office of Science and Technology Policy “Increasing Access to the Results of Federally Funded Scientific Research” dated February 22, 2013, available at: https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/ostp_public_access_memo_2013.pdf

Researchers Registered in the Data Repository

PII needs to be collected directly from individuals who create Data Repository accounts so that FMCSA can manage system usage and determine whether system upgrades are necessary.

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.

Data Minimization

Research Participants

The 2013 policy memorandum mentioned above states: “To achieve the Administration’s commitment to increase access to federally funded published research and digital scientific data, Federal agencies investing in research and development must have clear and coordinated policies for increasing such access.” The Data Repository represents the results of the efforts of FMCSA’s Office of Analysis, Research, and Technology to meet this requirement.

Participant data on the Data Repository website is anonymized by assigning each participant a Driver ID (e.g., “Driver 001”) at the start of the corresponding project’s data collection. Each Driver ID is then linked to all data collected on that driver (including driving data, safety-critical event data, ELD data, actigraph data, questionnaire data, etc.). To access data containing PII, external users must visit the VTTI secure data enclave. To access the enclave, the researcher must first request the specific dataset(s) from VTTI. Next, they must provide proof of IRB training and approval for their intended research. Then, they must sign a DUL with VTTI describing their need for the data. Finally, they request and schedule a visit to the enclave where only the specific dataset(s) requested is made available for access.

Retention

Research Participants

All ICFs completed by individuals providing data that might eventually be used in the Data Warehouse discuss the possibility of PII being accessed by qualified researchers in a secure setting (i.e., the secure data enclave). Data is only collected from participants who sign these ICFs, so all data in the Data Repository has been gathered from people who have specifically consented to make their data available in this manner. More recent (i.e., after the start of the Data Repository project) ICFs specify that a public use dataset has been posted online for public download. Before any data is included in the Data Repository, IRB materials are reviewed to ensure that publicizing the data is allowed.

Participant data falls under the research record retention requirements found in the Department of Health and Human Services (HHS) regulations for Protection of Human Research Subjects at 45 CFR 46. The HHS protection of human subjects' regulations require institutions to retain records of Institutional Review Board (IRB) activities for at least three years after completion of the research (45 CFR 46.115(b)).

Researchers Registered in Data Repository

This data is used by FMCSA to plan and manage usage of the system and determine whether system upgrades are necessary. FMCSA only uses and retains data that are relevant and necessary for the purpose of the Data Repository system in accordance with the National Archives and Records Administration (NARA) General Records Schedule 3.2, Transmittal No. 26, Information Systems Security Records, System Access Records, Item 030 and Item 031 (September 2016). System Access Records are records created as part of the user identification and authorization process to gain access to system, and include user profiles, log-in files, password files, and system usage files. Records under Item 030 are identification records generated according to preset requirements which are temporary records to be destroyed when business use ceases. They are also temporary records but should be destroyed 6 years after a password is altered or user account is terminated, however longer retention is authorized if the records are required for business use.

NARA's GRS 3.2, Transmittal No. 26, Information Systems Security Records, Systems and data security records, Item 010 (September 2016), describes the retention period for records related to maintaining the security of the system and data. These records outline the official procedures for securing and maintaining the system. They include the analysis of security policies, processes, and guidelines, such as System Security Plans for de-identification. These records are to be destroyed 1 year after the system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system.

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.

Each research project with data made accessible via the Data Repository receives IRB approval prior to the collection of data. The IRB process requires the researcher to provide a detailed protocol explaining the purpose of the study, how the data is collected and stored, and who may have access to the data in the future. Each study also includes an Informed Consent Form (ICF) signed by each participant. The ICF details the types of data collected and who may have access to the data in the future. All datasets made available through the Data Repository must clearly articulate in the IRB documents that the data may be included in the Data Repository, otherwise it is not included.

External researchers can request access to identifiable data by submitting a request on the Data Repository website. For access to be approved, the user must show proof of IRB approval and sign a DUL with VTTI describing their need for the identifiable data requested. The request must also be approved by FMCSA.

The Data Repository provides the public with a centralized repository of datasets from previous FMCSA studies, as required in the policy memorandum from the Office of Science and Technology Policy "Increasing Access to the Results of Federally Funded Scientific Research" dated February 22, 2013, available at: https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/ostp_public_access_memo_2013.pdf

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).

Anonymized data included in the public use datasets are always anonymized, as the original research team has the only access to information linking PII to the Driver ID (i.e., the anonymizer). Driving data, safety-critical event data, ELD data, actigraph data, are collected from cameras or sensors placed on or in vehicles. Questionnaire data is collected directly from study participants and is assumed to be accurately reported by them.

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 is protected by reasonable security safeguards against loss or unauthorized access, destruction, usage, modification, or disclosure. These safeguards incorporate standards and practices required for Federal information systems under the Federal Information System Management Act (FISMA) and are detailed in Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems, dated March 2006, and NIST Special Publication (SP) 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, dated April 2013. FMCSA has a comprehensive information security program that contains management, operational, and technical safeguards that protect PII. These safeguards are designed to achieve the following objectives:

- Protect against any reasonably anticipated threats or hazards to the security or integrity of PII
- Protect against unauthorized access to or use of PII
- Ensure the security, integrity, and confidentiality of PII

Records in the Data Repository system are safeguarded in accordance with applicable rules and policies, including all applicable DOT automated systems' security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in the Data Repository system is limited to those individuals who have a need to know the information for the performance of their official duties and who have appropriate clearances and permissions. All records in the Data Repository system are protected from unauthorized access through appropriate administrative, physical, and technical safeguards. All access to the Data Repository system is logged and monitored.

Users are required to authenticate with a valid user identifier and password to gain access to the information contained within the Data Repository system. Furthermore, datasets containing PII can only be viewed at the secure data enclave location. This strategy improves data confidentiality and integrity. These access controls were developed in accordance with Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems dated March 2006 and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Rev. 5, Recommended Security Controls for Federal Information Systems, dated April 2013. Regular monitoring activities are also performed annually to provide ongoing oversight of security controls and to detect misuse of information stored in the Data Repository system.

The Data Repository system is assessed in accordance with the Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic resource, and the DOT Certification and Accreditation Guidance. The Data Repository is approved through the Security Authorization Process under the National Institute of Standards and Technology.

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.

Regular testing of information systems security is performed by VTTI information technology personnel. These tests include the use of assessment and scoring tools provided by the Center for Internet Security (CIS). FMCSA personnel and FMCSA contractors are required to attend security and privacy awareness training and role-based training offered by DOT/FMCSA. These trainings allow individuals with varying roles to understand how privacy impacts their role and retain knowledge of how to properly act in situations where they may use PII while performing their duties.

FMCSA follows the Fair Information Principles as best practices for the protection of information associated with the Data Repository. In addition to these practices, policies and procedures are consistently applied, especially as they relate to protection, retention, and destruction of records. Federal and contract employees are given clear guidance in their duties as they relate to collecting, using, processing, and securing data. The FMCSA Security Officer and FMCSA Privacy Officer conduct regular periodic security and privacy compliance reviews of the Data Repository consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Managing Information as a Strategic Resource.

Responsible Official

Dan Britton
System Owner
Mathematical Statistician, FMCSA Research Division

Prepared by: Dan Britton

Approval and Signature

Karyn Gorman
DOT Chief Privacy Officer
Office of the Chief Information Officer