U.S. Department of Transportation

Privacy Impact Assessment

National Highway Traffic Safety Administration
Vehicle Research and Test Center (VRTC)

Questionnaire Tool for Independently Calculating Statistical Rates of Potential Safety Defects

Responsible Official

Bill Collins
General Engineer, NHTSA VRTC
(937) 243-2264
bill.collins@dot.gov

Reviewing Official

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer
privacy@dot.gov

Executive Summary

One of the responsibilities of the National Highway Traffic Safety Administration (NHTSA) is to ensure that motor vehicles throughout the United States and its Territories operate safely and within the requirements of the Federal Motor Vehicle Safety Standards (FMVSS). TheNHTSA Office of Defects Investigation (ODI) conducts investigations into alleged vehicle defects. NHTSA's Vehicle Research and Test Center (VRTC) is a Federal laboratory located on a proving ground in Ohio that physically inspects, tests, and recreates vehicle defect allegations to confirm whether the evidence of a defect is valid. To further assist ODI in conducting investigations, VRTC developed a voluntary questionnaire that contains two (2) to nine (9) questions relevant to a defects investigation. The questionnaire is sent to registered owners of the same make and model of vehicle under investigation. This PIA is necessary because PII in the form of names and addresses, and the Vehicle Identification Number (VIN) are required information on the questionnaire.

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

NHTSA receives information about possible vehicle safety defects from many sources around the country. NHTSA's Office of Defects Investigations (ODI) is responsible for investigating and enforcing recalls of safety defects in

[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).

vehicles operating on US roadways. Safety defect information is gathered and analyzed to determine whether an investigation should be opened. Based upon additional information gathered during the investigation, ODI will determine whether an unreasonable risk to safety exists due to the alleged defect, and whether the manufacturer is required to conduct a safety recall.

NHTSA's Vehicle Research and Test Center (VRTC) is the agency's in-house laboratory. VRTC conducts research, and vehicle and equipment testing in support of NHTSA's mission to save lives, prevent injuries, and reduce traffic-related health care and other economic costs. Studies performed by VRTC cover the areas of crash avoidance, crashworthiness, biomechanics, and defects analysis. The Defects Analysis engineers support the agency's work to identify and correct safety-related defects in motor vehicles and motor vehicle equipment, and to ensure that recalls are effective and conducted in accordance with Federal law and regulations. To further support the work, VRTC Defects Analysis developed an outreach questionnaire for defect investigations, where additional vehicle field data are collected and used to assist in ODI's safety defect determinations. The questionnaire typically contains two (2) to nine (9) questions that are relevant to the defects investigation. VRTC sends the questionnaires via U.S. mail to a sample of approximately 500 to 3,000 registered owners of the make and model of vehicle under investigation. This questionnaire creates at least two statistically valid metrics: 1) issues reported per total questionnaires mailed; and 2) issues reported per total number of responses. These results assist ODI in determining the existence of a defect. This information may support the agency's position that a safety recall be conducted or support a finding that a safety defect is not evident, and that the investigation should be closed.

In order to obtain the contact information of potential consumers to whom to send the questionnaires, VRTC contacts the state bureau of motor vehicles (usually Ohio's BMV) to request a search for registered vehicles matching the make, model, and year of vehicle subject to the ODI investigation. The BMV provides a service to match letter and number patterns in the vehicle identification number (VIN) with registration records and outputs those matches to a digital file. BMV then sends the file to VRTC via a secure FTP site. For each vehicle identified, the data will contain the VIN, make, model, and owner's name and address.

After obtaining the file from the BMV, VRTC uses the data to send the questionnaire via US mail to the owners of the vehicles identified. This questionnaire is comprised of two to nine questions. The questionnaire includes a field for a narrative response that the consumer can use to voluntarily describe details of any incidents concerning the subject safety issue. The questionnaires request contact information, but clearly state that providing such information or even responding is optional. Consumers' responses include "yes" or "no" responses and spaces for voluntary follow-on comments related to consumers' experiences with the potential safety issue under investigation. Consumers are requested to complete the questionnaire and return it via postage-paid mail. Upon receipt of the questionnaire, VRTC manually enters the data into a database where it will be reviewed for information such as a crash or injury that may have been caused by the alleged defect under investigation. When a questionnaire indicates a potential safety incident, VRTC will contact the consumer to verify the claim. After enough responses are received and incidents are validated, a statistical summary of vehicle conditions is produced that indicates metrics to support the agency's investigation. The statistical work is related to vehicles and does not make any reference to participating consumers.

