U.S. Department of Transportation

Privacy Impact Assessment

Federal Motor Carrier Safety Administration

FMCSA

Impact of Driver Detention Time on Safety and Operations

(Detention Time)

Responsible Official

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

Reviewing Official

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

Executive Summary

The core mission of the Federal Motor Carrier Administration (FMCSA) is to reduce commercial motor vehicle (CMV)-related crashes and fatalities. In carrying out this mission, and in accordance with 49 U.S.C. 504, 31133, 31136, 31502, 49 CFR 1.73, and 49 U.S.C. 31108, FMCSA conducts research to identify and assess contributing factors associated with CMV crashes and performs analyses to identify potential mitigation strategies that could be used to improve safety.

To carry out these research studies, FMCSA contracted with the Virginia Tech Transportation Institute (VTTI) to evaluate the impact of CMV driver detention time (the time CMV drivers spend at shipping and receiving facilities not associated with essential tasks) on roadway safety and CMV operations. Specifically, FMCSA needs additional data from a broad sample of carriers to understand the safety and operational impacts of detention time and why it occurs. Further, this study will assess the utility of existing intelligent transportation system (ITS) solutions to measure detention time. This Privacy Impact Assessment is being conducted to address the risks associated with VTTI collecting, processing, and maintaining Personally Identifiable Information (PII) from study participants on behalf of FMCSA.

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 study includes data collected via electronic logging devices (ELDs), transportation management systems (TMS), vehicle telematic systems, safety records, and answers to questions delivered through carriers' dispatching systems from a sample of up to 2,500 trucks across up to 80 carriers who choose to participate in the project. The TMS, ELD, telematics, and safety data are already collected by carriers. The only additional data collected will be answers to questions about events during individual trips, which will be submitted through the carriers' dispatching systems. This information will allow FMCSA to identify the severity and frequency of detention time, the factors that contribute to detention time, and the administrative, operational, and safety outcomes of detention time. Data collected will include carrier information, driver information, pick-up/delivery information, driver duty status, driving performance, insurance claims, crashes, and detention time information.

Participant Selection

The carriers who participate will hopefully produce a representative sample of the nation in terms of carrier size. Many participating carriers will be current or prospective clients of Motive, a company with a variety of ELD, TMS, and telematics products, with a focus on serving small carriers and owner-operators. However, all interested carriers will be considered for participation if they meet the data collection requirements, whether they are Motive clients or not. Participation by drivers employed by these carriers will be voluntary. The final sample will include up to 80 carriers with up to 2,500 total vehicles, covering a variety of carrier operations, including long haul/short haul, private/company carriers and for-hire carriers, port servicing (primarily chassis), owner-operators, hourly and mileage-based operators, truckload/less-than-truckload, and dedicated local delivery. These carriers will range in size from single-vehicle owner-operators to carriers with hundreds of trucks, with a likely average carrier size of around 30 vehicles.

Study Participation

Participating carriers will agree to share access to their TMS with the research team, who will geofence each shipper/receiver facility with a custom polygon. Each time a truck from one of the participating fleets enters the geofenced facility, the research team will send a message through the driver's current ITS dispatching device. This message will prompt the driver to answer a series of questions related to their arrival. For example, drivers will select whether they are (1) on time, (2) late, (3) early, or (4) detained. Upon exiting the geofenced facility, the driver will receive a message with a delivery summary, and the driver will be able to offer edits through the dispatching device when the vehicle is safely stopped. The TMS will provide information related to each delivery/pick-up order, arrival times, appointment times, and waiting times. Additionally, data from the carriers' telematics and ELD will be collected to identify driver performance and driver duty status. Finally, the research team will collect federal crash and violation data to link to the carrier data.

All data will be encrypted and automatically transferred to the research team via the carriers' existing TMS. Carrier and Driver ID numbers will be created specifically for this project, with a key linking them to the carriers' and drivers' actual names. The key will only include carrier and driver names, or similar identifiable data, and project ID numbers. Data collected for the project will use these Carrier and Driver ID numbers, making it impossible to link project data to the names of participating carriers and drivers without the key. The key will never leave VTTI and will be stored in a project folder only accessible by VTTI's principal investigator and chief statistician. The key will not be accessible to anyone else at VTTI or FMCSA, and it will be deleted one year after the project is completed. The remaining study data, which only use the project ID numbers, will be stored in a separate project folder location, accessible only by the VTTI's study team. Further, this study was reviewed and has been approved by the contractor's Institutional Review Board (IRB) to ensure participant protection.

Study Termination

After data collection is complete, administrative data will be destroyed at a predetermined date; these data will include participants' names, addresses, etc. Study data will be processed for inclusion in FMCSA's Data Repository so that the datasets may be used for future analyses. This study will produce two datasets for the Data Repository: (1) an anonymized, public-use dataset, with no PII; and (2) a dataset with identifiable data, for use only within the Data Repository's secure data enclave located at VTTI.

The public-use dataset will be scrubbed of all data that could potentially identify drivers or carriers, such as names, locations, dates, and times, though dates and times may be systematically shifted (e.g., by 56 weeks) to allow analyses related to issues such as seasonal variations, but to ensure participants' privacy. However, the identifiable dataset

will not include carrier or driver names, as dictated by VTTI's non-disclosure agreements with participating carriers.

The identifiable dataset will only be accessible at the Data Repository's secure data enclave, located at VTTI. Anyone who wants to view it will have to show proof of IRB approval, sign a Data Use License (DUL) with VTTI describing their need for the identifiable data, and obtain approval from FMCSA.

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[2], 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[3].

Transparency

Sections 522aI(3) aI(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.

When recruiting carriers, VTTI will discuss how their data will be used and stored. VTTI will ensure all carriers understand that their names and their drivers' names will not be shared and that any PII (i.e., time and date of a crash) would only be accessible by qualified researchers in a secure setting (i.e., the Data Repository's secure data enclave).

FMCSA clearly discloses its policies and practices concerning all PII collected, maintained, used, and disseminated by the Agency. FMCSA provides notice to individuals in several different ways—for example, notices of proposed rulemaking, final rules, notices of proposed information collections, the privacy policy on the FMCSA website, system of record notices, and privacy impact assessments (PIAs).

In addition to this PIA, FMCSA has published a 60-day Federal Register notice announcing this proposed information collection and a 30-day Federal Register notice announcing its

[2] http://www.cio.gov/documents/FEA-Security-Privacy-Profile-v3-09-30-2010.pdf
[3] http://csrc.nist.gov/publications/drafts/800-53-Appdendix-J/IPDraft_800-53-privacy-appendix-J.pdf

intent to submit the information collection request to the Office of Management and Budget (OMB), which was approved on May 22, 2024. These documents are publicly available on OMB's Office of Information and Regulatory Affairs website (https://www.reginfo.gov/public/). The publication of this PIA demonstrates FMCSA's commitment to transparency and may be found on the DOT website at http://www.dot.gov/privacy.

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.

Before participating in the study, prospective carriers and drivers will be told what information would be collected from them. Each participating carrier will be asked to sign a participation agreement documenting the responsibilities of all parties. This agreement will allow their de-identified data to be posted in FMCSA's Data Repository, and will explain that any PII (i.e., time and date of a crash) would only be accessible by qualified researchers in a secure setting (i.e., the Data Repository's secure data enclave). While all data shared on the Data Repository website will be de-identified, any concerns by participants may be expressed by sending an email to VTTI.

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 core mission of FMCSA is to reduce CMV-related crashes and fatalities. In carrying out this mission, and in accordance with 49 U.S.C. 504, 31133, 31136, 31502, 49 CFR 1.73, and 49 U.S.C. 31108, FMCSA conducts research to identify factors that contribute to CMV crashes and performs analyses to identify strategies that could improve safety. Detention time consistently ranks as one of the top problems for CMV operators, and it might have a significant negative impact on safety.

In February 2011, the Government Accountability Office (GAO) issued a report indicating that approximately two thirds of drivers had experienced detention time in the past month[4]. In 2018, the Office of the Inspector General (OIG) estimated that detention time is

[4] Government Accountability Office. (2011). *Commercial motor carriers: More could be done to determine impact of excessive loading and unloading wait times on hours of service violations* (Report No. GAO-11-198).

associated with reduced annual driver earnings of $1.1 billion to $1.3 billion for certain sectors of the trucking industry[5]. In addition, detention time affects CMV drivers' abilities to meet hours of service (HOS) requirements by reducing their available driving time, which might contribute to unsafe driving.[4,6] The 2018 OIG study concluded that a 15-minute increase in average dwell time increases the average expected crash rate by 6.2%.[5]

An important first step in addressing detention time is understanding the factors that contribute to the issue. FMCSA and the VTTI research team are unaware of other research that could fulfill the research goals of this project. A 2014 FMCSA[7] study provided valuable initial insights on detention time; however, the study had several limitations. Specifically, the study's sample was not representative of the trucking industry, detention time was estimated based on GPS coordinates without requiring information from drivers on specific activities performed onsite, data were only recorded when a driver was on duty which missed detention time not recorded if the driver was off duty, time spent loading/unloading was not differentiated from time spent waiting, and data were collected over a 6-month period which did not account for seasonal variations.

The current study will address these limitations to provide FMCSA with a robust assessment of the impacts of driver detention time on safety and operation in the trucking industry. We will collect data from multiple sources to accurately identify detention time by differentiating the many activities drivers may perform at a facility, while also considering the many nuances associated with detention and appointment times.

Prospective participants will be provided with the necessary information regarding the collection, use, and disclosure of their PII during the informed consent process. Participants' PII will only be used or disclosed under the terms outlined in the participation agreement.

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.

FMCSA has determined that this collection of information is necessary for study completion because there is no existing data that can adequately address the project's research questions, and the answers to these questions may provide important insights on how

[5] Office of Inspector General. (2018). *Estimates show commercial driver detention increases crash risk and costs, but current data limit further analysis* (Report No. ST2018019). Federal Motor Carrier Safety Administration.
[6] Knipling, R.R., Hickman, J.S., & Bergoffen, G. (2003). *CTBSSP Synthesis 1: Effective commercial truck and bus safety management techniques: A synthesis of safety practice*. Transportation Research Board.
[7] Dunn, N.J., Hickman, J.S., Soccolich, S., & Hanowski, R.J. (2014). *Driver detention times in commercial motor vehicle operations* (Report No. FMCSA-RRR-13-060). Federal Motor Carrier Safety Administration.

detention time can impact safety. The only data collected during the study will be the data needed to meet the study's objectives.

The records for the Driver Detention Time on Safety and Operations Program will be retained according to records control schedule number DAA-0557-2024-0002 – Research, Technology, and Information Management. All records maintained in the system will be treated as permanent records until the schedule is approved by NARA.

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 carrier participation agreement details the types of data collected and who may have access to the data in the future. This study will only collect the data necessary to answer the research questions, complying with the requirements of the Paperwork Reduction Act (PRA).

The identifiable dataset will only be accessible at the Data Repository's secure data enclave at VTTI. Anyone who wants to view it will have to show proof of IRB approval, sign a Data Use License (DUL) with VTTI describing their need for the identifiable data, and obtain approval from FMCSA.

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).

Carrier-provided data will be collected through their TMS, ELD, and telematics systems and devices. Detention time data will be provided directly by carriers and their drivers. Verifying this data, which will not contain PII, would not be feasible, but there would likely be no reason to doubt its accuracy.

Data included in the anonymized, public-use datasets will not contain PII. Data with PII will only be available to researchers who gain the necessary approvals and visit the Data Repository secure data enclave at VTTI. Attention will be taken to ensure the accuracy of the data, both for the success of the project and the integrity of the data.

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.

The PII collected for this project will be 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 are appropriate for the protection of PII. These safeguards are designed to achieve the following objectives:

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

Records held by VTTI and in the Data Repository 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 Data Repository system is limited to individuals who 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.

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. FMCSA personnel and FMCSA contractors are required to attend security and privacy awareness training and role-based training offered by DOT/FMCSA. This training allows individuals with varying roles to understand how privacy impacts their role and retain knowledge of how to properly and securely act in situations where they may use PII in the course of performing their duties.

FMCSA follows the Fair Information Principles as best practices for the protection of information associated with the Data Repository. In addition, policies and procedures are consistently applied, especially as they relate to the 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.

Responsible Official

Dan Britton
System Owner
Mathematical Statistician, FMCSA

Prepared by: Pamela Gosier-Abner
Director, Cybersecurity and Privacy Office

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

KARYN MARIE GORMAN Digitally signed by KARYN MARIE GORMAN Date: 2024.06.21 13:33:47 -04'00'