National Highway Traffic Safety Administration
Docket No. NHTSA–2016–0090, www.nhtsa.gov/AV
Accelerating the Next Revolution in Roadway Safety

Guidance and Recommended Best Practices: Safety-Related Defects, Unreasonable Risk, and Automated Safety Technologies

Robert Thibadeau, Ph.D., Lucy Thomson, Esq., CISSP, CIPP/US/G,
and Michael Willett, Ph.D.

Drive Trust Alliance, www.drivetrust.com

Comments on Privacy Issues in Federal Automated Vehicles Policy

NHTSA published the Federal Automated Vehicles Policy *Accelerating the Next Revolution in Roadway Safety* in the Federal Register requesting public comments by November 22, 2016.

To aid NHTSA in monitoring highly automated vehicles (HAV), the Agency will request that manufacturers and other entities voluntarily provide reports regarding how the Guidance has been followed. This reporting process may be refined and made mandatory through a future rulemaking. It is expected that this would require entities to submit a Safety Assessment to NHTSA for each HAV system, outlining how they are meeting this Guidance at the time they intend their product to be ready for use (testing or deployment) on public roads.

Among other issues, the Safety Assessment would address the issue of Privacy.[1] We recommend that certain essential privacy requirements regarding the use of encryption be specifically required in the Guidance.

---

[1] 2. Privacy (Guidance pages 21-22).

The Department and the Administration strongly believe in protecting individuals' right to privacy. This is exemplified by the White House Consumer Privacy Bill of Rights and the Federal Trade Commission's privacy guidance. In November 2014, the Alliance of Automobile Manufacturers and the Association of Global Automakers published Privacy Principles for Vehicle Technologies and Services. Given these available resources, HAV manufacturers and other entities, either individually or as an industry, should take steps to protect consumer privacy.

Manufacturers' privacy policies and practices should ensure:

a. **Transparency**: provide consumers with accessible, clear, meaningful data privacy and security notices/agreements which should incorporate the baseline protections outlined in the White House Consumer Privacy Bill of Rights and explain how Entities collect, use, share, secure, audit, and destroy data generated by, or retrieved from, their vehicles;

b. **Choice**: offer vehicle owners choices regarding the collection, use, sharing, retention, and deconstruction of data, including geolocation, biometric, and driver behavior data that could be reasonably linkable to them personally (i.e., personal data);

c. **Respect for Context**: use data collected from production HAVs only in ways that are consistent with the purposes for which the data originally was collected (as explained in applicable data privacy notice/agreements);

We agree that manufacturers' privacy policies and practices should protect personal data by providing transparency, choice, respect for context, minimization, de-identification and retention, data security, integrity and access, and accountability. However, it is not enough to merely enunciate broad principles. Certain essential privacy requirements should be specified in the Guidance.

In this developing area, huge volumes of personal data about drivers and passengers in vehicles, including geolocation, biometric, and driver behavior data, will be created. While the use of sensitive personal data may be essential for the safe operation of UAV at the time the vehicle is in use, these data should always be private, secure, and disposed of at the earliest appropriate time.

As HAV levels expand and become more sophisticated for the desired automation and safety required, we can be sure there will be catastrophic violations of personal information privacy in violation of the spirit of the privacy guideline. Yet these catastrophes are fully predictable. The collection of person data in this context has many ramifications, both foreseen and unforeseen. The guidelines need to at least reflect controls that we know we can foresee. The need for privacy safeguards is heightened over the existing proposed guideline.

Because of the nature of this technology, the use of HAVs presents very serious risks to the privacy of the owner(s), operator(s), and, by the way, passenger(s) in the vehicles. As the use of HAVs expands, the collection of private data may grow as well. Individuals in HAVs should have industry standard privacy with respect to where they have been, what they have been doing, and their actions and conversations when they are in or near the vehicle. This privacy sensitive data should be used solely for the safe operation of the vehicle.

---

d. **Minimization, De-Identification and Retention**: collect and retain only for as long as necessary the minimum amount of personal data required to achieve legitimate business purposes, and take steps to de-identify sensitive data where practical, in accordance with applicable data privacy notices/agreements and principles;

e. **Data Security**: implement measures to protect data that are commensurate with the harm that would result from loss or unauthorized disclosure of the data;

f. **Integrity and Access**: implement measures to maintain the accuracy of personal data and permit vehicle operators and owners to review and correct such information when it is collected in a way that directly or reasonably links the data to a specific vehicle or person; and

g. **Accountability**: take reasonable steps, through such activities as evaluation and auditing of privacy and data protections in its approach and practices, to ensure that the entities that collect or receive consumers' data comply with applicable data privacy and security agreements/notices.

Encryption Privacy Protections – The current guidance fails to reflect learning in other industries. In existing computing, including servers, desktops, laptops, pads, phones, and, to a much lesser degree, IoT, there is a developed and deployed technology for data protection associated with encryption to protect individual, corporate, and governmental privacy. Whether or not the privacy of sensitive personal data are protected will depend on the implementation of specific technologies and policies that we believe should be explicitly required in the guidance.

There are three use cases, or policies, that need to be added to the existing privacy guidance. It is no accident, given the maturity of the technologies for the three use cases in other industries, that these use cases will be familiar to many people. For example, all iPhones and (newer) Android phones exhibit these protections, and the guidelines should require them on all appropriate HAV vehicles (HAV Levels 1-5)

1. ***Repurposing a Vehicle*** – When a vehicle is repurposed to a different owner or driver, whether this be a family, company or other organization, all individual or organizational data about owners, drivers and passengers should be erased, bringing the vehicle, in fact, back to factory state with respect to sensitive personal data. Where appropriate, this permanent erasure can be individualized for particular people or roles. In modern phones and pads and many other devices such as servers, this involves fast crypto-erasure. A new vehicle owner should not know what an individual or family member has been doing in the car in past years. Similarly, a corporation or other organization with a fleet of vehicle will want all records erased when transferring the vehicle to another organization. All personal data from the vehicle that may be stored in the cloud or other technology platform should be deleted as well.

2. ***Multiple Drivers*** – In a vehicle with multiple drivers, only the personal information of the person driving, and the people riding, should have their data unlocked for reading and writing. We already use keys, and in the future with higher levels of HAV, the HAV will identify all the passengers. For example, the HAV needs to know to ignore a “stop!” scream from an eight-year-old.

3. ***Central Management Privacy Guarantees*** – We know from experience that a remote, cloud manager is essential for privacy protection. This way the HAV can be proven to have been protected even if it is stolen, lost, or under the control of others such as vehicle servicers. In the medical industry such central management is essential in providing confidence that patient data is not compromised. This protection, called “central management of privacy guarantees” is required whether the vehicle is an individual, family, or organizational vehicle.

The guideline today only requires a Privacy Statement, not its contents. Even if a Privacy Statement is provided for a vehicle, it may well not be adequate. It must provide explicit minimal standards for the protection of privacy, and the three use cases described above must be affirmatively asserted. We recommend that these be added to the Privacy Guidance.

The Drive Trust Alliance

www.drivetrust.com

Also see www.drivetrust.com/autoerase

	Bright Plaza, Inc., through its operation of the Drive Trust Alliance (DTA) (www.DriveTrust.com), has an educational and technical mission to improve adoption of hardware-encrypting storage technologies. These include Apple iOS devices and Trusted Computing Group (www.trustedcomputinggroup.org/storage) self-encrypting drive technologies. The DTA website provides an authoritative single resource on these technologies, including a complete suite of open-source software for managing hardware encryption on Windows, Macs, and Linux.
	**Robert Thibadeau**, *Ph.D., Chairman and CEO of Bright Plaza, Inc.* Dr. Thibadeau invented self-encrypting drives (SEDs) and lead their commercialization in his tenure as Chief Technologist of Seagate Technology (2002-09). He also served as Chair of the Storage Workgroup in the Trusted Computing Group that standardized SEDs globally. Dr. Thibadeau is an Adjunct Professor in the School of Computer Science at Carnegie Mellon University where he has taught IT Security since 1997. He was a founding Director of the Robotics Institute at CMU from 1980-2008. He is the inventor on over 25 U.S. patents and holds degrees from Emory University and the University of Virginia. Contact: rht@drivetrust.com
	**Lucy L. Thomson**, *Esq., M.S. CISSP, CIPP/US/G, Chief Counsel and Board Secretary* Ms. Thomson focuses her legal practice on cybersecurity, global data privacy, and compliance and risk management. She is principal of Livingston PLLC, Washington, D.C. and worked as a senior engineer at CSC, a global technology company. A career Justice Department attorney, Ms. Thomson managed and conducted complex litigation in the Criminal and Civil Rights Divisions. She was 2012-13 Chair of the American Bar Association (ABA) Section of Science & Technology Law. She earned a Master's degree from RPI and holds a J.D. degree from Georgetown.
	**Michael Willett,** *Ph.D. VP of Marketing* As a Senior Director for Seagate Research, Dr. Willett managed security functionality on hard drives, self-encryption, related standardization, product rollout, patent development, and partner liaison. He has had previous tenures with IBM as a design architect for the IBM Cryptography Competency Center, as well as Fiderus, a privacy and security consulting firm. He served as Chair of the OASIS Privacy Management Reference Model Technical Committee (PMRM TC) where he developed an operational reference model for implementing privacy requirements. He holds degrees from the U.S. Air Force Academy and N.C. State University.