The database is stored on the privileged "Defects Analysis Group" network drive at the VRTC in Ohio. Permission for access to this drive is limited to people on-site who are involved with the analysis of defects for NHTSA at VRTC, all of whom are either NHTSA employees or contractors.

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 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.

Each questionnaire introduces the agency, its mission, and the details and objective of the investigation. The consumer's rights protected by Privacy Act of 1974 are briefly explained. Consumers are provided with the name of a project engineer in the Defects Analysis group. They are also provided with the main telephone number for VRTC, 937-666-4511, and instructed to call if they have questions or want to express concerns about the investigation.

Additionally, NHTSA informs the public that their PII is stored and used through the publication of this Privacy Impact Assessment, which identifies the information collection's purpose and uses of the PII stored and can be found at: https://www.transportation.gov/privacy

Individual Participation and Redress

DOT should provide 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 be provided reasonable access to their PII and the opportunity to have their PII corrected, amended, or deleted, as appropriate.

The collection of the data occur primarily at the state level with the BMV and VRTC receives a version of the data that is filtered to only provide vehicle information, name, and address. The consumer can make the decision to not participate in further data collection or use by not responding to the questionnaire. The questionnaire briefly explains the purpose for which the information will be used. VRTC also provides a contact name and phone number if a consumer has concerns or questions. If the consumer responds and requests that their data be updated or deleted, VRTC complies with their request.

Additionally, an individual can contact a responsible NHTSA staff member to address a privacy concern or data inaccuracy by writing to NHTSA.Privacy@dot.gov

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.

Authorities: National Traffic and Motor Vehicle Safety Act 1966, CFR Part 510 and Part 554.

Data are collected to identify and communicate with consumers who may be or may have been operating a motor vehicle with a safety defect that may have caused or may cause harm. The gathered vehicle information will be used

[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

to inform the agency of whether a safety defect exists and whether a recall should be conducted. The information is used exclusively to gather data related to potential vehicle safety defects.

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. DOT should retain PII for only as long as necessary to fulfill the specified purpose(s) and in accordance with a National Archives and Records Administration (NARA)-approved record disposition schedule. Forms used for the purposes of collecting PII shall be authorized by the Office of Management and Budget (OMB).

VRTC collects, uses, and retains only the data elements that are relevant and necessary for the purpose of identifying vehicles that may have a potential safety defect. The data is also used to support or refute evidence of the defect. Name and address information is used only to contact consumers in order to gather such evidence. Data collected pursuant to an investigation are maintained in a spreadsheet or database while the questionnaires are being developed and processed. The investigation is typically completed within three years. Safety defect questionnaires , typically, have been maintained for at least 10 years. As this information pertains to a Federal investigation, the retention period is expected to remain the same under the new NARA-approved retention schedule that has been requested by NHTSA. It should be noted that the name and address of the consumer become considered extraneous to the investigation once it is closed, and and are typically deleted 6 months to 3 years after their collection.

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.

Access to data is restricted to employees and stored on a drive with limited access at VRTC. Name and address are typically deleted once the investigation is closed. Once the investigation is complete the data is archived, as it serves no other purpose and is not used in any other capacity.

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).

Incorrect address information received from the BMV will preclude VRTC from contacting consumers. Responses will not be collected unless the questionnaire successfully reaches consumers and they choose to respond. To prevent external manipulation, data are stored on one, limited access drive at VRTC. The possible responses to the questionnaire are typically limited to "yes" or "no" for simplicity and to minimize the potential for error. Name or vehicle ownership errors are corrected when the respondent provides the requested corrections in the comments section of their response. VRTC also provides a contact name and phone number if a consumer has concerns or questions. If the consumer responds and requests that their data be updated or deleted, VRTC complies with their request.

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.

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. 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 and acceptable levels.

Under this policy NHTSA has implemented appropriate Administrative, Physical and Technical safeguards to protect the confidentiality, availability and integrity of the system and information. Controls contributing to the protection of PII confidentiality include, but are not limited to, the requirement that all federal employees and contractors undergo appropriate background checks prior to being granted access to the DOT network.

Additionally, VRTC utilizes role-based security to restrict user access to application functions and the information required to meet their job function.

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 the organization's personnel accountable for adhering to the DOT and NHTSA privacy and security policies and regulations. NHTSA follows the Fair Information Principles as best practices for the protection of PII. The current practices, policies and procedures will be 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 privacy data. Guidance is provided in the form of mandatory annual privacy awareness training. The NHTSA Security Officer and 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 Stategic Resource.

Responsible Official

Bill Collins
General Engineer, NHTSA VRTC

Approval and Signature

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer