



U.S. Department of Transportation

Privacy Impact Assessment

Federal Motor Carrier Safety Administration

FMCSA

Human Factors Considerations in Commercial Motor Vehicle Automated Driving Systems and Advanced Driver Assistance Systems (HF in ADS)

Responsible Official

Terri Hallquist
Email: Theresa.hallquist@dot.gov
Phone Number: 202-366-1064

Reviewing Official

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer

privacy@dot.gov





Executive Summary

The core mission of the Department of Transportation (DOT) Federal Motor Carrier Administration (FMCSA) is to reduce commercial motor vehicle (CMV) related crashes and fatalities. In carrying out its safety mission, and in accordance with 49 U.S.C. 504, 31108, 31133, 31136, 31502, and 49 CFR 1.73, FMCSA conducts research to identify and assess contributing factors associated with CMV crashes and performs analyses to identify effective countermeasures, including the use of advanced vehicle technologies.

To carry out these research studies, FMCSA maintains contracted support with the Virginia Tech Transportation Institute (VTTI) to assess the risk of engaging in non-driving secondary tasks while operating a CMV equipped with advanced driver assistance systems (ADAS) and automated driving system (ADS) advanced safety technologies. Further, this study is used to develop training tools for the integration of advanced safety technologies within the trucking industry. The study uses a heavy vehicle simulator to evaluate the impact of secondary tasks, transfer of control, and training on driver behavior in CMVs equipped with ADAS or ADS in a sample of 100 CMV drivers. The simulator study consists of two 4-hour simulator study sessions completed at VTTI with a simulated Level 2 (L2) ADAS or Level 3 (L3) ADS.

This Privacy Impact Assessment (PIA) 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

¹Office 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).



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

The study uses a heavy vehicle simulator to evaluate the impact of secondary tasks, transfer of control, and training on driver behavior in CMVs equipped with ADAS or ADS in a sample of 100 CMV drivers. The simulator study consists of two 4-hour simulator study sessions completed at VTTI with a simulated Level 2 (L2) ADAS or Level 3 (L3) ADS. Specific driving scenarios, including different secondary tasks, roadway types, weather, and roadway geometry, were developed to address the impact of secondary tasks and transfer of control on CMV driver behavior. Data collected includes quantitative and qualitative dependent variables, such as simulated driving performance, eye-glance patterns and duration, demographic characteristics, opinions and perception of situation awareness, risky driving, advanced technology, and effectiveness of driver training.

Participant Selection

Participants were identified using VTTI's large database of truck drivers who participated in previous research studies, expressed interest in participating in future studies, or work for a carrier within a 24-hour drive of Blacksburg, Virginia. Eligible drivers must hold a valid commercial driver's license with class A or B specification (CDL-A or CDL-B), currently drive a CMV, be 21 years of age or older, and pass the motion sickness history screening questionnaire. As mentioned above, 100 participants participated in the driving simulator study. Fifty drivers have participated in the L2 study, and the other 50 drivers participated in the L3 study.



Study Participation

The study participants drive the heavy vehicle driving simulator which collects continuous data such as steering input, brake input, acceleration/deceleration, speed, stop sign/traffic light violations, major and minor crashes, curb strikes, near-crashes, and lane excursions. A data acquisition system called FlexDas (Managed and operated by VTTI) collects continuous video and simulator data during the driving scenarios. While active, the FlexDas is integrated to record data from the forward roadway simulation, the left-side and right-side simulations, a driver-facing camera, and an over-the-shoulder camera (when appropriate). The data is encrypted and stored on a removable solid-state drive within the FlexDas that can only be retrieved by select VTTI staff. Further, participants have received an anonymous Driver ID (e.g., Participant 001, 002, etc.) at the beginning of participation. The key information linking the Driver ID to the driver and the key information linking the driver to the PII data does not leave VTTI. Key information is stored in a limited access project folder. This key information is deleted at the end of the study. Role-based access controls are utilized to ensure appropriate data use, as described in NIST 800-53, AC-3(7). Levels of access are based on the least-privilege model.

Study Termination

All study data is maintained or destroyed in accordance with the approved Record Disposition Schedule (RDS). After the study ends, administrative data is destroyed at a predetermined date annually; this data includes participants' names, addresses, SSNs, etc. Administrative data is used to administer the study and ensure participant payment is lawfully completed. Study data, or non-identifying data collected while performing the study or calculated from data collected during the study, is processed for inclusion in FMCSA's Data Repository so that the datasets may be used for future analyses. Study data is further detailed below in the numbered list. This study results in two datasets that are included in FMCSA's Data Repository: (1) an anonymized, public-use dataset; and (2) limited access identifiable data. Each of these datasets is described below.

The publicly used/de-identified dataset featuring study data includes the following de-identified information:

1. *Reduced simulator performance data:* Data that has been identified as containing a safety-critical event and evaluated for contributing characteristics such as eyes off road, internal/external distraction, and fatigue.
2. *Eye-glance data:* Data collected via an eye-tracking technology to identify gaze patterns, glance locations, workload, etc.
3. *PVT data:* Reaction time data that determines fitness for duty.



4. *Questionnaire data:* Questionnaires are administered to obtain driver demographics as well as opinions related to each study.

Access to the identifiable data requires approval by FMCSA to ensure that data is made available only to qualified researchers. A qualified researcher can request access to identifiable data from VTTI via the Data Repository.

For access to be approved, the user must show proof of Institutional Review Board (IRB) approval and sign a Data Use License (DUL) with VTTI describing their need for identifiable data. The request must also be approved by FMCSA. Identifiable data may only be viewed in the secure data enclave located at VTTI. This dataset includes video containing images of the participant driver's face while operating the driving simulator.

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, 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.

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.

As this study requires the collection of data about human subjects, approval from Virginia Tech's IRB is required before data collection begins. This study was reviewed and approved by Virginia Tech's IRB (IRB #21-827). As part of the IRB process, an Informed Consent Form (ICF) was developed which details the participant's role in the study and how their data is protected. All ICFs discuss the possibility of PII being accessed by qualified researchers in a secure setting (i.e., the secure data enclave) and therefore by signing the ICF, participants agree to make their data available in this manner. The ICFs specify that a



public-use dataset is be posted online. An example of the ICF for this study has been included in Attachment A.

FMCSA informs the public that their PII is stored and used by the Data Repository via the data enclave through this PIA, published on the DOT website. 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.

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 opting into participation in the study, prospective participants are informed on what information is collected from participants. This is in addition to the information provided during the informed consent process to ensure the participant is capable of making an informed decision regarding the collection, use, and disclosure of their PII.

Since data is de-identified, there will be no way for participants to identify their data to ask for removal. Furthermore, when participants signed the ICF to participate in the study, they agree to allow their de-identified data to be posted online for future use. While all data shared on the website is 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.

FMCSA and the VTTI research team are unaware of other research conducted, currently or in the past, that could be used to fulfill the research goals of the Human Factors Considerations in CMV ADAS/ADSs project. A recently completed gap analysis by FMCSA on research involving ADAS/ADSs in CMVs found a minimal amount of existing research related to ADS-equipped CMVs. Much of the work relating to ADS technology involved passenger vehicles. However, the CMV environment is unique considering the physical vehicle differences, opposing use cases, and varying driver characteristics when compared to passenger vehicles. In general, the authors indicated that existing research lacks an understanding of safe and effective use of ADS-equipped CMVs on U.S. roadways and specific research needs.



Prospective participants are provided with the necessary information regarding the collection, use, and disclosure of their PII during the informed consent process. PII of participants is only used or disclosed under the terms outlined in the ICF.

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 determined that this collection of information is necessary for study completion; currently, there is no existing dataset that can be used for this project. Participant data is anonymized by assigning each participant a Driver ID (e.g., Driver 001) at the start of data collection. That driver ID is then linked to all driving data, safety-critical event data, FlexDas data, eye-tracking data, and questionnaire data. The only data collected during the study is the data that is needed to meet the study's objectives.

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 IRB activities and certain other records frequently held by investigators for at least three years after completion of the research (45 CFR 46.115(b)).

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 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 ICF signed by each participant. The ICF details the types of data collected and who may have access to the data in the future. This study only collects the data necessary to answer the research questions and that have been approved by Virginia Tech's IRB and approved via the Paperwork Reduction Act (PRA).

External researchers can request access to identifiable data by submitting a request on the website to the Data Repository. For access to be approved, the requester must show proof of IRB approval and sign a DUL with VTTI describing their need for identifiable data. The request must be approved by FMCSA. Identifiable data may only be viewed in the secure data enclave located at VTTI. Researchers cannot remove PII from the secure data enclave. All personal items are examined before the researcher can leave the secure data enclave to ensure no PII is removed.



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).

The Data Acquisition System (DAS) allows for the collection of high-quality behavioral data throughout the ADAS/ADS driver scenarios. Driving data, safety-critical event data, DAS data, and eye-tracking 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. Data included in the anonymized, public-use datasets are available for public download. Website users must log in so downloads can be tracked.

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. 5, Security and Privacy Controls for Federal Information Systems and Organizations, dated September 2020. 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](#) system are safeguarded in accordance with applicable rules and policies, including all applicable DOT automated systems' security and access policies. Strict controls are 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.

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 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.

Attachment A:

Informed Consent Form (ICF)



VTTI Informed
Consent Form (ICF)

Responsible Official

Theresa Hallquist
System Owner

Research Analyst, FMCSA

Prepared by: Pamela Gosier-Abner (FMCSA Privacy Officer)

Approval and Signature

Karyn Gorman
Chief Privacy Officer
Office of the Chief Information Officer