

EV + AI Panel – CLE Resources

Table of Contents

Introduction to AI in Vehicles

- [FPF Infographic](#) (2024)
- [FPF Vehicle Safety Systems Report \(2024\)](#)
- [Consumer Privacy Principles for Vehicle Technologies Services-03-21-19.pdf](#) (autosinnovate.org)

Evolving EU Regulations Affecting AI in the Automotive Context

- [Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications](#)
- [UN Regulation No. 155 - Cyber security and cyber security management system | UNECE](#)
- [EC Background on Vehicle Safety](#)

US Self-Regulatory Standards

- [NHTSA Self Certification Guidelines](#)

Global Regulatory Focus on AI + Data Minimization

- [IAPP's Global AI Law and Policy Tracker](#)
- [EU AI Act](#)
- [Colorado AI Act](#)
- [CPPA Data Minimization Enforcement Advisory](#)
- [Drizly Consent Order \(ftc.gov\)](#)

DATA and the CONNECTED VEHICLE

Version 2.0

Today's vehicles include many new features enabled by the collection and processing of data. These connected technologies are making transportation safer and more convenient. To foster a trusted mobility ecosystem, it is vital to ensure appropriate and secure data flows between a network of carmakers, vendors, and others to support individuals' safety, logistics, and infotainment needs. This infographic demonstrates a range of devices that may be employed in today's connected vehicles and highlights the type of data and AI to operate different systems. Few cars have all of these features, but most new cars will have some. Much connected car data is protected by technical controls, laws, self-regulatory commitments, privacy policies, and other emerging mechanisms or controls. For more information, visit fpf.org/mobility.

Produced by FPF.ORG



DATA HANDLERS

A growing number of entities receive and transmit data through the connected vehicle ecosystem



WIRELESS CONNECTIVITY

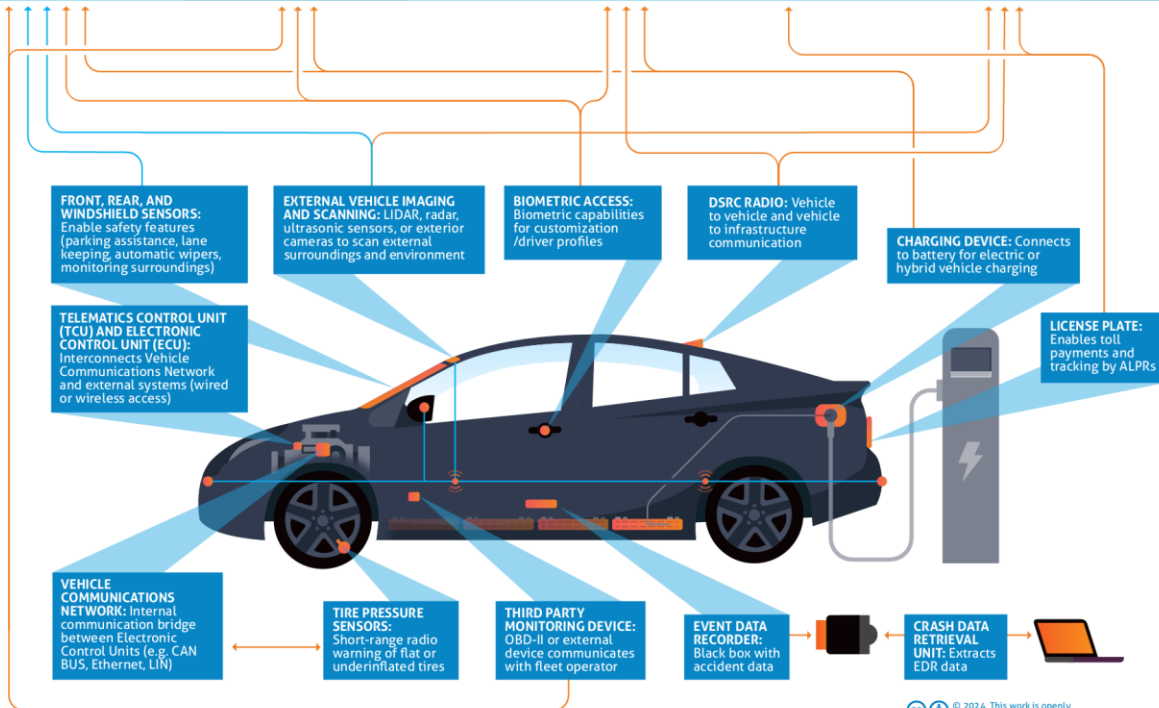
- CELLULAR
 - CELLULAR V2X/DSRC
 - SATELLITE/GPS
 - SHORT RANGE RADIO
- NON-CELLULAR
 - BLUETOOTH
 - WIFI
 - CELLULAR V2X/DSRC
 - SATELLITE/GPS
 - SHORT RANGE RADIO

TYPES OF DATA

- VEHICLE & SAFETY**
Can include: Vehicle diagnostic and health data (CPU health, oil pressure) vehicle data, driver assistance systems, and battery and charging data
- OCCUPANTS**
Can include: Occupant's physical characteristics, driver monitoring systems (speed, seat belt use, etc.), and driver preferences (climate control, seat position, etc.)
- LOCATION**
Can include: Precise geographic location of the vehicle and/or other location data like vehicle surroundings and location flags
- ACCOUNT**
Can include: Personal accounts established by vehicle users (mobile apps, car-related accounts, etc.)
- BIOMETRIC & BODY-RELATED**
Can include: Information from interior or exterior sensors about the physical characteristics of occupants or those nearby (fingerprints, faceprints, etc.)

DATA PROCESSING

- ARTIFICIAL INTELLIGENCE**
Can include: Algorithmic processing, decision making, and machine learning present throughout various vehicle systems and features



CC BY 4.0 © 2024. This work is openly licensed via CC BY 4.0.

DATA and the CONNECTED VEHICLE

Version 2.0

Today's vehicles include many new features enabled by the collection and processing of data. These connected technologies are making transportation safer and more convenient. To foster a trusted mobility ecosystem, it is vital to ensure appropriate and secure data flows between a network of carmakers, vendors, and others to support individuals' safety, logistics, and infotainment needs. This infographic demonstrates a range of devices that may be employed in today's connected vehicles and highlights the type of data and AI to operate different systems. Few cars have all of these features, but most new cars will have some. Much connected car data is protected by technical controls, laws, self-regulatory commitments, privacy policies, and other emerging mechanisms or controls. For more information, visit fptf.org/mobility.

Produced by FPTF.ORG



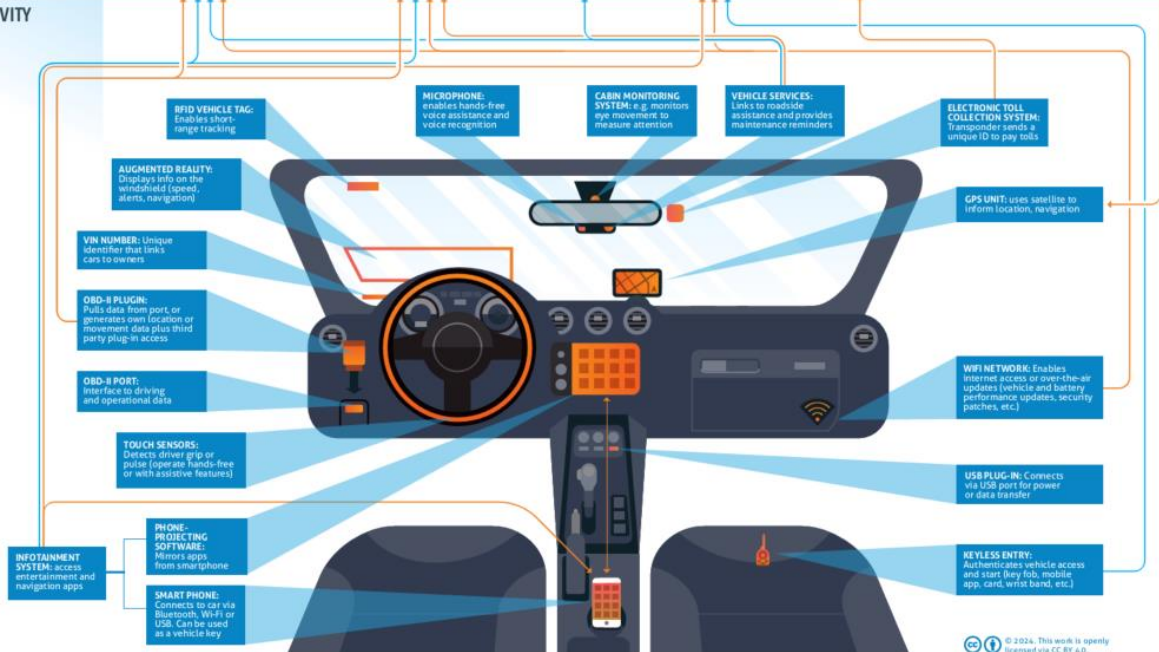
DATA HANDLERS

A growing number of entities receive and transmit data through the connected vehicle ecosystem



WIRELESS CONNECTIVITY

- CELLULAR
- NON-CELLULAR
 - BLUETOOTH
 - WIFI
 - CELLULAR V2X/DSRC
 - SATELLITE/GPS
 - SHORT RANGE RADAR



© 2024. This work is openly licensed via CC BY 4.0.

MARCH 2024

VEHICLE SAFETY SYSTEMS

Privacy Risks and Recommendations



AUTHORED BY

Adonne Washington

Policy Counsel, Mobility, Location, and Data
Future of Privacy Forum

EDITORS

Amie Stepanovich

Vice President for U.S. Policy, Future of Privacy Forum

John Verdi

Senior Vice President for Policy, Future of Privacy Forum

ACKNOWLEDGEMENTS

The author would like to thank Jordan Wrigley, Shea Swauger, Stacey Gray, Lee Matheson, Niharika Vattikonda, Angela Guo, Nancy Levesque, Payal Shah, and the many experts and stakeholders whom were consulted for their contributions to this report.



The Future of Privacy Forum (FPF) is a non-profit organization that serves as a catalyst for privacy leadership and scholarship, advancing principled data practices in support of emerging technologies. Learn more about FPF by visiting fpf.org.

TABLE OF CONTENTS

EXECUTIVE SUMMARY	2
INTRODUCTION	4
I. Overview of Current and Emerging Vehicle Safety Systems	4
A. Vehicle Safety Systems and How They Work Together	4
B. Overview of Current and Emerging Impairment-Detection Technologies	5
II. Privacy and Security Risks	7
III. Background on the Congressional Mandate to Prevent Impaired Driving	8
A. Purpose of the Mandate and Political Process	8
B. Scope and Timeline of the Mandate	9
C. NHTSA Authority and Responsibility	9
IV. Public Awareness and Attitudes Toward Vehicle Safety Systems	9
A. Many Drivers Value Vehicle Safety Technologies, While Worrying About the Privacy Risks	9
B. Individuals Generally Trust Carmakers' Data Practices More than Online Companies and the Government, but Worry About Vehicle Safety Systems that Collect Information About Occupant Behaviors	10
C. Most Drivers Support the Use of Impairment-Detection Technologies, but have Concerns about Accuracy, Cost, and Data Disclosures to Third Parties	10
D. Individuals Say that Privacy and Data Protection Practices Like Disclosure Limits, Encryption, On-Car Storage, and De-Identification are "Must Haves" for Vehicle Data	11
V. Recommendations for Impairment-Detection Technologies in Vehicles	11
VI. Conclusion	13
APPENDIX	14
ENDNOTES	20

EXECUTIVE SUMMARY

Today's vehicles are equipped with sophisticated safety technologies, from airbags and automatic braking systems to sensors that can help keep vehicles in their lanes and prompt drivers to keep their eyes on the road. Carmakers are developing and offering ever more advanced anti-collision features that can protect drivers, passengers, pedestrians, and others.

Increasingly, these safety systems rely on data about vehicles and their occupants in order to operate. Some of this information is not personal, relates to regular vehicle operation, and raises few privacy risks. However, other safety system data can raise substantial privacy risks, and vehicle occupants (or owners) may be harmed if the risks are not well managed through appropriate legal, policy, and technical safeguards. The risks can be particularly acute when vehicle safety systems collect sensitive personal information, such as biometric data, or make sensitive inferences, such as inferring drivers' potential impairment or to measure and quantify impairment. In addition, the risks can be particularly widespread when these technologies are legally mandated.

One group of Vehicle Safety Systems is known as Advanced Driver Assistance Systems (ADAS). ADAS are primarily focused on collision avoidance technologies such as blind spot detection or front crash protection. ADAS technologies monitor driver input and the environment around the vehicle and warn the driver of the possibility of a crash. ADAS also include driver aids such as night vision and adaptive cruise control. Advanced ADAS may intervene momentarily to automatically brake or steer the vehicle if the driver does not act. Next-generation ADAS may leverage wireless network connectivity by using car-to-car communications.

Another group of Vehicle Safety Systems are called Driver Monitoring Systems (DMS). These systems use in-cabin-focused cameras and other sensors to infer the driver's fitness to drive. DMS assess the driver's alertness by monitoring a driver's eye gaze, eye movement, posture, driving performance, and other sensitive data in combination with proprietary software to infer when vehicles are being operated safely or unsafely. Similar to ADAS, DMS provide visual, haptic, and/or audible alerts to drivers and can intervene momentarily to automatically avoid collisions should the driver fail to respond to an alert.

An ADAS or DMS may be turned off or ignored by a driver, for example, when it erroneously detects a hazard.

One final vehicle safety system is the Alcohol Detection System (ADS), which can directly measure and/or quantify a driver's blood or breath alcohol concentration. Like ADAS and DMS, ADS may provide a warning to the driver or intervene to prevent or inhibit vehicle operation if a driver's alcohol concentration is above a preset limit, such as the per se legal limit of 0.08 adopted by every state but Utah (which has adopted a 0.05 limit). The technology developed by the Driver Alcohol Detection System for Safety (DADSS) Program is an example of an ADS system. Similar to DMS, ADS assesses a driver's fitness to drive.

Finally, ADAS, DMS, and ADS (collectively "Vehicle Safety Systems") may be installed in vehicles as separate, discrete systems or used in combination to enhance detection of impaired drivers and provide added customer value. The individual technologies developed and used to detect different types of driver impairment are referred to as Impairment-Detection Technologies.

Personal or biometric data from ADAS, DMS, and ADS are mainly used to reduce crash risk, but could also be used to reconstruct crash events, assist in determining crash causality and responsibility, price insurance, or for other uses. Some data may be commercially valuable, either because it enhances product development by carmakers or is useful to third parties. Regulators acknowledge that many in-vehicle technologies create tensions between occupant safety and privacy interests while recognizing that consumer acceptance and adoption are key components of successful implementation of safety technologies. Stakeholders have successfully navigated these tensions in the past. For example, mandatory automobile event data recorders have assisted in crash investigations, product recalls, and other safety efforts for decades while minimizing privacy risks; EDR data fields are standardized to include only essential information, recording time is strictly limited, and data is stored on-vehicle.

Regulators increasingly turn to Vehicle Safety Systems to reduce dangerous driving, including impaired driving. Notably, Congress has mandated that National Highway Traffic Safety Administration (NHTSA) conduct rulemaking on the inclusion of Impairment-Detection Technology in future new

vehicles, the United States Department of Transportation (USDOT) has initiated rulemaking to implement Congress' mandate, and similar efforts are underway in other countries worldwide.

USDOT's efforts to mandate the installation of Impairment-Detection Technology in every new car and light truck sold in the U.S. must be accompanied by strong, practical measures that ensure the privacy of drivers, passengers, and others. Different types of these technologies require different privacy protections, but it is clear that meaningful legal, policy, and technical safeguards are needed. Such safeguards must take account of the practical limitations and opportunities of current Vehicle Safety Systems and be flexible enough to accommodate rapidly evolving technologies. Depending on the context, appropriate safeguards could include legal protections codified in statutes or rules, contractual limits on data use and transfers,

enforceable public promises regarding data practices, or technical measures that minimize data collection, de-identify data, or delete information on an appropriate schedule.

In light of the growing use of Vehicle Safety Systems generally, as well as USDOT's impairment-detection efforts specifically, FPF analyzed the relevant technologies and business practices, consulted with experts, and surveyed the public regarding the intersection of these important safety and data protection issues. Our work identifies 5 core recommendations for organizations building, implementing, and regulating these technologies. It is clear that advanced Vehicle Safety Systems can save lives and reduce injuries. It is equally clear that personal data used by those systems must be handled with the utmost care in order to protect drivers and ensure drivers trust and accept Vehicle Safety Systems and other emerging technologies.

FPF Recommends

1. Regulators, technology developers, and technology deployers should ensure that privacy is a foundational principle for Impairment-Detection Technologies and should implement appropriate legal, policy, and technical safeguards when personal information is implicated, including safeguards to:
 - Minimize the collection and retention of personal data;
 - Process and store personal data on vehicles when possible, with strict limits on off-device data use by Impairment-Detection Technologies;
 - Set reasonable retention limits of data from Impairment-Detection Technologies;
 - Provide robust access and deletion options;
 - Secure personal data at rest and in transit; and
 - Set reasonable limits of data use and third party sharing, including bars on sharing personal impairment-detection data or using that information for other purposes.
2. Technology developers and technology deployers should de-identify data collected by Impairment-Detection Technologies as appropriate.
3. Impairment-detection systems should be accurate, should be tested for potential bias, and should not produce false-positive results more often for people from underrepresented, marginalized and multimarginalized communities. Well-defined standards for consistent deployment and alignment across the industry may be beneficial.
4. Driver acceptance should be promoted through transparency about the systems' functions and operations, as well as the handling of personal data.
5. Regulators, technology developers, and technology deployers should identify and mitigate, to the extent possible, potential future harms to drivers, especially to people from underrepresented, marginalized and multimarginalized communities.

INTRODUCTION

Vehicle manufacturers continue to integrate technology into their products, with the resulting advanced capabilities intended to provide drivers with greater safety, better user experience, and increased convenience. For instance, many vehicles sold today contain Advanced Driver Assistance Systems (ADAS) and Driver Monitoring Systems (DMS) for the general purpose of providing extra safety to drivers. In the future, these technologies and Alcohol Detection Systems (ADS) (collectively Vehicle Safety Systems), along with other related tools to detect impairment, are likely to gain new traction. Mandates within the 2021 Infrastructure Investment and Jobs Act (Infrastructure Act), also known as the Bipartisan Infrastructure Law (BIL), direct the National Highway Traffic Safety Administration (NHTSA), the regulator for highway and vehicle safety, to establish a federal motor vehicle safety standard (FMVSS) requiring certain vehicles are equipped with “advanced impaired driving prevention technology.” To ensure public support and adoption of these systems, it is important that NHTSA use the rulemaking process to highlight privacy risks for newer safety systems and provide data protection and privacy guidance to those developing and implementing new technologies.

Reconciling safety measures with privacy risks can become challenging when the safety features require the collection and processing of personal data about drivers and vehicle occupants, which can raise or exacerbate risks for those individuals.¹ Yet, with proper safeguards, data can be protected. Privacy risks, therefore, should be considered prior to the implementation of any new technology, including for safety features and functions. To further explore the intersection of vehicle safety technologies and privacy, the Future of Privacy Forum (FPF) conducted a survey in 2023 in partnership with the Automotive Coalition for Traffic Safety (ACTS) on public understanding and attitudes toward the technology, as well as their trust in those systems and perception of data collection and associated privacy risks. The results of that survey found, among other things, that drivers have an interest in technology for safety but are concerned about the accuracy of the technology and the privacy implications.

The outcome of the rulemaking initiated by NHTSA will be crucial to ensuring that the public is able to benefit from safety systems while mitigating the privacy risks to vehicle occupants. In the rest of this report, we will more thoroughly detail the history and scope of the current Congressional mandate to prevent impaired driving, examine the technology behind common Vehicle Safety Systems that are designed to detect driver impairment (Impairment-Detection Technologies), analyze the privacy risks associated with those systems, and, finally, issue recommendations for ensuring the mitigation of those risks in any final standards requiring the use of such systems in vehicles.

I. Overview of Current and Emerging Vehicle Safety Systems

Modern passenger vehicles currently integrate several different types of technology with the express purpose of increasing driver safety and preventing motor vehicle crashes. Vehicle Safety Systems include technologies that assist drivers in the safe operation of a vehicle, with some having specific driver monitoring capabilities.² Of these, Advanced Driver Assistance Systems (ADAS) and Driver Monitoring Systems (DMS) are the most commonly used suites of technologies, though there is variation in how they are defined throughout the vehicle industry.³

A. Vehicle Safety Systems and How They Work Together

ADAS in vehicles can include several features, such as collision warning, collision intervention, driving control assistance, or parking assistance. ADAS are generally designed to provide various levels

of assistance to drivers. ADAS may also include technology capable of monitoring drivers, and consequently Driver Monitoring Systems (DMS) can be part of ADAS. However, DMS are not necessarily ADAS, and may stand on their own when they are not intended as a driver-assistance tool.

ADAS and DMS may be used in combination with one another to provide various features. ADAS systems can operate without DMS, such as in ADAS that use a vehicle’s location or roadway position to issue lane departure warnings or provide lane-keeping assistance systems.⁴ Other ADAS include DMS as a central component. For instance, eye-tracking technology that uses gaze direction and eyelid movement analysis may determine driver attentiveness in order to alert drivers to warning signs of impairment.⁵ It can be paired with other technology, such as facial detection, characterization, or recognition. DMS can identify the individual driving or determine safety conditions inside or outside of the vehicle.⁶ The ADAS may then display a notice on the dash or infotainment system to alert the driver that they may be in an unsafe situation.⁷

Both ADAS and DMS can be programmed to respond to triggers with a series of escalating actions, for instance beginning with a driver alert or warning. Additional technologies are in the research and development phase that could intervene if the triggering behavior, such as lane departure, continues based upon the technology determination.⁸

One final vehicle safety system is the Alcohol Detection System (ADS), which can directly measure and/or quantify a driver's blood or breath alcohol concentration. Like ADAS and DMS, ADS may provide a warning to the driver or intervene to prevent or inhibit vehicle operation if a driver's alcohol concentration is above a preset limit, such as the per se legal limit of 0.08 adopted by every state but Utah (which has adopted a 0.05 limit). The technology developed by the Driver Alcohol Detection System for Safety (DADSS) Program is an example of an ADS system. Similar to DMS, ADS assesses a driver's fitness to drive.

B. Overview of Current and Emerging Impairment-Detection Technologies

One frequent goal of ADAS, DMS, and ADS can be to identify driver impairment whether by alcohol, drugs, inattention, or drowsiness. Impairment refers to the deterioration of a driver's ability to safely perform the driving task, either through a driver's physiological and cognitive impairment or their blood alcohol content (BAC).⁹ A driver's performance in standardized field sobriety tests (SFST) or other observed behavior are commonly used when direct measurement of a driver's BAC is not possible.¹⁰ ADAS and DMS systems aimed at detecting driver impairment utilize multiple metrics.¹¹ For instance, some may be designed to directly detect driver intoxication levels through BAC or Carbon Dioxide (CO₂) readings to determine impairment. However, others might infer intoxication by combining one or more systems.¹² Traditional signs of impaired driving (closed eyes, erratic lane-swerving) may be used as a proxy to indicate that a driver may be impaired.¹³ Furthermore, the same signs of impairment can also be indicative of other causes such as sleepiness, as well as certain medical conditions. Impairment may not be determined, however, when intoxicated drivers do not show any signs of intoxication.

Today, the use of some methods of in-vehicle intoxication detection, namely Breath Alcohol Ignition Interlock Devices (BAIIDs), are often court-ordered following a driver's conviction for driving under the influence of alcohol.¹⁴ Devices subject to court orders

may also include logging functions, which can be used in reports back to the mandating agency or judge. In addition to mandated devices, however, individuals can also voluntarily purchase and install these devices in vehicles.¹⁵ This may be done for any number of reasons, including as a way for transport company managers or personal vehicle owners to enforce limits on other known drivers, out of a desire for external forcing functions, or in response to incentives from insurance companies.

1. Breath

a. Breath Alcohol Ignition Interlock Devices (BAIID or "Breathalyzer")

An aftermarket BAIID is about the size of a cell phone and is wired to a vehicle's ignition.¹⁶ After installation, the ignition interlock device requires the driver to provide a breath sample directly into the device through a tube before the engine starts. If the ignition interlock device detects alcohol, the engine will not start. These devices may also require periodic breath samples while driving, requiring the driver to stop and breathe into the device while on their trip. Certain forms of BAIIDs may also include a camera to record the driver while using the device. Often, a BAIID is designed to log sample data and readings from the use of the device, and sometimes the system can also track the length of time on the road, and any attempts to "disable or circumvent" the device.¹⁷ Creating a log of alcohol intoxication readings may be necessary for court order, but may also raise privacy risks in other contexts due to the sensitive nature of the data. It should be noted that in the most recent review of all technologies, National Highway Traffic Safety Administration (NHTSA) determines that in their current state, BAIIDS do not fit the likely rule, but with further improvements, they might.¹⁸

b. The Driver Alcohol Detection System for Safety (DADSS)

The Driver Alcohol Detection System for Safety (DADSS) is an Impairment-Detection Technology, specifically an Alcohol Detection System, developed by the Automotive Coalition for Traffic Safety (ACTS), made up of the world's leading light vehicle manufacturers, in conjunction with NHTSA. The DADSS system non-invasively measures and precisely quantifies a driver's alcohol intoxication level through an embedded sensor in the vehicle cabin.¹⁹ The technology requires a small receptor positioned behind the steering wheel or in the driver-side door that takes in the driver's breath passively as the driver breathes normally. It is attached to a sensor that would measure the alcohol content and, if above the limit, would not allow the vehicle to move. While not required for successful operation, the technology could be capable of creating a log of incidents when a sensor is triggered. Information contained in the log would be sensitive data about the drivers' intoxication readings, creating a heightened privacy risk.

2. Touch (Palmprint, Fingerprint, or other body-based touch)

A subset of biometric technologies, touch sensor technologies can be incorporated into existing biometric systems already widely deployed for authenticating driver identity.²⁰ These biometric systems require that a driver register a fingerprint, which can then be used by in-vehicle systems, such as for unlocking doors or starting the vehicle.²¹

Not all touch-based systems rely on the same underlying technology. One touch system is being developed in cooperation with NHTSA and the DADSS Program (discussed above).²² This system would require the driver to interact with the touch technology before operating the vehicle through a

biometric scan, and the derived data from that scan would then be used to measure and precisely quantify the driver's BAC. This is done through a method known as spectroscopy, utilizing detection of light absorption at a particular wavelength from a beam of near-infrared light reflected from within the subject's tissue, similar to shining a light under the driver's fingertip or palmer side of the hand.²³ Other systems, however, use other metrics, such as SOBRsafe, which advertises that it measures the alcohol emitted through the pores in the fingers.²⁴ While the DADSS touch system does not include any technology to identify the driver or subject, the privacy implications of identifying drivers through biometric data that can be linked to a particular individual are numerous, mainly being the direct linkage of data to the individual and the amount of information that can be collected from biometric identifiers.

3. Cameras

Cameras in vehicles can serve a few different purposes.²⁵ Most DMS use cameras to operate and some ADAS may incorporate cameras, for example to operate hands free driving features. Incorporating a camera into the vehicle could aid in assuring that there is a driver, but could also be used to determine attention and awareness or even the identity of the driver. While DADSS technology does not include use of cameras, these are features that could be useful in determining intoxication or impairment.²⁶ Detecting impairment through just a camera, however, may create privacy issues as well as general accuracy issues. While a camera may be successful in inferring that an individual is drowsy, it might not be as good at determining that an individual is drowsy due to intoxication. A camera alone to determine impairment or intoxication would likely be making an inference about the driver and would vary depending on the individual.

II. Privacy and Security Risks

Technology that relies upon the collection, analysis, and application of personal or biometric information creates privacy and security risks for drivers. Those risks may be more severe in certain circumstances, such as for people from certain communities or when the information is particularly sensitive. The prospect of new technologies being developed to detect and measure driver impairment creates a new sensitive data point that likely requires stronger privacy protections than others. As the safety features in vehicles increasingly collect and use sensitive personal data to function, the importance of protecting individual privacy and preventing data misuse is paramount.²⁷ When a driver operates a vehicle, several data points about the speed, breaking habits, or overall functionality are collected. But unlike those data points that may relate to driver behavior and vehicle function, data related to alcohol impairment is a data point specifically about the health of an individual. Health data is often considered sensitive data and legally protected.²⁸ When considered sensitive, the data is likely subject to protection in state or federal privacy laws, meaning it would be a data point covered outside the bounds of the FMVSS.²⁹

Privacy risks of Vehicle Safety Systems to detect and measure impaired drivers are, in large part, related to the types of data directly or indirectly collected. These systems may implicate a wide range of data beyond the specific determination if a driver is or is not intoxicated. For instance, many technologies will tie that data to a specific driver's identity and may include it in a general driver profile.³⁰ Driver profiles can combine multiple features and technologies to create a highly desired customized driver experience in terms of both safety and convenience.³¹ The privacy risks are exacerbated here as disparate pieces of personal information are aggregated together in an identifiable format.

Data handling decisions can impact the risks related to the collection of that data. For instance, risks are often lowest when a system is designed such that personal information is only processed on the vehicle and not in a central database, such that it is never accessed or used by the manufacturer or shared with third parties. Another avenue for mitigating risk is in removing personally identifiable information. Data controllers in many industries take steps to ensure individualized profiles are de-identified. Unfortunately, this can be more difficult with vehicle-specific accounts, since Vehicle Identification

Numbers (VINs) may be used to access full vehicle histories, including details on vehicle owners as well as other pertinent data.³²

Impairment-Detection Technologies may also implicate a wide list of other data types. When cameras are involved, systems may also be designed to make approximate judgements of a driver's race, gender, or other biological characteristics. Some systems could link data to the GPS location of a vehicle, tying it to a specific address, such as a person's residence or a certain place of business. In addition, many of the same technologies that allow for detection of intoxication levels may also implicate other private information about a driver, such as sensitive health information including the potential for certain physical, mental, or emotional health conditions.

In the collection of data in any of these categories, not only do specific privacy risks need to be considered related to the intended purpose of the collection, but also for the potential incidental uses. Privacy risks may increase when data collected for one purpose (for instance, to prevent impaired driving) is used for another (like setting insurance options).³³ Additional uses may be anticipated by the manufacturer itself or by partners and other third parties. Third party relationships are those relationships that a company has with external entities.³⁴ These relationships can be contractual or not with vendors, service providers, data brokers, or supply-side partners. In the vehicle space, these third party relationships exist in the above ways, with an additional relationships created with the insurance industry and other entertainment partners who provide infotainment equipment or technology.³⁵ Vehicle manufacturers have wide-ranging partnerships with companies and organizations with whom they could transfer personal information collected via in-vehicle systems, including outside companies who develop aspects of in-vehicle technology, insurance companies, law enforcement, or marketing and advertising platforms. Recent stories have demonstrated some of the harms that can occur when the risks related to sharing data with third parties manifest, including a lack of access to vehicle insurance.³⁶ This underscores the need for strong privacy protections to be put in place as impairment technologies evolve.³⁷

In regard to some data collection, the underlying technology may be able to be explained, and informed consent may be obtained by the vehicle

manufacturer at the time of purchase. However, this is not always the case. For instance, manufacturers of vehicles sold on the secondary or “used car” market cannot ensure the same guarantees. A recent study found that sales of used vehicles outnumbered new vehicles by more than 250% in 2022, making this a substantial part of the market for passenger vehicles.³⁸ In addition, the owner of a vehicle is often not the sole or primary driver. Particularly in unhealthy or abusive relationships, the collection of information about a driver that is reported back to the vehicle owner may raise significant safety risks.³⁹

Depending on the design of any Impairment-Detection Technology, including its intent and levels of accuracy, other vehicle occupants beyond the driver may have their information implicated. This may be either an intentional part of the system’s design, where the data may be tracked back to a passenger, potentially even an identified or identifiable passenger. Passenger information, however, may also be implicated unintentionally related to issues with the system’s targeting or accuracy.

Risks for people who are not aware of the specific monitoring technology can be heightened since they may not fully understand what information is collected or how it can be used. Moreover, the risks can be particularly significant if people are aware of the technology but have not had its features accurately communicated. The reason for this is that they could create false beliefs or understandings that lead to decisions that are not only not in their best interest but may be specifically harmful to their safety or security.

In addition to privacy risks, the collection of personal information also raises security risks stemming from unauthorized access. Storing this data on the vehicle in perpetuity or sending the data off the vehicle to a cloud-based server or remote server could allow this data to be transmitted to third parties. Third parties can act to undermine the confidentiality of the information, by making it available to either the general public or specific individuals or groups; the integrity of the information, by adding or changing data related to specific vehicles or drivers such that it reflects inaccurate reports; or the availability of the data or the systems, such that the systems may not work properly in vehicles or do not communicate properly back to the systems’ operator.

III. Background on the Congressional Mandate to Prevent Impaired Driving

In the Infrastructure Act, Congress mandated that the United States Department of Transportation (USDOT) establish a Federal Motor Vehicle Safety Standard (FMVSS) to “passively monitor a motor vehicle driver’s performance to accurately detect if the driver may be impaired.”⁴⁰ The stated purpose of this impaired driving provision is “to ensure the prevention of alcohol-impaired driving fatalities.” The provision requires that passenger motor vehicles manufactured after the established standard’s effective date be equipped with advanced drunk and impaired driving prevention technology.

A. Purpose of the Mandate and Political Process

The mandate in the Infrastructure Act was adapted from the HALT Act, first introduced in 2019 by Congresswoman Debbie Dingell (D-MI).⁴¹ It was reintroduced in 2021 alongside a Senate companion bill sponsored by Senators Ben Ray Lujan (D-NM) and Rick Scott (R-FL).⁴² Mothers Against Drunk Driving (MADD) was a champion of each version of the bill and called the provision in the Infrastructure Act both “monumental” and “historic.”⁴³ Other anti-drunk driving and driver safety organizations also supported the law. However, some lawmakers opposed the legislation, citing privacy concerns of unregulated tech in consumer vehicles.⁴⁴

In creating the advanced drunk and impaired driving prevention technology mandate, Congress specifically cited data that showed “in 2019, there were 10,142 alcohol-impaired driving fatalities in the United States involving drivers with a blood alcohol concentration level of .08 or higher.”⁴⁵ This number has since increased: NHTSA found that 13,384 people died in alcohol-impaired driving crashes in 2021 alone.⁴⁶

The stated purpose of the mandate is to prevent and decrease the number of serious accidents and injuries that are caused by intoxicated, distracted, or drowsy drivers.⁴⁷ Congress found that “advanced drunk and impaired driving prevention technology can prevent more than 9,400 alcohol-impaired driving fatalities annually.”⁴⁸ An economic rationale was also given for the mandate. Congress pointed to data from 2010 that the estimated annual economic cost of alcohol-impaired driving crashes was \$44 billion.⁴⁹ However, this number is also on the rise, with 2019 data estimating tangible costs to add up to \$58 billion.⁵⁰

B. Scope and Timeline of the Mandate

President Biden signed the Infrastructure Act on November 15, 2021.⁵¹ NHTSA, a part of USDOT, announced an Advance Notice of Proposed Rulemaking (ANPRM) in December 2023 as the first step in establishing the FMVSS.⁵² The ANPRM was published in the U.S. Federal Register on January 5, 2024.⁵³

The Infrastructure Act requires the implementation of technology with the ability to either passively monitor the driver to detect impaired driving or passively and accurately detect if the driver's blood alcohol level is beyond the legal limit, and in either case, to prevent or limit the operation of the vehicle.⁵⁴ Beyond these central requirements,⁵⁵ Congress has delegated most of the technical details and deliberations to NHTSA within the scope of its work to establish the FMVSS. For instance, NHTSA has already proposed a definition for the term "passive" within the ANPRM, namely to mean that "the system functions without direct action from vehicle occupants."⁵⁶

The Infrastructure Act grants three years for NHTSA to release the final FMVSS, though it also allows for NHTSA to extend this deadline by another three years, putting the final date for the Agency to act at November 15, 2027. However, it remains to be seen if NHTSA will take advantage of this extension. Once implemented, the compliance date of the new rule will be set at least two years after the FMVSS is issued, though not more than three years.⁵⁷

C. NHTSA Authority and Responsibility

NHTSA is responsible for enforcing vehicle performance standards and partnerships with state and local governments.⁵⁸ NHTSA's goal is to reduce deaths, injuries, and economic losses from motor vehicle crashes.⁵⁹ In the past 5 years, NHTSA has deeply engaged on issues of privacy and has issued guidance and voluntary best practices, as well as regulations and standards, to highlight the importance of strong privacy and cybersecurity protections.⁶⁰ A 2017 study from the Government Accountability Office (GAO) found that while NHTSA "does not have the authority to regulate consumer privacy as it relates to motor vehicles or motor vehicle data," the agency does "consider the privacy impacts of its regulatory activities" by conducting privacy impact assessments and informing the public about how NHTSA regulations will impact consumer privacy.⁶¹ NHTSA has also taken steps to offer guidance on cybersecurity, bolster its own

privacy page, provide guidance on automated vehicles, and consider privacy implications in the context of safety regulations.⁶²

IV. Public Awareness and Attitudes Toward Vehicle Safety Systems

With more attention being drawn to the data collected within vehicles, vehicle owners have expressed a heightened desire to understand what data is collected and used by manufacturers.⁶³ In 2023, FPF and ACTS conducted a comprehensive survey of individuals over the age of 21 to holistically understand their views regarding new vehicle technology, including Vehicle Safety Systems generally and, in particular, Impairment-Detection Technologies.⁶⁴ Below, we include more detailed information and analysis on attitudes toward various types of technologies in vehicles.⁶⁵ Our key findings include:

- > Many drivers value Vehicle Safety Systems, while worrying about the privacy risks;
- > Individuals generally trust carmakers' data practices more than online companies and the government, but worry about vehicle systems that collect information about occupant behaviors;
- > Most drivers support the use of Impairment-Detection Technologies, but have concerns about accuracy, cost, and data disclosures to third parties; and
- > Individuals say that privacy and data protection practices like disclosure limits, encryption, on-car storage, and de-identification are "must haves" for vehicle data.

A. Many Individuals Value Vehicle Safety Technologies, While Worrying About the Privacy Risks

Most drivers are aware of in-vehicle safety technologies.⁶⁶ 86% of respondents indicated that they know that self-driving vehicles are on the roads, and 68% indicated familiarity with automated lane-keeping and adaptive cruise control.⁶⁷ However, respondents are less familiar with other emerging car safety technologies.

55% of drivers think that technology is helpful, and 32% say that it is exciting.⁶⁸ These positive sentiments outpace drivers' negative views of technology, though a substantial minority of drivers characterize

some in-vehicle technologies as “invasive” (25%) and “creepy” (20%).⁶⁹

When respondents express concerns about in-vehicle tech, inaccuracy and privacy risks top the list. Respondents’ top concern regarding Vehicle Safety Systems is the risk of inaccuracy, with about 60% of drivers expressing trepidation about the technologies’ accuracy.⁷⁰ Privacy came in second, with just under half of drivers expressing concerns about how personal data might be collected, used, or disclosed.⁷¹

Respondents’ top privacy concerns involve data potentially being transmitted off their vehicles.⁷²

B. Individuals Generally Trust Carmakers’ Data Practices More Than Online Companies and the Government, but Worry About Vehicle Safety Systems that Collect Information About Occupant Behaviors

Each Vehicle Safety System has implications for privacy depending on functionality, as discussed above. They all collect or rely on different data types to operate. When data is collected, it can be used to inform insurance rates, how vehicle manufacturers can improve vehicle functions, or how to ensure the safety features are operating as they should. When asked about the privacy of personal data when interacting with different types of companies and organizations, respondents were least concerned when interacting with automotive manufacturers (38%), and more concerned when interacting with social media companies (69%), websites (63%), mobile phone and app makers (58%), government and law enforcement (56%), and online and in-person retail stores (53%).⁷³ Categories of data that most respondents think is collected and shared with third parties include that related to navigation (46%), crash notifications (38%), and roadside assistance (45%).⁷⁴

The overall trust, adoption, and effectiveness of vehicle safety technology will suffer if data is over-collected, subject to data breaches, results in bias or discrimination, or is misused by unexpected third parties (such as insurers or data brokers). Currently, a narrow majority of drivers indicated that they trust data collected by cars will be kept safe (51%) and that the data will only be used for the intended purpose (53%).⁷⁵ Collecting specific, sensitive data from Vehicle Safety Systems like alcohol intoxication level or video—which is data specifically about the driver and not about the vehicle itself—would require further protection as it

has broader implications should this information be used for insurance or law enforcement, which both raised strong concerns for drivers.⁷⁶

C. Most Drivers Support the Use of Impairment-Detection Technologies, but have Concerns about Accuracy, Cost, and Data Disclosures to Third Parties

When ranking concerns about technology to automatically detect a driver’s alcohol levels, respondents pointed to reservations about accuracy (60%) and privacy (48%).⁷⁷ When ranking those same concerns about technology to monitor driver behavior to detect impaired driving, the results were essentially identical (accuracy at 59% and privacy at 46%).⁷⁸ Accuracy is the top priority for drivers when it comes to vehicle technology. At the same time, a close follow-up was the technology’s added expense (36%).⁷⁹

Drivers have strong concerns about data being shared with third parties, such as law enforcement and social media companies.⁸⁰ As privacy and data are often at the forefront of public policy conversations surrounding developing and implementing new technologies, drivers also think critically about what data collection means in the vehicle space.

D. Individuals Say that Privacy and Data Protection Practices Like Disclosure Limits, Encryption, On-Car Storage, and De-Identification are “Must Haves” for Vehicle Data

For Vehicle Safety Systems generally, respondents indicated that the number one essential or “must have” feature would be for data not to be shared with third parties (39%).⁸¹ Other privacy practices also ranked highly, such as data encryption (38%), anonymized data for drivers (37%), anonymized data for vehicles (36%), data storage localized (34%), data deletion after a fixed period of time (34%), and instant data deletion (33%).⁸² When the same question was asked in relation to technology that passively detects alcohol levels, the number one essential or “must have” feature was tied between anonymized data not linked to individual drivers (39%) and data not shared with third parties.⁸³ Respondents overall evinced a want for more assurances of privacy and safety, transparency in the data usage, and deletion of user data when asked in an open-ended format, about what they need to trust a vehicle safety system.⁸⁴ Drivers want the technology in their vehicles to be safe and trustworthy; a majority of respondents expressed concerns that insufficiently protective data practices create concerns for them. These concerns are likely to erode trust and limit adoption.⁸⁵

V. Recommendations for Impairment-Detection Technologies in Vehicles

For one and a half centuries, vehicles have been made of metal and four wheels, intended to get people from point A to point B. Continuous vehicle improvements and government standards, such as those issued by NHTSA, have ensured that these vehicles get us where we need to go more safely year after year. Yet, while life-saving guidance and rules have been issued to protect vehicle occupants physically, there is a gap in the guidance offered to protect those same occupants digitally. As vehicles continue to become more advanced in the technology offerings for safety and convenience, the amount of data collected increases, too. FPF offers the following recommendations for how NHTSA can ensure Impairment-Detection Technologies such as those intended to detect driver impairment can best protect the privacy and data of vehicle occupants.

Recommendation 1

Regulators, technology developers, and technology deployers should ensure that privacy is a foundational principle for Impairment-Detection Technologies and should implement appropriate legal, policy, and technical safeguards when personal information is implicated, including safeguards to:

-) **Minimize the collection and retention of personal data;**
-) **Process and store personal data on vehicles when possible, with strict limits on off-device data use by Impairment-Detection Technologies;**
-) **Set reasonable retention limits of data from Impairment-Detection Technologies;**
-) **Provide robust access and deletion options;**
-) **Secure personal data at rest and in transit; and**
-) **Set reasonable limits of data use and third party sharing, including bars on sharing personal impairment-detection data or using that information for other purposes.**

The Fair Information Practice Principles established by the Federal Privacy Council serve as baseline principles that agencies can apply to their privacy programs.⁸⁶ “The FIPPs are a collection of widely accepted principles that companies, organizations, and government agencies use when evaluating information systems, processes, programs, and activities that affect individual privacy.”⁸⁷ The principles can be used by NHTSA to align proposed FMVSS with privacy best practices.

The principle of data minimization requires “that one should only collect and retain that personal data which is necessary.”⁸⁸ Developers and deployers of Impairment-Detection Systems that implicate personal data should ensure privacy and security protections for that data, including, for instance, through on-vehicle data processing and limited retention. Data and information from Impairment-Detection Technologies should be stored and secured separately from the data related to vehicle diagnostics, which could additionally benefit anyone looking to assess vehicle diagnostics, allowing them to more easily access relevant data to address a physical or mechanical problem, such as a faulty tire pressure sensor.

When a data point related to impairment is collected, vehicles should only retain the data as long as necessary to deter impaired driving or limit the ability of the impaired driver to operate the vehicle. This should be established through a retention schedule, and could be measured by a number of key starts, for instance. Should data be processed, stored, or retained off the vehicle, it should be for the limited purpose of diagnosing, servicing, or repairing the technology.

Drivers should have clear and easily accessible means of accessing and deleting personal information.⁸⁹ Allowing a person to whom data relates to request the deletion of personal information is an important right for individuals and a central feature of multiple data protection regimes.⁹⁰ Whether drivers have access to delete either specific data points or broad categories, every vehicle should provide sufficient clarity and capabilities to delete personal information directly from the infotainment interface or vehicle-connected mobile app.

Ensuring that data is properly secured will require the use of the most robust security practices available, which continues to change due to frequent advancements in related sciences. Today, this includes advancing encryption mechanisms for data stored either locally (i.e., on the vehicle) or centrally (i.e., cloud storage). Current cybersecurity practices for the automotive industry are outlined in NHTSA's 2016 "Cybersecurity Best Practices," updated most recently in 2022.⁹¹ A majority of respondents to the survey conducted in advance of this report indicated that they would feel more comfortable if vehicle data related to impaired driving was, among other things, encrypted, deleted, and anonymized.⁹²

Finally, there should be limitations on the purposes for which data collected by Impairment-Detection Technologies may be used, including for both the data collected by manufacturers and any third parties that may receive it. Entities should be clear about the purpose for which data is collected and how it will be used, and provide documentation of those purposes. Additionally, if the data is to be used for something other than initially collected, it should still comport with the initial purpose of the collection.

Recommendation 2

Technology developers and technology deployers should de-identify data collected by Impairment-Detection Technologies as appropriate.

Much of the data generated from Impairment-Detection Technologies, especially those that collect data points about the driver, are inherently sensitive. Limiting the ability for data to be linked directly to any particular driver is essential to protecting driver privacy. As a plurality of respondents to the survey indicated, deidentification of driver and vehicle data are central to driver trust.⁹³ While automakers are likely already practicing deidentification, increasing the visibility of deidentification methods and ways to anonymize data, especially when taken from the vehicle, and aligning regulatory requirements with agency practices should be considered.

Recommendation 3

Impairment-Detection Technologies should be accurate, should be tested for potential bias, and should not produce false-positive results more often for people from underrepresented, marginalized, and multimarginalized communities. Well-defined standards for consistent deployment and alignment across the industry may be beneficial.

Developers and deployers of Impairment-Detection Technologies require clearly defined metrics and standards to establish how to determine that their systems are working accurately. If accuracy is not able to be assured drivers are less likely to trust its use.⁹⁴ Ensuring that the technology can detect and distinguish between impairment and any number of alternative instances will be essential for customer adoption and trust. This may require consistent testing and auditing of systems to ensure quality control and integrity of the system, similar to AI auditing practices.⁹⁵ "Systems that annoy drivers or mistakenly prevent sober drivers from traveling will not succeed. Although avoiding false alarms is necessary to retain public support, it is also imperative to minimize the incidence of false negative readings."⁹⁶

Developers and deployers must establish processes in support of privacy and data protection. The Automotive Alliance for Innovation has established

Privacy Principles that OEMs can employ and that NHTSA can reference in establishing regulatory obligations.⁹⁷ The voluntary principles created in 2014 and recently updated in 2022 serve as a guidepost for those companies that agree to take the pledge.⁹⁸ Many OEMs are already in alignment with the Automotive Alliance for Innovation Privacy Principles and other laws with similar requirements, such as the California Privacy Protection Act. Providing explicit guidance on continuing transparency and expanding that to cover safety systems, especially those collecting sensitive information such as intoxication levels, will need to be included.

Recommendation 4

Driver acceptance should be promoted through transparency about the systems' functions and operations, as well as the handling of personal data.

Driver acceptance and consent to the adoption of Impairment-Detection Technologies requires transparency in understanding how these systems operate and how any personal information is used. A clear explanation of the technology should provide for its function and operation to allow drivers to understand the technologies in their vehicle at the point of sale, be it the first sale of a vehicle or the sale of a used vehicle. Drivers should also understand how the technologies collect data, use data, and store or retain that data.

Recommendation 5

Regulators, technology developers, and technology deployers should identify and mitigate, to the extent possible, potential future harms to drivers, especially to people from underrepresented, marginalized, and multimarginalized communities.

No matter what the technology is contemplated, limiting harm to marginalized communities should be a top priority. There is no way to predict with certainty that specific harm could result from the use of any specific technology. However, broad technology mandates without testing and evaluation to understand how they could impact specific communities, including individuals in specific geographic regions, can raise the specter of great harms.⁹⁹ Ensuring that impairment detection systems

protect, and do not harm, historically marginalized communities and individuals is essential when new technologies are adopted.¹⁰⁰ For instance, requiring technology in vehicles to monitor and detect impairment could have disproportionate impacts on black and brown communities, immigrants, or others who face greater threats from law enforcement and others behind the wheel.¹⁰¹ This technology should not be considered an on-vehicle police officer, nor should the automatic response of this technology be to involve police.

VI. Conclusion

Safety and privacy go hand-in-hand, and as the auto industry progresses with technology, NHTSA will continue to play an important role in overall guidance on privacy and data protection in the vehicle space as they set safety standards. Establishing a FMVSS as required by the Infrastructure Act would be the first and best opportunity to address privacy and data protection, in the use of safety technology. Through this rule, NHTSA has the opportunity to specifically define the parameters of technology that fits within the rule, acknowledge and recommend limitations on the collection, use, and data retention, and provide a standard for vehicle manufacturers and those subjected to NHTSA rules on how to handle data collected from vehicles.

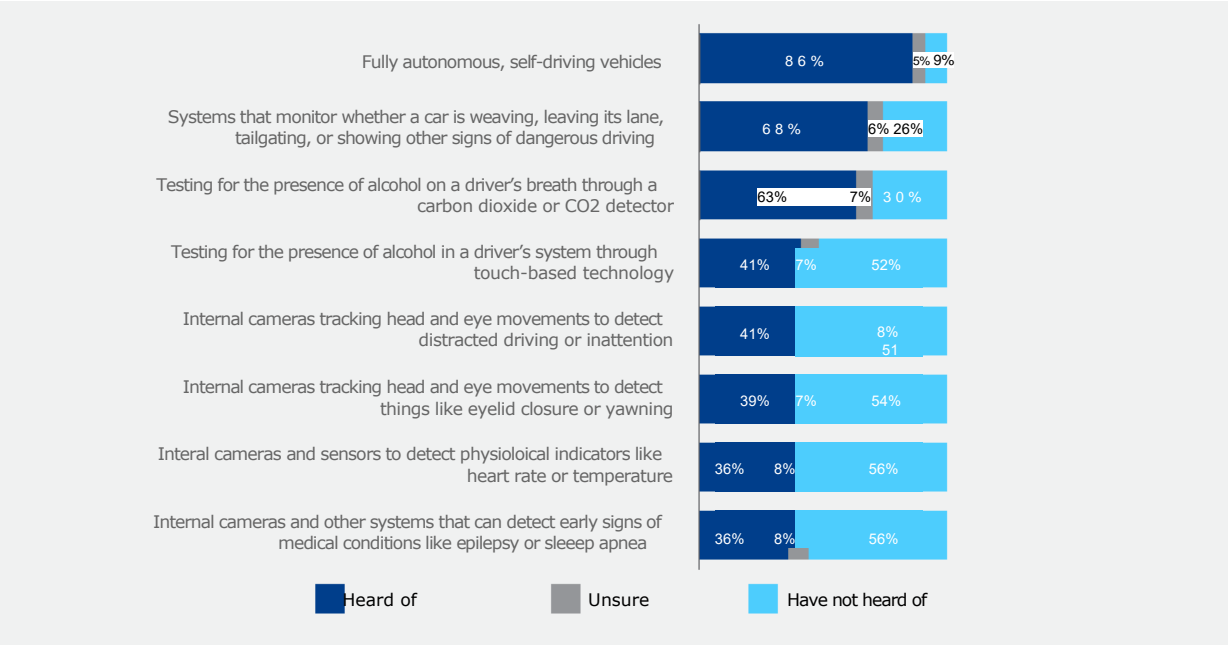
Understanding the privacy implications of Impairment-Detection Technologies can inform policymakers, vehicle manufacturers, and anyone in the vehicle lifecycle how to handle data. NHTSA should consider and address privacy and data especially when requiring a new technology that collects sensitive data. Regardless of the outcome of the rule, any organization developing or implementing technologies, including vehicle manufacturers, should ensure that privacy is a foundational principle for any Vehicle Safety System and should implement appropriate legal, policy, and technical safeguards when personal information is implicated. With drivers focused on their vehicles and what data they collect, it has never been more important to protect driver privacy.

APPENDIX

In 2023, the Future of Privacy Forum (FPF) and the Automotive Coalition for Traffic Safety (ACTS) surveyed drivers’ attitudes regarding technology and privacy. To conduct this survey, FPF and ACTS, along with our research partners, developed a set of questions to holistically understand how drivers feel when incorporating new technology into their vehicles. The methodology: N=2063 adults aged 21+ who either currently own a driver’s license or have owned a driver’s license in the past five years, including an oversample of n=723 respondents who do not currently own or lease a car but plan to in the next five years, were surveyed from July 7–12, 2023. The sample was drawn from online panels. The following encompasses a portion of the total survey questions that were used within the report.

Fig 1: Which of the following types of driver safety technology have you heard of?

Fig 2: Which words do you think best describe these kinds of driver safety technologies,



assuming that these technologies would not impact the price of a vehicle?

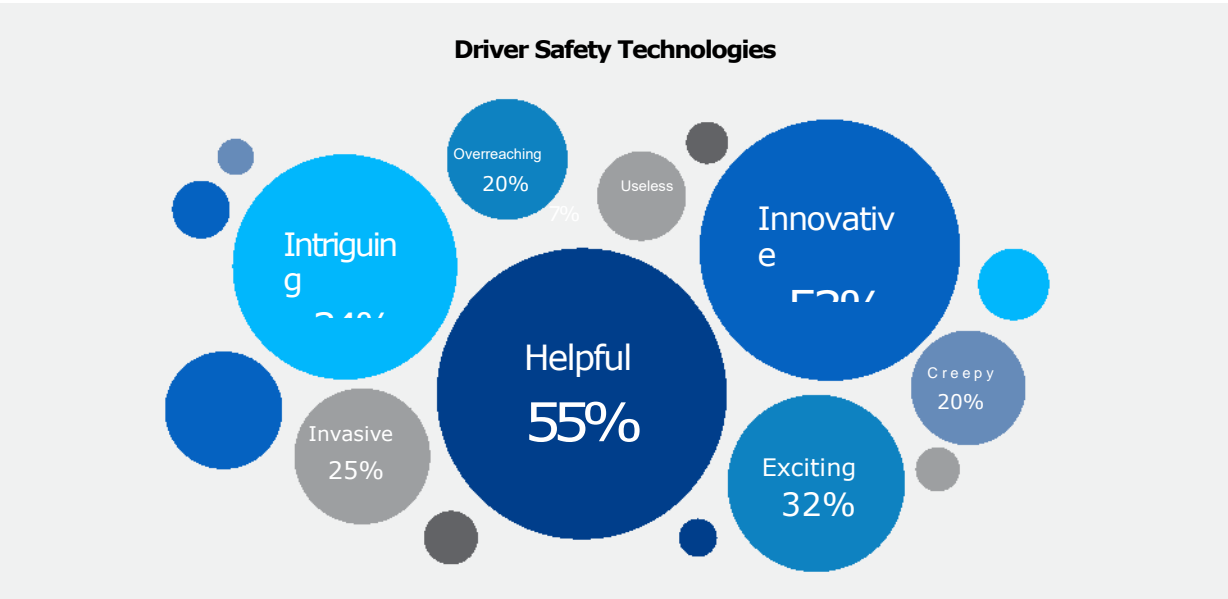


Fig 3: To what extent, if at all, are you concerned about the privacy of your personal data when interacting with the following types of companies and organizations?

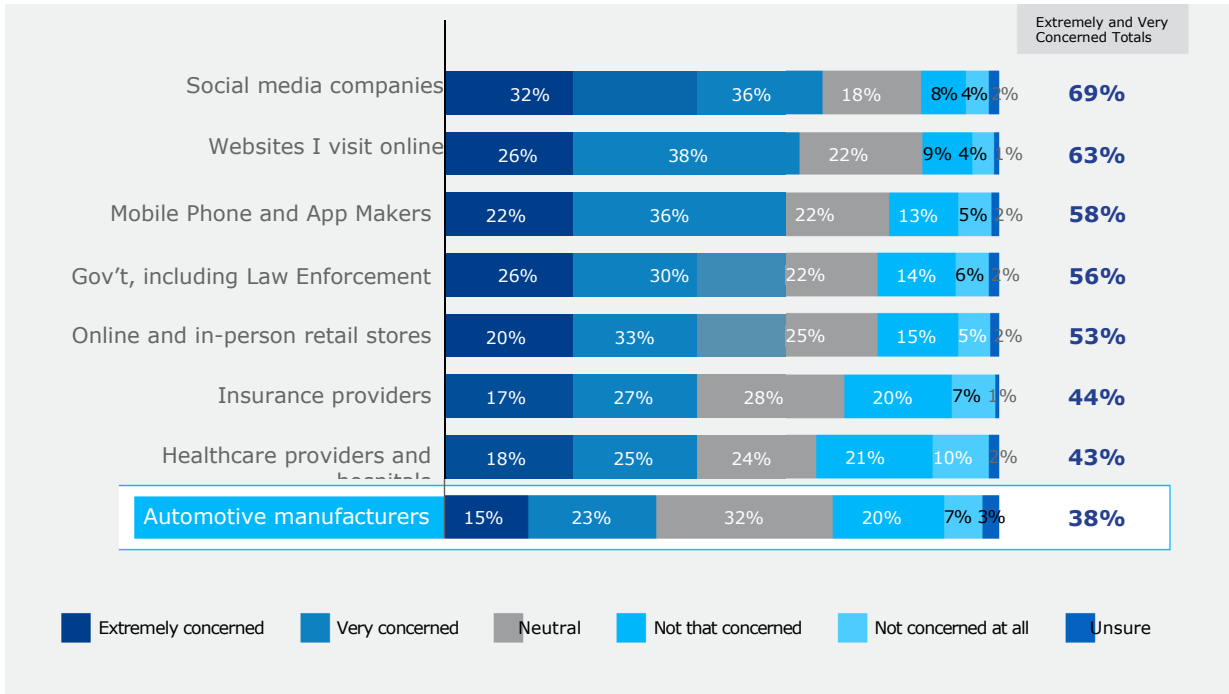


Fig 4: When it comes to data collection in passenger cars, just based on what you know, which of the following activities do you think collects user data that can be accessed by automotive manufacturers or third parties like insurance companies, advertisers or government agencies (including law enforcement)? Choose all that apply.

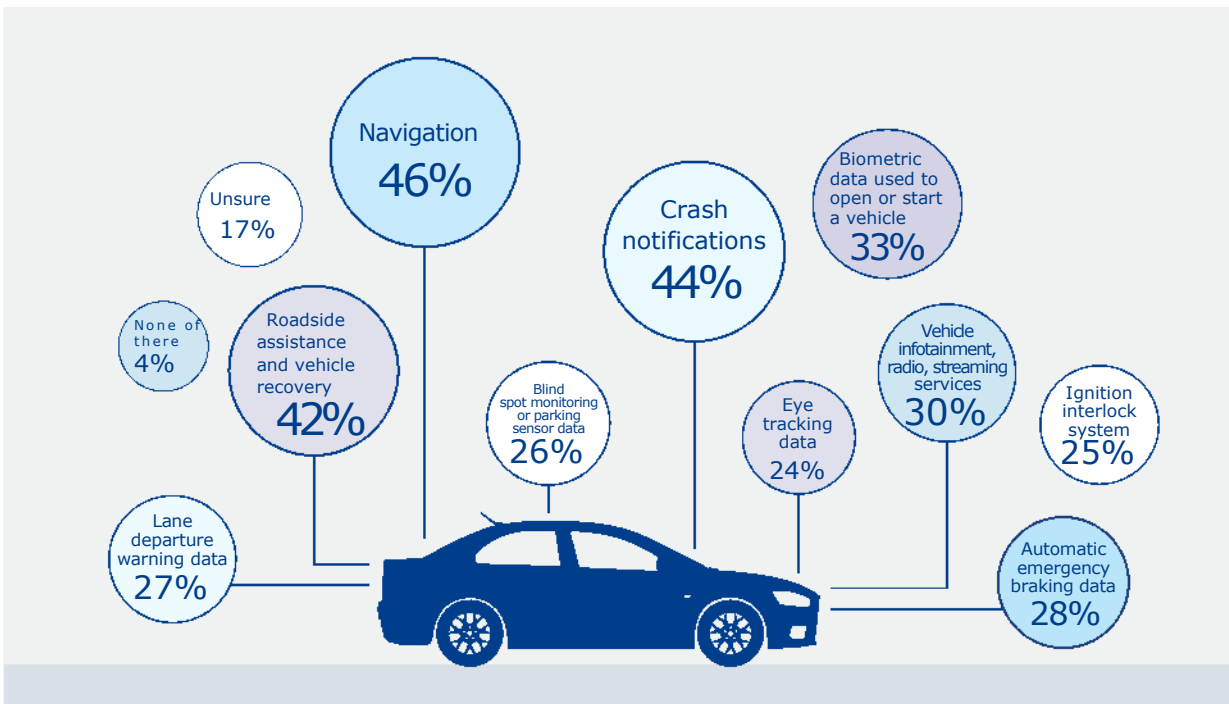


Fig 5: If you have concerns about technology to automatically detect a driver’s alcohol levels, what best characterizes those concerns?

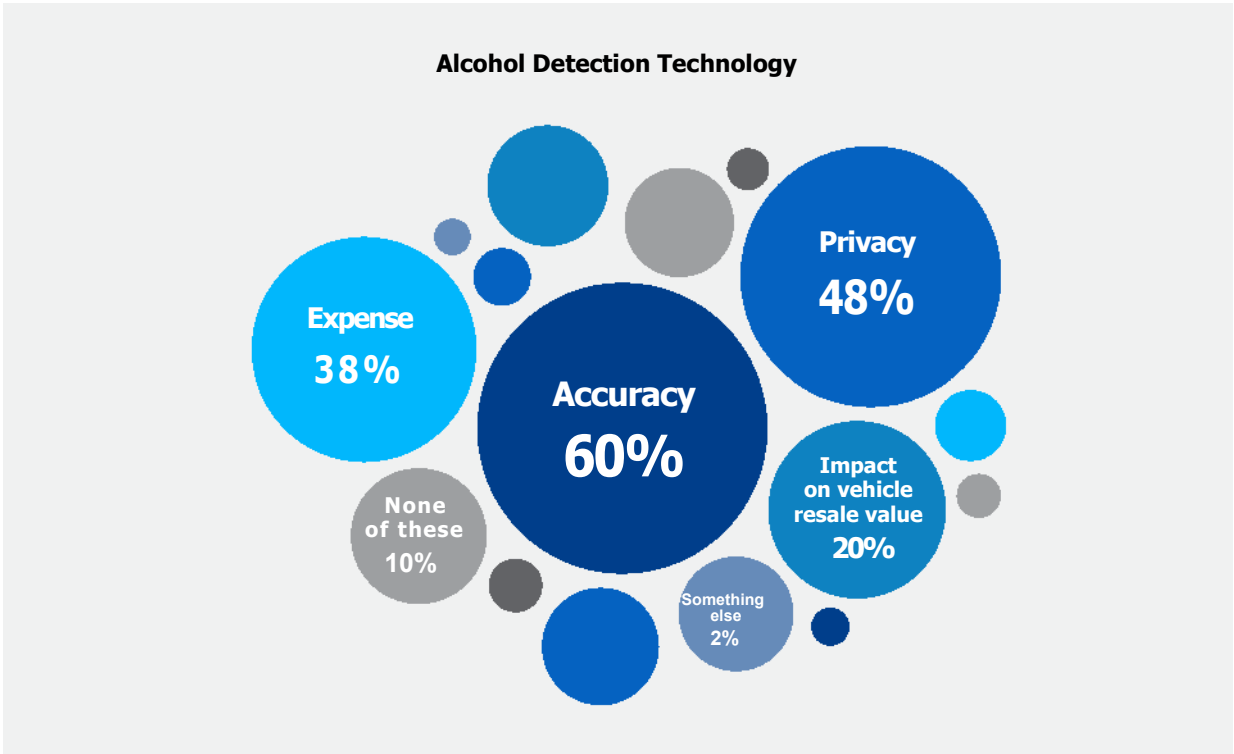


Fig 6: If you have concerns about technology to automatically detect impaired driving by monitoring driving behavior, what best characterizes those concerns?

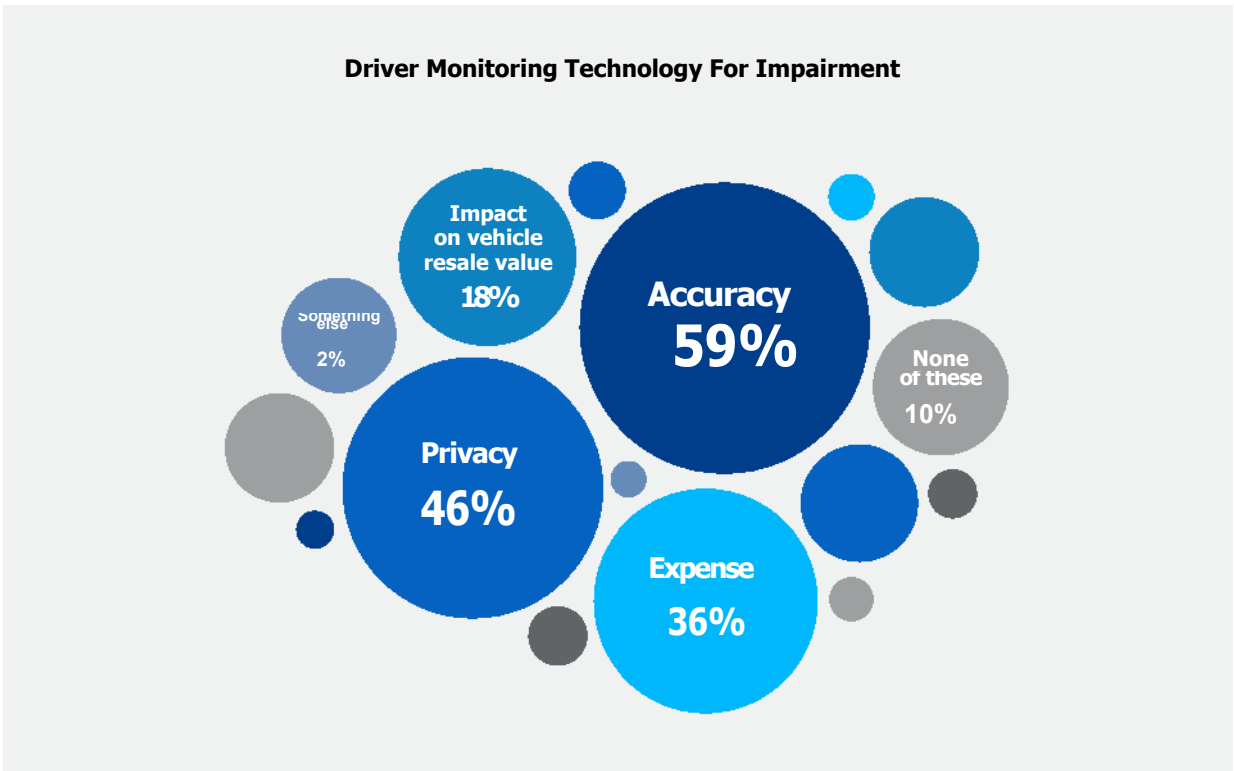


Fig 7: In general, how much would you say you trust that data collected about passenger cars is kept safe?

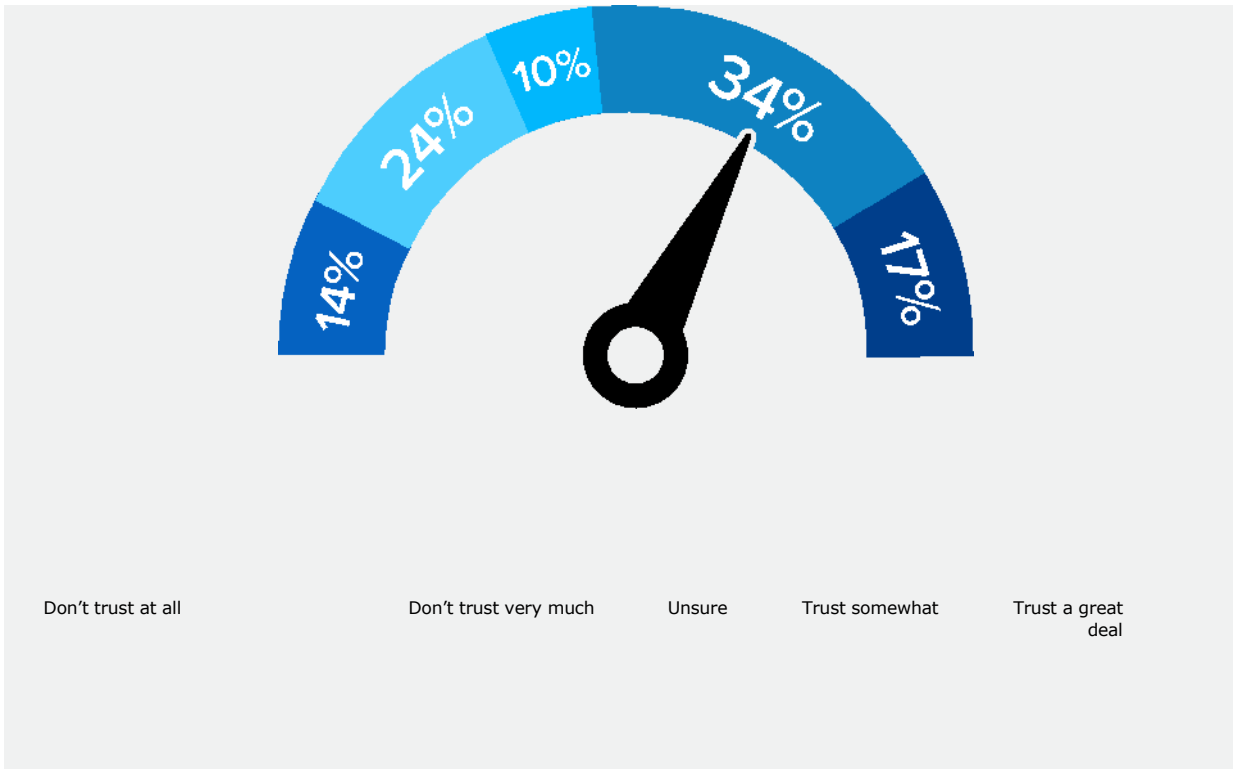


Fig 8: In general, how much would you say you trust data collected about you in automotive vehicles to be only used for the intended purpose?

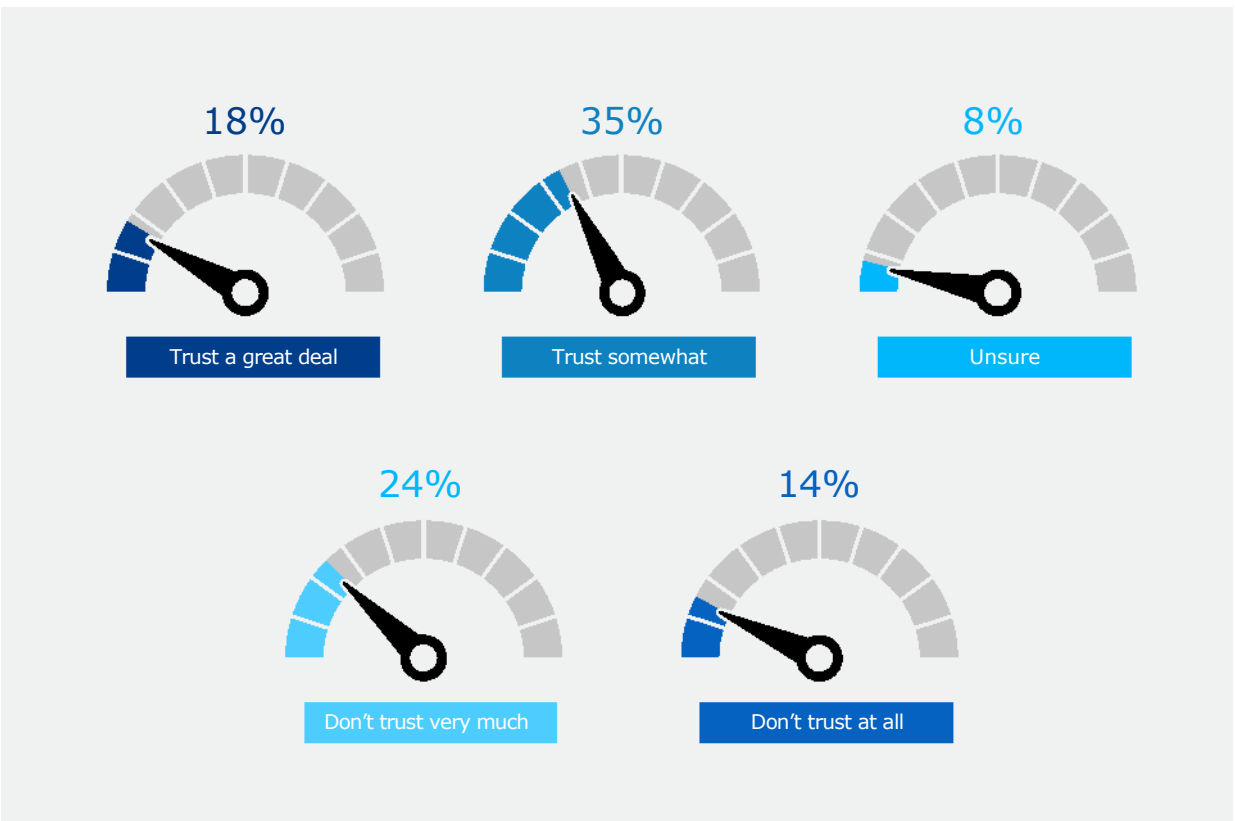


Fig 9: How much trust do you have in each of the following types of technology to report accurate data?

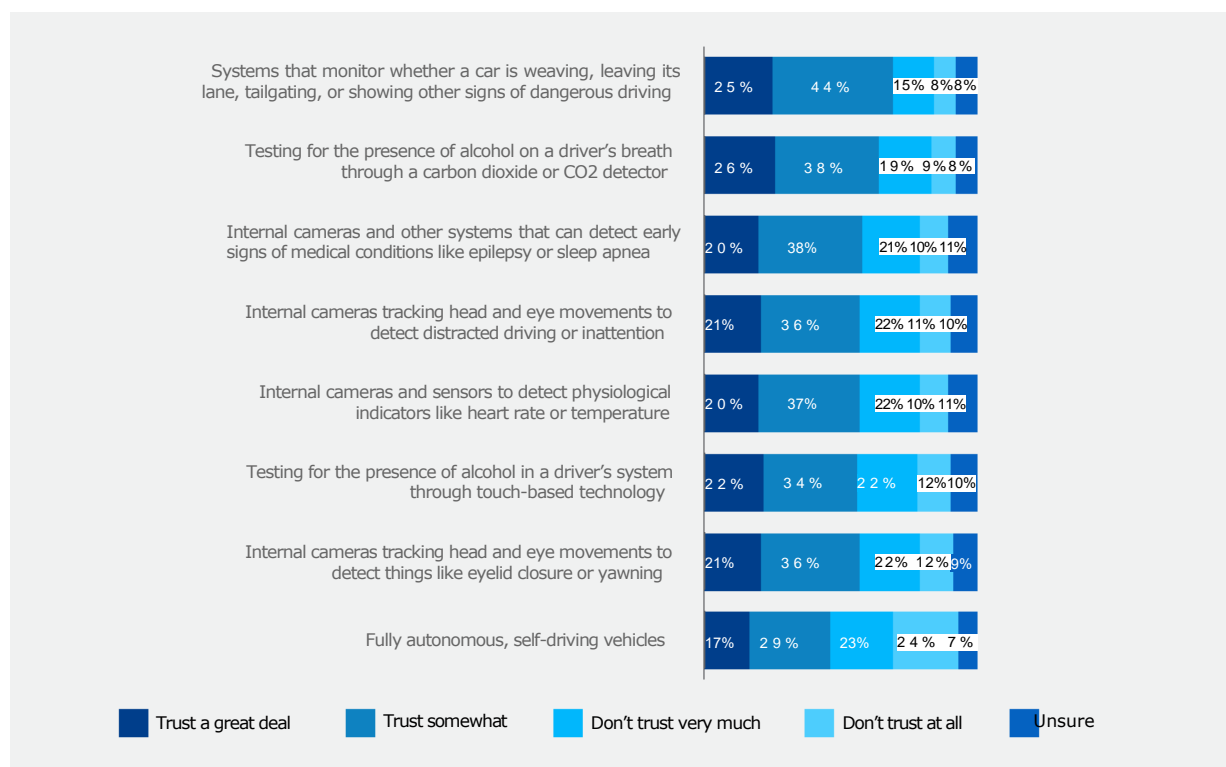


Fig 10: How concerned are you about driver safety technologies sharing your data in the following ways?

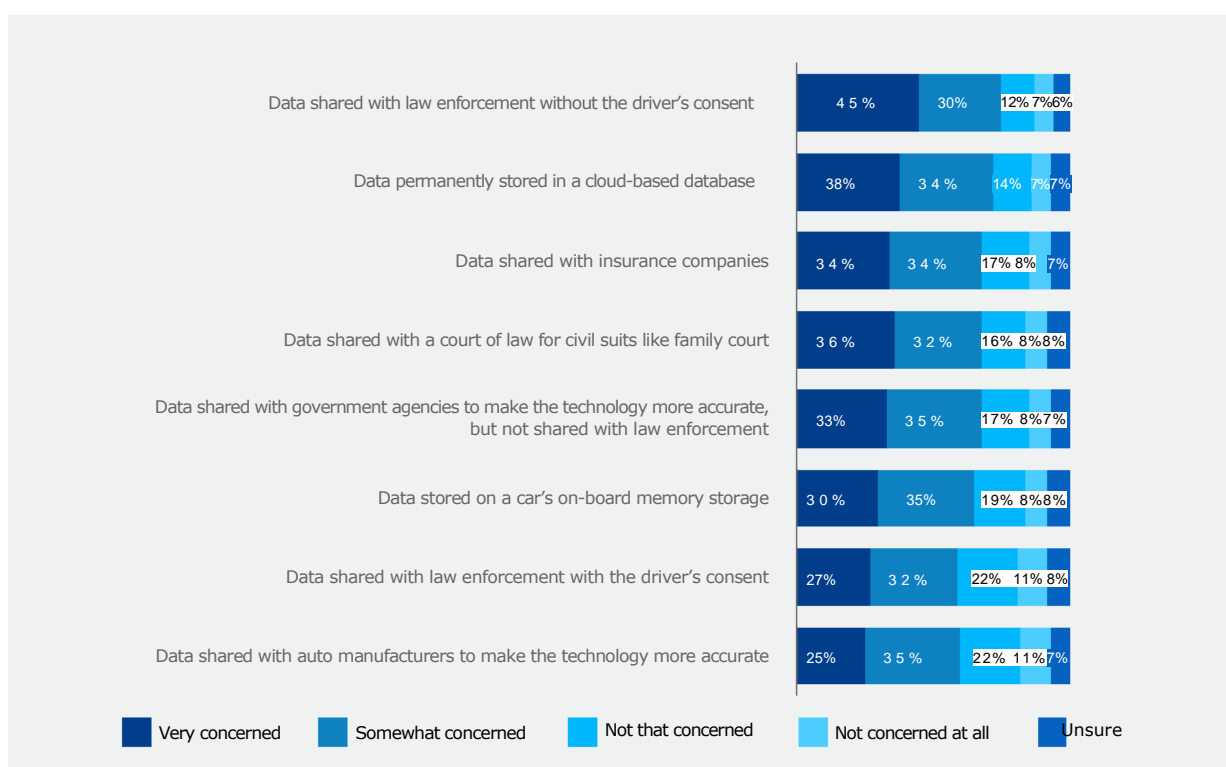


Fig 11: How comfortable would you be with technology that passively detects alcohol levels to identify whether a driver may be impaired and prevents them from starting their car, if...

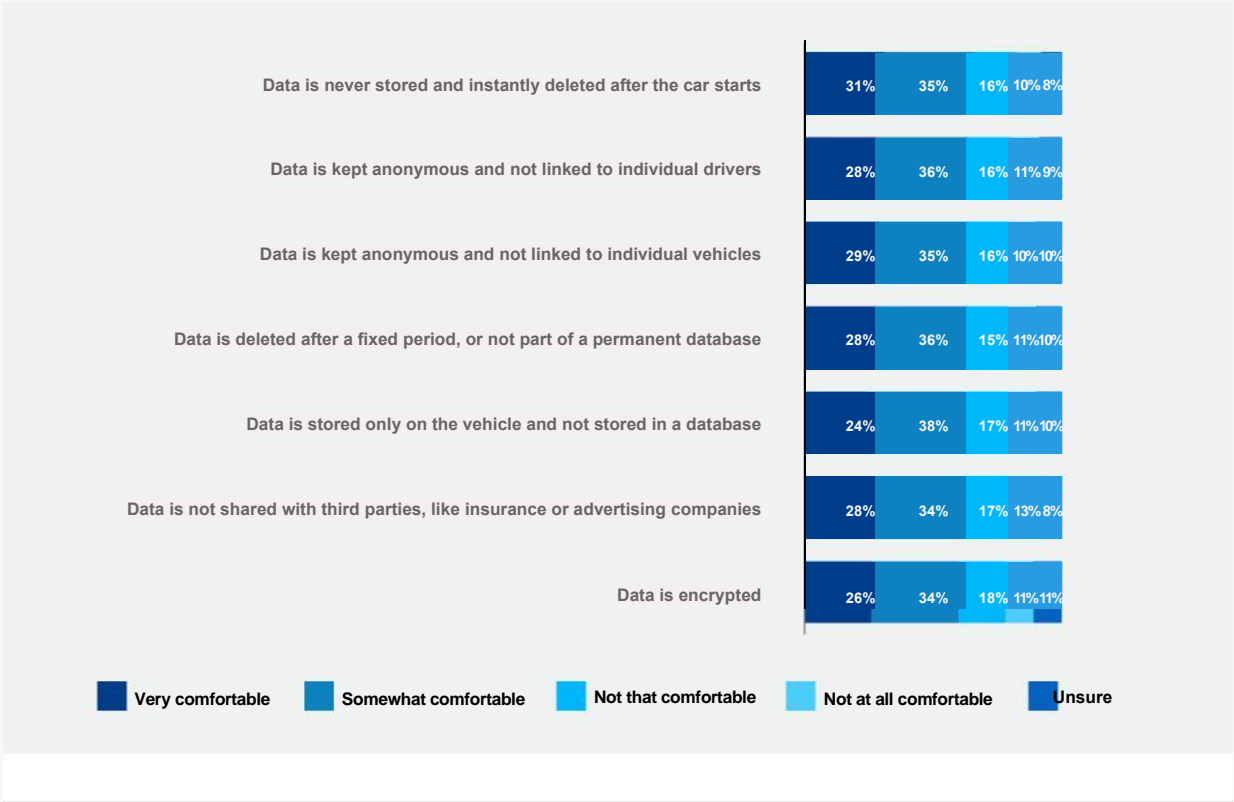


Fig 12: Which of these would you consider essential, or “must have,” as part of any technology that passively detects alcohol levels to identify whether a driver may be impaired and prevents them from starting their car? Choose all that apply.

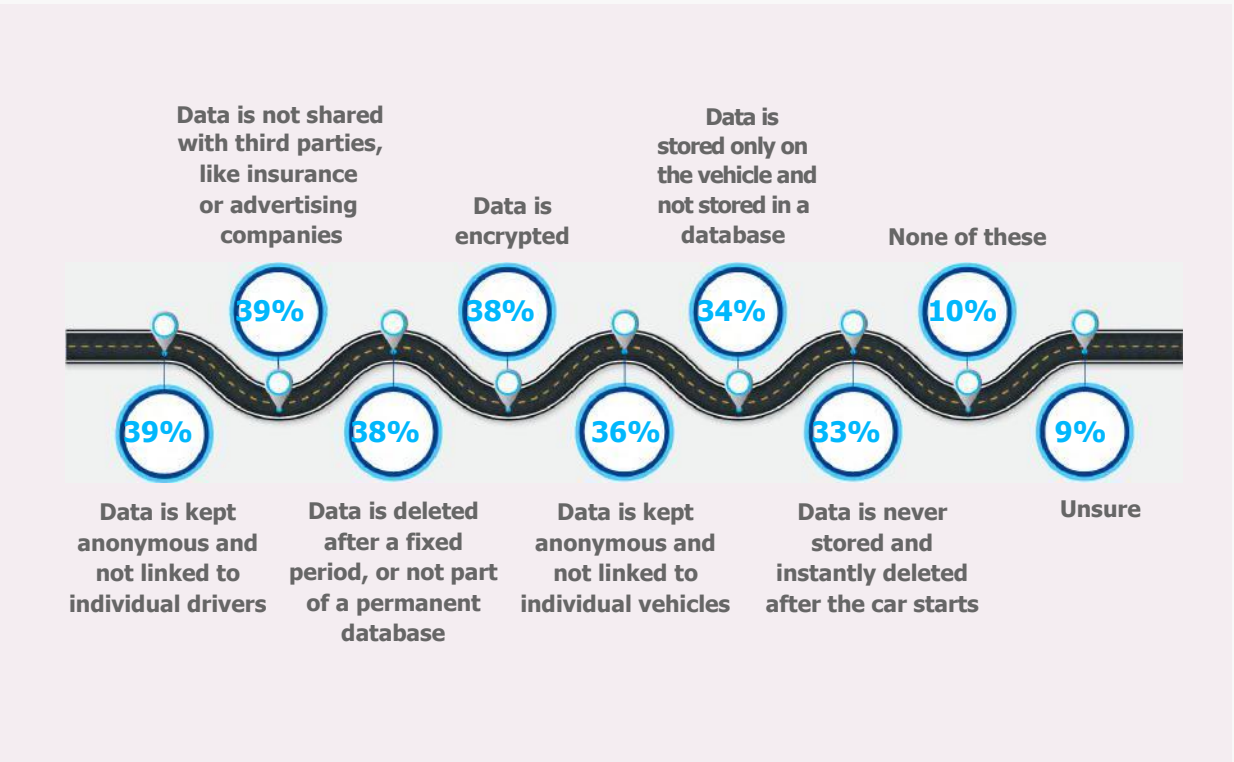


Fig 13: Which of these would you consider essential or “must-have” as part of any technology that monitors whether a driver is weaving, leaving their lane, tailgating, or showing other signs of impaired driving by constantly monitoring driving behavior? Choose all that apply.

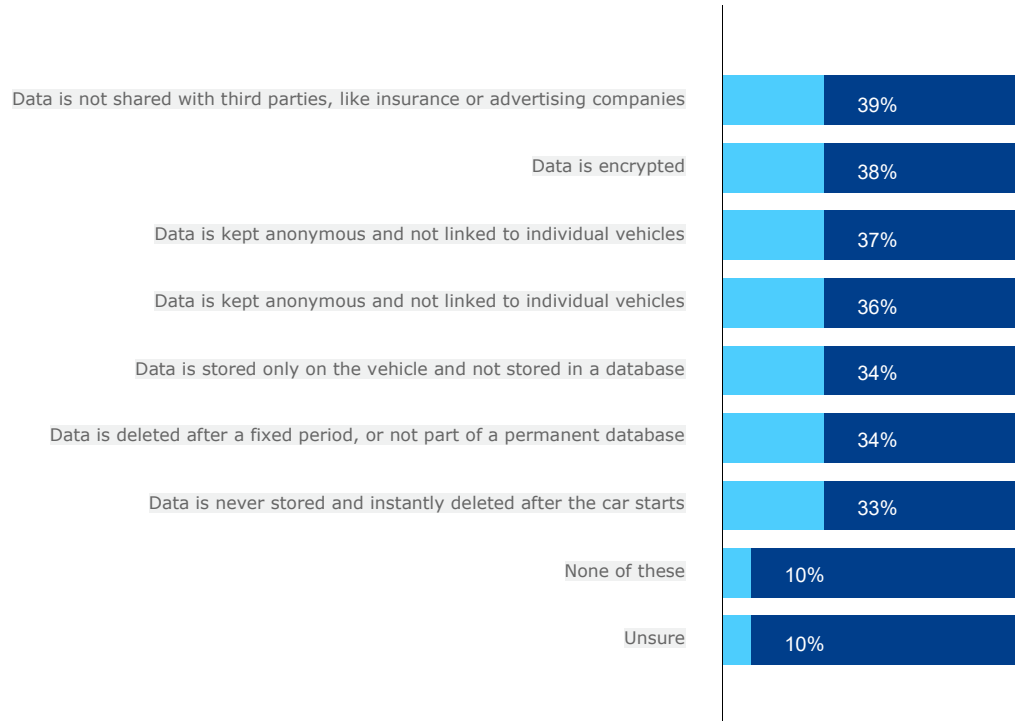
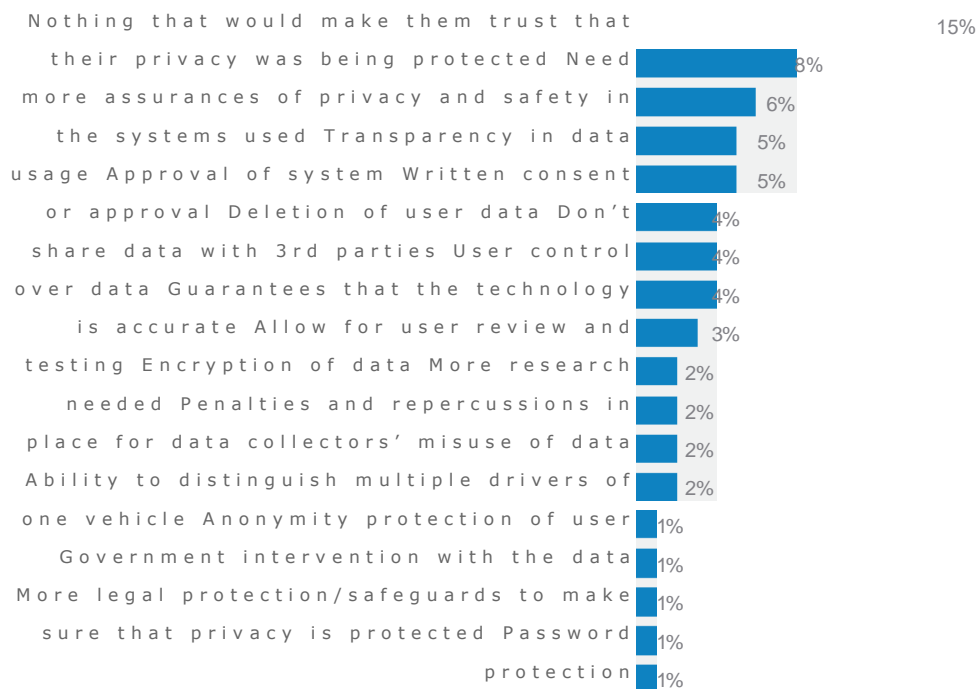


Fig 14: In general, what do you think you would need in order to trust that these driver safety systems were protecting your privacy?



ENDNOTES

- 1 Press Release, Otonomo, Majority of New Connected Car Buyers Are Willing to Trade Personal Data for Improved Safety and Driver Services, According to New Otonomo Study (June 6, 2018), <https://otonomo.io/press-releases/majority-of-new-connected-car-buyers-are-willing-to-trade-personal-data-for-improved-safety-and-drive>
- 2 Driver Assistance Technologies, Nat'l Highway Traffic Safety Admin., <https://www.nhtsa.gov/vehicle-safety/driver-assistance-technologies> (last visited Jan. 23, 2024).
- 3 For a complete list of all ADAS and DMS features, see American Automobile Association (AAA), *Clearing the Confusion: Common Naming for Advanced Driver Assistance Systems* (July 25, 2022), <https://newsroom.aaa.com/wp-content/uploads/2023/02/Clearing-the-Confusion-One-Pager-New-Version-7-25-22.pdf>.
- 4 Keith Barry, *Guide to Lane Departure Warning & Lane Keeping Assist*, Consumer Reports (May 9, 2022), <https://www.consumerreports.org/cars/car-safety/lane-departure-warning-lane-keeping-assist-guide-a7087080070/>.
- 5 Pete Norloff, *Eye Tracking Technology is Making New Cars Safer*, Eyegaze (Sep. 19, 2019), <https://eyegaze.com/eye-tracking-technology-is-making-new-cars-safer/>.
- 6 Brenda Leong, FPF Releases "Understanding Facial Detection, Characterization, and Recognition Technologies" and "Privacy Principles for Facial Recognition Technology in Commercial Applications," Future of Privacy Forum (Sep. 20, 2018), <https://fpf.org/blog/fpf-releases-understanding-facial-detection-characterization-and-recognition-technologies-and-privacy-principles-for-facial-recognition-technology-in-commercial-applications/>.
- 7 Vasileios Selimis, *Eye-Tracking Technology in Vehicles: Application and Design* 116–17 (City University London, Aug. 2015), https://scholar.google.com/scholar_url?url=https://core.ac.uk/download/pdf/42630671.pdf&hl=en&sa=X&ei=MtDeZKyKJouNy9YPme6JyAU&scisq=AFWwaebUoBmTEAJQP6FtDj219w7t&oi=scholarr.
- 8 Mike Lenné, *The World is Waking Up to Driver Monitoring Systems*, Tech Crunch (November 15, 2021), <https://techcrunch.com/2021/11/15/the-world-is-waking-up-to-driver-monitoring-systems/>; see also *Lexus Safety Technology*, Lexus (last visited Jan. 11, 2024), <https://www.lexus.com/safety>; *Ford Driver Assist Technologies*, Ford (last visited Jan. 11, 2024), <https://www.ford.com/technology/driver-assist-technology/>.
- 9 BAC represents the percentage of alcohol within the bloodstream. Szymon Paprocki et al., Review of Ethanol Intoxication Sensing Technologies and Techniques, 22 *Sensors* 6819 (Sep. 9, 2022), <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9501510/>; Harding P, Field PH. Breathalyzer accuracy in actual law enforcement practice: a comparison of blood- and breath-alcohol results in Wisconsin drivers. *J Forensic Sci.* 1987 Sep;32(5):1235–40. PMID: 3668478.
- 10 The SFST, which is used to determine if a driver is impaired by alcohol or drugs, is comprised of three scientifically-proven tests: the horizontal gaze nystagmus (HGN), the walk-and-turn, and one-leg stand tests. If a driver fails any one of these tests, then the driver is administered a breath test or a blood test.
- 11 Intoxication is "the point at which alcohol depresses the central nervous system so that mood and physical and mental abilities are noticeably changed." What is Intoxication?, University of Notre Dame Division of Student Affairs (last visited Jan. 11, 2024), <https://mcwell.nd.edu/your-well-being/physical-well-being/alcohol/what-is-intoxication/#:~:text=Intoxication%20is%20the%20point%20at,mental%20abilities%20are%20noticeably%20changed>. The legal definition of intoxication is a Blood Alcohol Content (BAC) of .08 grams, which 49 states and the District of Columbia have adopted, with some imposing higher penalties on those with higher percentages when driving under the influence ("DUI"/"drunk driving"). Utah is the only state where the threshold is .05 grams. New .05 BAC Law, Utah Department of Public Safety (last visited Jan. 11, 2024), <https://highwaysafety.utah.gov/drive-sober/new-05-bac-law/>.
- 12 Advanced Impaired Driving Prevention Technology, 89 Fed. Reg. 830 (Jan. 5, 2024) (to be codified at 49 C.F.R. § 571).
- 13 *Id.* at 849
- 14 State Ignition Interlock Laws, National Conference of State Legislatures (NCSL) (Sep. 24, 2021), <https://www.ncsl.org/transportation/state-ignition-interlock-laws#:~:text=The%20court%20may%20require%20that,functioning%2C%20certified%20ignition%20interlock%20device>.
- 15 *Can I Voluntarily Install an Ignition Interlock Device?*, Alcolock (last visited Jan. 11, 2024), <https://alcolockusa.com/faq/can-i-voluntarily-install-an-ignition-interlock-device/>.
- 16 *Increasing Alcohol Ignition Interlock Use*, Centers for Disease Control and Prevention (CDC) (Dec. 29, 2022), https://www.cdc.gov/transportationsafety/impaired_driving/ignition_interlock_states.html.
- 17 *How Does an Ignition Interlock Device Work?* LifeSafer (last visited Jan. 11, 2024), https://www.lifesafes.com/blog/how-does-an-ignition-interlock-device-work/#:~:text=Camera%20ignition%20interlocks%20will%20also,a%20printed%20or%20_electronic%20format.
- 18 Advanced Impaired Driving Prevention Technology, 89 Fed. Reg. 830 at 831 (Jan. 5, 2024) (to be codified at 49 C.F.R. § 571). It should be noted that in the most recent review of all technologies, NHTSA determines that in their current state, the available technologies specifically for intoxication detection do not fit the likely rule, but with further improvements, they might.
- 19 Driver Alcohol Detection System for Safety (DADSS) (last visited July 24, 2023), <https://dadss.org/>.
- 20 Joel McConvey, Face Biometrics Coming to Vehicles Will Allow Keyless Access and More, Biometric Update (Dec. 14, 2022), <https://www.biometricupdate.com/202212/face-biometrics-coming-to-vehicles-will-allow-keyless-access-and-more>.
- 21 Press Release, Hyundai, *Hyundai Reveals World's First Smart Fingerprint Technology to Vehicle* (Dec. 24, 2018), <https://www.hyundai.news/eu/articles/press-releases/hyundai-reveals-worlds-first-smart-fingerprint-technology-to-vehicles.html>.
- 22 Touch Technology, Driver Alcohol Detection System for Safety (DADSS), <https://dadss.org/touch-technology/> (last visited Mar. 01, 2024).
- 23 Measurement begins by shining an infrared light on the driver's skin, similar to a low-power flashlight. A portion of the light is reflected back to the skin's surface, where it can reveal information on the skin's unique chemical properties, including alcohol concentration within an individual's system. Susan Ferguson et al. *Driver Alcohol Detection System for Safety (DADSS). Background and Rationale for Technology Approaches*, SAE Technical Paper 2010-01-1580 (2010), <https://doi.org/10.4271/2010-01-1580>.

- 24 Meet SOBRsafe, SOBRsafe, <https://sobrsafe.com/about-us/#meet-sobrsafe>. (last visited Jan. 23, 2024).
- 25 *Model Y Owner's Manual: Cabin Camera*, Tesla (last visited Jan. 11, 2024), https://www.tesla.com/ownersmanual/modely/en_us/GUID-EDAD116F-3C73-40FA-A861-68112FF7961F.html.
- 26 Keith Barry, *How Driver Monitoring Systems Can Protect Drivers and Their Privacy*, Consumer Reports, Feb. 17, 2022), <https://www.consumerreports.org/electronics/privacy/driver-monitoring-systems-can-protect-drivers-and-privacy-a7714760430/>.
- 27 *Connected Car Infographic Version 1.0*, Future of Privacy Forum (June 27, 2017), https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf.
- 28 Kristin Cohen, *Location, Health and Other Sensitive Information: FTC Committed to Fully Enforcing the Law Against Illegal Use and Sharing of Highly Sensitive Data*, Federal Trade Commission (July 11, 2022), <https://www.ftc.gov/business-guidance/blog/2022/07/location-health-and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal>.
- 29 Revised Code of Washington § 19.373.005 - 19.373.900 (2023).
- 30 *Examples of Data Points Used in Profiling*, Privacy International (April 2018), https://privacyinternational.org/sites/default/files/2018-04/data%20points%20used%20in%20tracking_0.pdf.
- 31 Yassine Zahraoui et al., *Driver Profiling: The Pathway to Deeper Personalization*, 34 J. of King Saud Univ. – Comput. and Info. Sci. 9088 (Nov. 2022), <https://www.sciencedirect.com/science/article/pii/S1319157822003160>. Driver profiling can be identified in two forms, those meant to respond to either driver preferences or driver behavior: setting the seat position would be a preference whereas nudges to prevent speeding would be driver behavior.
- 32 VIN Decoder, Nat'l Highway Traffic Safety Admin., <https://vpic.nhtsa.dot.gov/decoder/> (last visited Jan. 23, 2024); Michael D. Frenchik, *Vehicle Identification Number (VIN), Using Manufacturer VIN Specifications as a Standard*, Nat'l Highway Traffic Safety Admin. (NHTSA) (May 2016), <https://www.nhtsa.gov/sites/nhtsa.gov/files/frenchik-vin-vpic.pdf>.
- 33 Dave LaChance, *Judge Allows Suit Over Subaru Driver Monitoring to Proceed*, Repairer Driven News, (Nov. 30, 2022) <https://www.repairerdrivennews.com/2022/11/30/judge-allows-suit-over-subaru-driver-monitoring-to-proceed-to-trial/>.
- 34 *Third-Party Relationships*, National Institute of Standards and Technology (NIST) Computer Security Resource Center (last visited Jan. 11, 2024), https://csrc.nist.gov/glossary/term/third_party_relationships.
- 35 David Straughan, *What Are Insurance Companies Doing With All That Telematics Data?* AutoMo Blog (Sep. 12, 2023), <https://www.automoblog.net/telematics-data/>.
- 36 Kashmir Hill, *Automakers Are Sharing Consumers' Driving Behavior With Insurance Companies*, The New York Times, (Mar. 11, 2024) <https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html>.
- 37 Apostolos Ziakopoulos, *The Transformation of the Insurance Industry and Road Safety by Driver Safety Behaviour Telematics*, 10 Case Studies on Transport Policy 2271 (Dec. 2022) <https://doi.org/10.1016/j.cstp.2022.10.011>; Michele Bertonecello et al., *Unlocking the Full Life-Cycle Value from Connected-Car Data*, McKinsey & Company (Feb. 11, 2021), <https://www.mckinsey.com/industries/automotive-and-assembly/our-insights/unlocking-the-full-life-cycle-value-from-connected-car-data>; Thomas Brewster, *Cops Can Extract Data From 10,000 Different Car Models' Infotainment Systems*, Forbes (Dec. 1, 2022), <https://www.forbes.com/sites/thomasbrewster/2022/12/01/10000-cars-can-be-data-raided-by-police-ice-cbp-love-it/?sh=6aea4ea169d8>.
- 38 Mathilde Carlier, *New and Used Light Vehicle Sales in the United States from 2010 to 2022*, Statista (Aug. 29, 2023), <https://www.statista.com/statistics/183713/value-of-us-passenger-cas-sales-and-leases-since-1990/>.
- 39 Kashmir Hill, *Your Car is Tracking You. Abusive Partners May Be, Too*, The New York Times (Dec. 31, 2023), <https://www.nytimes.com/2023/12/31/technology/car-trackers-gps-abuse.html>.
- 40 Infrastructure Investment and Jobs Act, Pub. L. No. 117-58, § 24220, 135 Stat. 149, 831-833 (2021). <https://www.congress.gov/bill/117th-congress/house-bill/3684/text>; the Secretary of Transportation, acting through the Administrator of the National Highway Traffic Safety Administration (NHTSA), must establish the FMVSS under Title 49 U.S.C. section 30111. *Id.* at §24220(b)(1)(A)(i)).
- 41 Press Release, Congresswoman Debbie Dingell, *Dingell: Time for Congress to take Action to Prevent Drunk Driving* (March 14, 2019), <https://debbiedingell.house.gov/news/documentsingle.aspx?DocumentID=1676>; Press Release, Congresswoman Debbie Dingell, *Dingell Releases Updates to Drunk Driving Bill* (Sep. 17, 2019), <https://debbiedingell.house.gov/news/documentsingle.aspx?DocumentID=1906>.
- 42 Press Release, Senator Ben Lujan, *Lujan, Scott Introduce Bipartisan Legislation to Prevent Drunk Driving and Help Save Lives* (April 22, 2021), <https://www.lujan.senate.gov/newsroom/press-releases/lujan-scott-introduce-bipartisan-legislation-to-prevent-drunk-driving-and-help-save-lives/>.
- 43 Press Release, Mothers Against Drunk Driving (MADD), *MADD Hails Monumental Drunk Driving Prevention Provision in Infrastructure Bill Passed by U.S. House of Representatives* (Nov. 6, 2021), <https://madd.org/press-release/madd-hails-monumental-drunk-driving-prevention-provision-in-infrastructure-bill-passed-by-u-s-house-of-representatives/>.
- 44 Emily Caldwell, *Texas Sen. John Cornyn Raises Privacy Concerns over Drunken Driving Prevention Tech*, The Dallas Morning News, (Aug. 29, 2022), <https://www.dallasnews.com/news/politics/2022/08/29/sen-john-cornyn-raises-privacy-concerns-over-drunk-driving-prevention-tech-in-cars/>. For the purposes of this report and to keep in line with the ANPRM, FPF will not be addressing drugged driving, although it is something that may also be detected through the technologies described within this report.
- 45 See *supra* IA. This data came from the Fatality Analysis Reporting System (FARS), a comprehensive database of fatal traffic crashes maintained by NHTSA and pulled from self-reported data from agencies within all 50 U.S. states as well as the District of Columbia and Puerto Rico. See <https://www.nhtsa.gov/crash-data-systems/fatality-analysis-reporting-system>.
- 46 NHTSA Drunk Driving Statistics and Risk Factors, <https://www.nhtsa.gov/risky-driving/drunk-driving> (last visited July 24, 2023).
- 47 See *supra* 38.
- 48 *Id.* at 831-33.

- 49 *Id.* at § 24220(a)(3); see also *Traffic Safety Fact 2014 Data: Alcohol-Impaired Driving*, Nat'l Highway Traffic Safety Admin. (Dec. 2015), <https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812231>
- 50 *Traffic Safety Facts – 2021 Data: Alcohol-Impaired Driving*, Nat'l Highway Traffic Safety Admin. (June 2023), <https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/813450>.
- 51 Press Release, White House, *President Biden to Sign Bipartisan Infrastructure Investment and Jobs Act Monday* (Nov. 10, 2021), <https://www.whitehouse.gov/briefing-room/statements-releases/2021/11/10/president-biden-to-sign-bipartisan-infrastructure-investment-and-jobs-act-monday/>.
- 52 For information on the rulemaking process see *A Guide to the Rulemaking Process*, Office of the Federal Register (last visited Jan. 11, 2024), https://www.federalregister.gov/uploads/2011/01/the_rulemaking_process.pdf.
- 53 Advanced Impaired Driving Prevention Technology, 89 Fed. Reg. 830 (Jan. 5, 2024) (to be codified at 49 C.F.R. § 571).
- 54 According to the proposed rule, “[a]dvanced drunk and impaired driving prevention technology” means a system that (A) can—(i) passively monitor the performance of a driver of a motor vehicle to accurately identify whether that driver may be impaired; and (ii) prevent or limit motor vehicle operation if an impairment is detected; (B) can—(i) passively and accurately detect whether the blood alcohol concentration of a driver of a motor vehicle is equal to or greater than the blood alcohol concentration described in section 163(a) of title 23, United States Code; and (ii) prevent or limit motor vehicle operation if a blood alcohol concentration above the legal limit is detected; or (C) is a combination of systems described in subparagraphs (A) and (B). Infrastructure Investment and Jobs Act, Pub. L. No. 117-58, § 24220(b)(1), 135 Stat. 149, 831032 (2021).
- 55 In the law, “passenger motor vehicle” is defined by Title 49 U.S.C. § 32101, and “new” is defined by Title 49 C.F.R. § 37.3 as “has not been purchased for purposes other than resale.”
- 56 Advanced Impaired Driving Prevention Technology, 89 Fed. Reg. 830 at 831 n.3 (Jan. 5, 2024) (to be codified at 49 C.F.R. § 571).
- 57 *Infrastructure Investment and Jobs Act*, Pub. L. No. 117-58, § 24220(d), 135 Stat. 149, 832 (2021).
- 58 See National Highway Traffic Safety Administration (NHTSA) (last visited Jan. 11, 2024), <https://www.nhtsa.gov/>.
- 59 49 U.S.C. 30101 et seq.
- 60 For further background on NHTSA activities related to cybersecurity and privacy see *Connected Cars: Privacy, Security Issues Related to Connected, Automated Vehicles*, Federal Trade Commission (June 28, 2017), <https://www.ftc.gov/news-events/events/2017/06/connected-cars-privacy-security-issues-related-connected-automated-vehicles>.
- 61 Gov. Accountability Office, *Vehicle Data Privacy: Industry and Federal Efforts Under Way but NHTSA Needs to Define Its Role* (Aug. 28, 2017), <https://www.gao.gov/products/gao-17-656>.
- 62 Nat'l Highway Traffic Safety Admin., *Cybersecurity Best Practices for the Safety of Modern Vehicles* (Sep. 2022), <https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf>; Nat'l Highway Traffic Safety Admin., *Vehicle Data Privacy* (last visited July 24, 2023), <https://www.nhtsa.gov/technology-innovation/vehicle-data-privacy#resources>; Nat'l Highway Traffic Safety Admin., *Automated Driving Systems* (last visited July 24, 2023), <https://www.nhtsa.gov/vehicle-manufacturers/automated-driving-systems>; see also 87 FR 37289, <https://www.federalregister.gov/documents/2022/06/22/2022-12860/event-data-recorders>.
- 63 Katie Malone, *Every Car is a Smart Car, and it's a Privacy Nightmare*, Engadget (Nov. 6, 2023), <https://www.engadget.com/every-car-is-a-smart-car-and-its-a-privacy-nightmare-193010478.html>.
- 64 The driver survey was conducted in July 2023 with a sample size of 2063, aged 21+ who either currently own a driver's license or have owned a driver's license in the past 5 years, including an oversample of 723 respondents who do not currently own or lease a car but plan to in the next 5 years.
- 65 For questions from the survey and results discussed here, see the Appendix, page (14). For a complete list of survey questions please contact FPF directly.
- 66 Appendix, Fig 1
- 67 Appendix, Fig 1
- 68 Appendix, Fig 2
- 69 Appendix, Fig 2
- 70 Appendix, Fig 5
- 71 Appendix, Fig 5
- 72 Appendix, Fig 3
- 73 Appendix, Fig 3
- 74 Appendix, Fig 4
- 75 Appendix, Fig 7 & 8
- 76 Appendix, Fig 10
- 77 Appendix, Fig 5
- 78 Appendix, Fig 6
- 79 Appendix, Fig 5 & 6
- 80 Appendix, Fig 10
- 81 Appendix, Fig 13
- 82 Appendix, Fig 13
- 83 Appendix, Fig 12
- 84 Appendix, Fig 14
- 85 Appendix, Fig 10
- 86 *Fair Information Practice Principles (FIPPs)*, Fed. Priv. Council, <https://www.fpc.gov/resources/fipps/> (last visited Jan. 11, 2024).
- 87 *Id.*

-
- 88 *Data Minimization Principle*, Int'l Ass'n of Priv. Pro. (IAPP) Res. Ctr., <https://iapp.org/resources/article/data-minimization-principle/> (last visited Jan. 11, 2024).
- 89 Some vehicle manufacturers offer drivers a clear and user-friendly guide on how to delete their personal data that is easily readable and accessible. *Personal Data Deletion*, Toyota, <https://www.toyota.co.uk/owners/vehicle-information/personal-data-deletion> (last visited Jan. 11, 2024); see also *Delete User Data From Your Volvo*, Volvo (Dec. 12, 2023), <https://www.volvocars.com/uk/support/topic/ee7af37a635a923ec0a80151057b4e38>.
- 90 The California Privacy Protection Act and the General Data Protection Regulation (GDPR) both impose substantial transparency obligations on organizations and establish a clear rights for individuals to request deletion of their personal information have organizations provide them with details on their data and give the option to delete it. *California Consumer Privacy Act (CCPA)*, State of Cal. Dep't of Just. Off. of the Att'y Gen., <https://oag.ca.gov/privacy/ccpa> (last visited Jan. 11, 2024); see also Art. 17, *Regulation (EU) 2016/679*, (General Data Protection Regulation) (hereafter cited as GDPR) *GDPR – Right to Erasure ('Right to be Forgotten')*, Intersoft Consulting, <https://gdpr-info.eu/art-17-gdpr/> (last visited Jan. 11, 2024).
- 91 *Cybersecurity Best Practices for the Safety of Modern Vehicles*, Nat'l Highway Traffic Safety Admin. (Sept. 2022), <https://www.nhtsa.gov/sites/nhtsa.gov/files/2022-09/cybersecurity-best-practices-safety-modern-vehicles-2022-tag.pdf>.
- 92 Appendix, Fig 11
- 93 Appendix, Fig 12 & 13
- 94 Appendix, Fig 5 & 6
- 95 *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, National Institute for Standards and Technology (Jan. 2023), <https://doi.org/10.6028/NIST.AI.100-1>; see also *Algorithmic Impact Assessment: User Guide*, Ada Lovelace Institute (Feb. 8, 2022), <https://www.adalovelaceinstitute.org/resource/aia-user-guide/>.
- 96 Charles M. Farmer, *Potential Lives Saved by In-Vehicle Alcohol Detection Systems*, 22 *Traffic Inj. Prevention* 7 (Nov. 12, 2020), <https://doi.org/10.1080/15389588.2020.1836366>.
- 97 *Consumer Privacy Protection Principles: Privacy Principles for Vehicle Technologies and Services*, Alliance for Automotive Innovation, (Nov. 12, 2014, reviewed March 2022), https://www.autosinnovate.org/innovation/Automotive%20Privacy/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services-03-21-19.pdf.
- 98 *Our Members*, Alliance for Automotive Innovation (Jan. 11, 2024), <https://www.autosinnovate.org/about/our-members>.
- 99 Jan Shelly Brown et al., *The Impact of Generative AI on Black Communities*, McKinsey Inst. for Black Econ. Mobility (Dec. 19, 2023), <https://www.mckinsey.com/bem/our-insights/the-impact-of-generative-ai-on-black-communities>.
- 100 Dr. Nicol Turner Lee & Caitlin Chin-Rothmann, *Police Surveillance and Facial Recognition: Why Data Privacy is Imperative for Communities of Color*, Brookings Inst. (Apr. 12, 2022), <https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/>.
- 101 Marin Cogan, *How Cars Fuel Racial Inequality*, Vox (June 13, 2023), <https://www.vox.com/23735896/racism-car-ownership-driving-violence-traffic-violations>.

ALLIANCE FOR AUTOMOTIVE INNOVATION, INC.

Consumer Privacy

Protection Principles

PRIVACY PRINCIPLES FOR VEHICLE TECHNOLOGIES AND SERVICES

Established: November 12, 2014
Reviewed: May 2018, March 2022

ALLIANCE FOR AUTOMOTIVE INNOVATION, INC.
CONSUMER PRIVACY PROTECTION PRINCIPLES
PRIVACY PRINCIPLES FOR
VEHICLE TECHNOLOGIES AND SERVICES

I. INTRODUCTION

The automotive industry is developing innovative technologies and services that promise to deliver substantial benefits and enhance the driving experience. These technologies and services may assist in enhancing safety, reducing the environmental impacts of vehicles, diagnosing vehicle malfunctions, calling for emergency assistance, detecting and preventing vehicle theft, reducing traffic congestion, improving vehicle efficiency and performance, delivering navigation services, providing valuable information services, and more. The Alliance for Automotive Innovation (Auto Innovators)¹ and their members are excited about the benefits offered by today's vehicle technologies and services and look forward to expanding the array of innovative technologies and services offered to consumers.

Many of these technologies and services are based upon information obtained from a variety of vehicle systems and involve the collection of information about a vehicle's location or a driver's use of a vehicle. Consumer trust is essential to the success of vehicle technologies and services. Auto Innovators and their members understand that consumers want to know how these vehicle technologies and services can deliver benefits to them while respecting their privacy.

Privacy is important to consumers, and it is important to us. That is why Auto Innovators have issued these Privacy Principles ("Principles"). The Principles provide an approach to customer privacy that members can choose to adopt when offering innovative vehicle technologies and services. Each member has made an independent decision about whether to adopt the Principles, and other companies may choose to adopt them as well. We provide a list of those companies that have adopted the Principles in the Appendix, and they are referred to as "Participating Members."

The Principles apply to the collection, use, and sharing of [Covered Information](#) in association with [Vehicle Technologies and Services](#) available on cars and light trucks sold or leased to individual consumers for personal use in the United States.

¹ On Jan. 1, 2020, The Alliance of Automobile Manufacturers, Inc. and the Association of Global Automakers, Inc. combined to form The Alliance for Automotive Innovation, Inc. The list of Participating Members reflects the list of companies that signed on to the document prior to the combined organization.

ALLIANCE FOR AUTOMOTIVE INNOVATION, INC.

CONSUMER PRIVACY PROTECTION PRINCIPLES

The Principles are subject to change over time. When they do change, Auto Innovators will post the updated Principles at and <https://www.autosinnovate.org/privacy>. The Principles are not intended to replace inconsistent or conflicting applicable laws and regulations, where they exist. So, the Principles should be interpreted as subject to and superseded by applicable laws and regulations. Participating Members may implement the Principles in different ways, reflecting differences in technologies and other factors. And Participating Members may choose to incorporate into their privacy programs elements that are not addressed in the Principles and are free to take additional privacy steps. But regardless of how Participating Members design their privacy programs and implement the Principles, Participating Members affirm the following fundamentals, as detailed in the relevant sections that follow:

- **Transparency:** Participating Members commit to providing [Owners](#) and [Registered Users](#) with ready access to clear, meaningful notices about the Participating Member's collection, use, and sharing of [Covered Information](#).
- **Choice:** Participating Members commit to offering [Owners](#) and [Registered Users](#) with certain choices regarding the collection, use, and sharing of [Covered Information](#).
- **Respect for Context:** Participating Members commit to using and sharing [Covered Information](#) in ways that are consistent with the context in which the [Covered Information](#) was collected, taking account of the likely impact on [Owners](#) and [Registered Users](#).
- **Data Minimization, De-Identification & Retention:** Participating Members commit to collecting [Covered Information](#) only as needed for legitimate business purposes. Participating Members commit to retaining [Covered Information](#) no longer than they determine necessary for legitimate business purposes.
- **Data Security:** Participating Members commit to implementing reasonable measures to protect [Covered Information](#) against loss and unauthorized access or use.

ALLIANCE FOR AUTOMOTIVE INNOVATION, INC.

CONSUMER PRIVACY PROTECTION PRINCIPLES

- **Integrity & Access:** Participating Members commit to implementing reasonable measures to maintain the accuracy of [Covered Information](#) and commit to giving [Owners](#) and [Registered Users](#) reasonable means to review and correct [Personal Subscription Information](#).
- **Accountability:** Participating Members commit to taking reasonable steps to ensure that they and other entities that receive [Covered Information](#) adhere to the Principles.

The application of these fundamental principles is described in more detail in the sections that follow.

II. APPLICABILITY

The Principles apply to the collection, use, and sharing of [Covered Information](#) in association with [Vehicle Technologies and Services](#) available on cars and light trucks sold or leased to individual consumers for personal use in the United States.

Participating Members are listed in the Appendix.

Each Participating Member commits to complying with the Principles for new vehicles manufactured no later than Model Year 2017 (which may begin as early as January 2, 2016) and for [Vehicle Technologies and Services](#) subscriptions that are initiated or renewed on or after January 2, 2016. To the extent practicable, each Participating Member commits to implementing the Principles for [Covered Information](#) collected from vehicles manufactured before January 2, 2016. If compliance with the Principles involves a vehicle engineering change, each Participating Member commits to complying with the Principles as soon as practicable, but by no later than vehicle Model Year 2018.

Some Participating Members may work with [Third-party Service Providers](#) to provide some or all of their [Vehicle Technologies and Services](#). When doing so, Participating Members commit to taking reasonable steps to ensure that [Third-party Service Providers](#) adhere to the Principles in providing [Vehicle Technologies and Services](#) that involve the collection, use, or sharing of [Covered Information](#). Businesses other than [Third-party Service Providers](#) may provide [Owners](#) and [Registered Users](#) with apps or other offerings that involve the collection of information from vehicles. Participating

ALLIANCE FOR AUTOMOTIVE INNOVATION, INC.

CONSUMER PRIVACY PROTECTION PRINCIPLES

Members will encourage those businesses to respect the privacy of [Owners](#) and [Registered Users](#) and will take reasonable steps to provide those businesses with an opportunity to provide [Owners](#) and [Registered Users](#) with information about the businesses' privacy practices.

However, the Principles directly apply only to Participating Members. The Principles do not apply directly to vehicle dealerships that are not owned by Participating Members.

III. SCOPE OF THE PRINCIPLES AND DEFINITIONS

The Principles provide a framework for Participating Members to embrace when collecting, using, and sharing [Covered Information](#). The following defined terms are used in the Principles. Together, the definitions describe the scope of the Principles.

Affirmative Consent: An [Owner's](#) or [Registered User's](#) clear action performed in response to a clear, meaningful, and prominent notice disclosing the collection, use, and sharing of [Covered Information](#).

Biometrics: [Covered Information](#) about an [Owner's](#) or [Registered User's](#) physical or biological characteristics that serves to identify the person.

Covered Information: 1) [Identifiable Information](#) that vehicles collect, generate, record, or store in an electronic form that is retrieved from the vehicles by or on behalf of a Participating Member in connection with [Vehicle Technologies and Services](#); or 2) [Personal Subscription Information](#) provided by individuals subscribing or registering for [Vehicle Technologies and Services](#).

Exclusion from Covered Information: If Participating Members collect [Covered Information](#) and then alter or combine the information so that the information can no longer reasonably be linked to the vehicle from which the information was retrieved, the [Owner](#) of that vehicle, or any other individual, the information is no longer [Covered Information](#). If Participating Members attempt to link the information to specific, identified individuals or vehicles or share the information without prohibiting the recipients from attempting such linking, the information becomes [Covered Information](#).

ALLIANCE FOR AUTOMOTIVE INNOVATION, INC.

CONSUMER PRIVACY PROTECTION PRINCIPLES

Driver Behavior Information: [Covered Information](#) about how a person drives a vehicle. Examples are vehicle speed, seat belt use, and information about braking habits. This does not include information that is used only for safety, diagnostics, warranty, maintenance, or compliance purposes.

Geolocation Information: [Covered Information](#) about the precise geographic location of a vehicle.

Identifiable Information: Information that is linked or reasonably linkable to i) the vehicle from which the information was retrieved, ii) the [Owner](#) of that vehicle, or iii) the [Registered User](#) using [Vehicle Technologies and Services](#) associated with the vehicle from which the information was retrieved.

Owners: Those individuals who have legal title to a vehicle that receives or is equipped with [Vehicle Technologies and Services](#) that use [Covered Information](#); those entitled to possession of such a vehicle, like purchasers under an agreement (for example, a vehicle loan where the vehicle is collateral); and those entitled to possession of such a vehicle as lessees pursuant to a written lease agreement that, at its inception, is for a period of more than three months. The term “Owners” does not include lienholders and lenders.

Personal Subscription Information: Information that individuals provide during the subscription or registration process that on its own or in combination with other information can identify a person, such as a name, address, credit card number, telephone number, or email address.

Registered User: An individual other than an [Owner](#) who registers with, and provides [Personal Subscription Information](#) to, a Participating Member in order to receive [Vehicle Technologies and Services](#) that use [Covered Information](#).

Third-party Service Providers: Companies unaffiliated with Participating Members that receive [Covered Information](#) when conducting business on behalf of a Participating Member.

Vehicle Technologies and Services: Technologies and services provided by, made available through, or offered on behalf of Participating Members that involve the

ALLIANCE FOR AUTOMOTIVE INNOVATION, INC.

CONSUMER PRIVACY PROTECTION PRINCIPLES

collection, use, or sharing of information that is collected, generated, recorded, or stored by a vehicle.

IV. SPECIFIC PRINCIPLES

1. TRANSPARENCY

Participating Members commit to providing [Owners](#) and [Registered Users](#) with ready access to clear, meaningful notices about the Participating Member's collection, use, and sharing of [Covered Information](#).

Participating Members commit to providing notices in a manner that enables [Owners](#) and [Registered Users](#) to make informed decisions.

How Participating Members may provide notices: Participating Members may make notices available in a variety of ways. Depending on the nature of the [Vehicle Technologies and Services](#) and the circumstances in which they are offered, different mechanisms may be reasonable to provide [Owners](#) and [Registered Users](#) with ready access to clear, meaningful notices about the [Covered Information](#) that Participating Members collect, use, and share. There is no one-size-fits-all approach. Among the various ways Participating Members may choose to provide notices are in owners' manuals, on paper or electronic registration forms and user agreements, or on in-vehicle displays. At a minimum, Participating Members commit to making information regarding the collection, use, and sharing of [Covered Information](#) publicly available via online web portals.

When Participating Members may provide notices: Participating Members commit to taking reasonable steps to provide [Owners](#) and [Registered Users](#) with ready access to clear, meaningful notices prior to initial collections of [Covered Information](#). Notices need not be provided prior to every instance of collection where addressed by prior notices.

Content of notices: Participating Members commit to designing the notices so that they provide [Owners](#) and [Registered Users](#) with clear, meaningful information about the following:

ALLIANCE FOR AUTOMOTIVE INNOVATION, INC.

CONSUMER PRIVACY PROTECTION PRINCIPLES

- the types of [Covered Information](#) that will be collected;
- the purposes for which that [Covered Information](#) is collected;
- the types of entities with which the [Covered Information](#) may be shared;
- the deletion or de-identification of [Covered Information](#);
- the choices [Owners](#) and [Registered Users](#) may have regarding [Covered Information](#);
- whether and how [Owners](#) and [Registered Users](#) may access any [Covered Information](#); and
- where [Owners](#) and [Registered Users](#) may direct questions about the collection, use, and sharing of [Covered Information](#).

Notices regarding the collection of [Geolocation Information](#), [Biometrics](#), and [Driver Behavior Information](#): When Participating Members collect, use, or share [Geolocation Information](#), [Biometrics](#), or [Driver Behavior Information](#), Participating Members commit to providing clear, meaningful, and prominent notices about the collection of such information, the purposes for which it is collected, and the types of entities with which the information may be shared. Please see the Choice section below for information about the Principles' [Affirmative Consent](#) conditions if Participating Members use [Geolocation Information](#), [Biometrics](#), or [Driver Behavior Information](#) as a basis for marketing or share such information with unaffiliated third parties for their own purposes.

Changing notices: Participating Members commit to taking reasonable steps to alert [Owners](#) and [Registered Users](#) prior to changing the collection, use, or sharing practices associated with [Covered Information](#) in ways that have a material impact on [Owners](#) or [Registered Users](#). If the new practices involve using [Covered Information](#) in a materially different manner than claimed when the [Covered Information](#) was collected, Participating Members commit to obtaining [Affirmative Consent](#) from [Owners](#) and [Registered Users](#) to the new practices.

ALLIANCE FOR AUTOMOTIVE INNOVATION, INC.

CONSUMER PRIVACY PROTECTION PRINCIPLES

2. CHOICE

Participating Members commit to offering [Owners](#) and [Registered Users](#) with certain choices regarding the collection, use, and sharing of [Covered Information](#).

Certain safety, operations, compliance, and warranty information may be collected by necessity without choice.

When Participating Members provide notices consistent with the Transparency principle, an [Owner's](#) or [Registered User's](#) acceptance and use of [Vehicle Technologies and Services](#) constitutes consent to the associated information practices, subject to the [Affirmative Consent](#) provisions below.

Participating Members understand that the sharing and use of [Geolocation Information](#), [Biometrics](#), and [Driver Behavior Information](#) can raise concerns in some situations, therefore Participating Members also commit to obtaining [Affirmative Consent](#) expeditiously for the following practices:

- using [Geolocation Information](#), [Biometrics](#), or [Driver Behavior Information](#) as a basis for marketing; and
- sharing [Geolocation Information](#), [Biometrics](#), or [Driver Behavior Information](#) with unaffiliated third parties for their own purposes, including marketing.

[Affirmative Consent](#) is not required, however, when [Geolocation Information](#), [Biometrics](#), or [Driver Behavior Information](#) is used or shared

- as reasonably necessary to protect the safety, property, or rights of Participating Members, [Owners](#), [Registered Users](#), drivers, passengers, or others (this includes sharing information with emergency service providers);
- only for safety, operations, compliance, or warranty purposes;
- for internal research or product development;

ALLIANCE FOR AUTOMOTIVE INNOVATION, INC.

CONSUMER PRIVACY PROTECTION PRINCIPLES

- as reasonably necessary to facilitate a corporate merger, acquisition, or sale involving a Participating Member's business;
- as reasonably necessary to comply with a lawful government request, regulatory requirement, legal order, or similar obligation, which, in the case of requests or demands from governmental entities for [Geolocation Information](#), must be in the form of a warrant or court order, absent exigent circumstances or applicable statutory authority; and
- to assist in the location or recovery of a vehicle reasonably identified as stolen.

Participating Members also need not obtain [Affirmative Consent](#) when sharing [Geolocation Information](#), [Biometrics](#), or [Driver Behavior Information](#) with [Third-party Service Providers](#) that assist in providing [Vehicle Technologies and Services](#) if those parties are not permitted to use that information for their independent use and the sharing is consistent with the notices that Participating Members have provided.

Participating Members may obtain [Affirmative Consent](#) at the time of vehicle purchase or lease, when registering for a service, or at another time.

3. RESPECT FOR CONTEXT

Participating Members commit to using and sharing [Covered Information](#) in ways that are consistent with the context in which the [Covered Information](#) was collected, taking account of the likely impact on [Owners](#) and [Registered Users](#).

The context of collection: Various factors will determine the context of collection, including the notices offered to [Owners](#) and [Registered Users](#), the permissions that they have provided, their reasonable expectations, and how the use or sharing will likely impact them.

- When Participating Members present clear, meaningful notices about how [Covered Information](#) will be used and shared, that use and sharing is consistent with the context of collection.

ALLIANCE FOR AUTOMOTIVE INNOVATION, INC.

CONSUMER PRIVACY PROTECTION PRINCIPLES

- Participating Members commit to making reasonable and responsible use of [Covered Information](#) and may share that information as reasonable for those uses. Reasonable and responsible practices may vary over time as business practices and consumer expectations evolve.

The following examples illustrate some of the reasonable and responsible ways in which Participating Members may use or share [Covered Information](#) consistent with the context of collecting that information, taking into account the likely impact on [Owners](#) and [Registered Users](#). The list is not meant to be exhaustive.

- Using or sharing [Covered Information](#) as reasonably necessary to provide requested or subscribed services;
- Using or sharing [Covered Information](#) to respond to a possible emergency or other situation requiring urgent attention;
- Using or sharing [Covered Information](#) to conduct research or analysis for vehicles or [Vehicle Technologies and Services](#);
- Using or sharing [Covered Information](#) to diagnose or troubleshoot vehicle systems;
- Using or sharing [Covered Information](#) as reasonably necessary to facilitate a corporate merger, acquisition, or sale involving a Participating Member's business;
- Sharing [Covered Information](#) for operational purposes with affiliated companies that are clearly associated with the Participating Member or with the [Vehicle Technologies and Services](#) from which the [Covered Information](#) was collected or derived;
- Using or sharing [Covered Information](#) to prevent fraud and criminal activity, or to safeguard [Covered Information](#) associated with [Owners](#) or their vehicles;
- Using or sharing [Covered Information](#) to improve products and services or develop new offerings associated with [Vehicle Technologies and Services](#), vehicles, vehicle safety, security, or transportation infrastructure;
- Using [Covered Information](#) to provide [Owners](#) or [Registered Users](#) with information about goods and services that may be of interest to them;
- Sharing [Covered Information](#) as reasonably necessary to comply with a lawful government request, regulatory requirement, legal order, or similar obligation, which in the case of requests or demands from governmental 10

ALLIANCE FOR AUTOMOTIVE INNOVATION, INC.

CONSUMER PRIVACY PROTECTION PRINCIPLES

entities for [Geolocation Information](#), must be in the form of a warrant or court order, absent exigent circumstances or applicable statutory authority; and

- Using or sharing [Covered Information](#) to protect the safety, property, or rights of [Owners](#), Participating Members, or others.

4. DATA MINIMIZATION, DE-IDENTIFICATION & RETENTION

Participating Members commit to collecting [Covered Information](#) only as needed for legitimate business purposes. Participating Members commit to retaining [Covered Information](#) no longer than they determine necessary for legitimate business purposes.

5. DATA SECURITY

Participating Members commit to implementing reasonable measures to protect [Covered Information](#) against loss and unauthorized access or use.

Reasonable measures to protect [Covered Information](#): Reasonable measures include standard industry practices. Those practices evolve over time and in reaction to evolving threats and identified vulnerabilities.

6. INTEGRITY & ACCESS

Participating Members commit to implementing reasonable measures to maintain the accuracy of [Covered Information](#) and commit to offering [Owners](#) and [Registered Users](#) reasonable means to review and correct [Personal Subscription Information](#).

Participating Members may provide the means to review and correct [Personal Subscription Information](#) in a variety of ways, including but not limited to web portals, mobile applications, or in-vehicle tools.

Participating Members commit to exploring additional means of providing [Owners](#) and [Registered Users](#) with reasonable access to [Covered Information](#), taking into account potential security and privacy issues.

ALLIANCE FOR AUTOMOTIVE INNOVATION, INC.

CONSUMER PRIVACY PROTECTION PRINCIPLES

7. ACCOUNTABILITY:

- *Participating Members commit to taking reasonable steps to ensure that they and other entities that receive [Covered Information](#) adhere to the Principles.*

Accountability mechanisms that Participating Members may implement:

Participating Members commit to implementing reasonable policies, procedures, and practices to help ensure adherence to the Principles. Participating Members may implement training programs for employees and other personnel that handle [Covered Information](#). Participating Members may consider creating internal privacy review boards to evaluate and approve new technologies and services involving [Covered Information](#). Participating Members should make available reporting mechanisms for consumers to report concerns to Participating Members. Participating Members also commit to taking reasonable steps to ensure that [Third-party Service Providers](#) adhere to the Principles in providing [Vehicle Technologies and Services](#) that involve the collection, use, or sharing of [Covered Information](#).

V. CONTACT INFORMATION

ALLIANCE FOR AUTOMOTIVE INNOVATION

1050 K ST NW, SUITE 650
WASHINGTON, DC 20001
[TEL: \(202\) 326-5500](tel:(202)326-5500)

**ALLIANCE FOR AUTOMOTIVE INNOVATION, INC.
CONSUMER PRIVACY PROTECTION PRINCIPLES**

**Appendix
Participating Members**

**AMERICAN HONDA MOTOR CO., INC.
ASTON MARTIN LAGONDA OF NORTH AMERICA,
INC.
BMW OF NORTH AMERICA, LLC
CHRYSLER GROUP LLC
FERRARI NORTH AMERICA
FORD MOTOR COMPANY
GENERAL MOTORS LLC
HYUNDAI MOTOR AMERICA
JAGUAR LAND ROVER NORTH AMERICA, LLC
KIA MOTORS AMERICA
MASERATI NORTH AMERICA, INC.
MAZDA NORTH AMERICAN OPERATIONS
MERCEDES–BENZ USA, LLC
MITSUBISHI MOTORS NORTH AMERICA, INC.
NISSAN NORTH AMERICA, INC.
PORSCHE CARS NORTH AMERICA
SUBARU OF AMERICA, INC.
TOYOTA MOTOR SALES, USA
VOLKSWAGEN GROUP OF AMERICA, INC.
VOLVO CAR GROUP**

Guidelines



13

Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications

Version 2.0

Adopted on 9 March 2021

Adopted

1

Version history

Version 2.0	9 March 2021	Adoption of the Guidelines after public consultation
Version 1.0	28 January 2020	Adoption of the Guidelines for public consultation

1	INTRODUCTION	4
1.1	Related works	5
1.2	Applicable law	6
1.3	Scope.....	8
1.4	Definitions	11
1.5	Privacy and data protection risks.....	13
2	GENERAL RECOMMENDATIONS.....	15
2.1	Categories of data	15
2.2	Purposes.....	17
2.3	Relevance and data minimisation.....	17
2.4	Data protection by design and by default	18
2.5	Information	21
2.6	Rights of the data subject	23
2.7	Security	23
2.8	Transmitting personal data to third parties.....	24
2.9	Transfer of personal data outside the EU/EEA	25
2.10	Use of in-vehicle Wi-Fi technologies.....	26
3	CASE STUDIES	26
3.1	Provision of a service by a third party	26
3.2	eCall.....	30
3.3	Accidentology studies	33
3.4	Tackle auto theft	35

The European Data Protection Board

Having regard to Article 70 (1) (e) of the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, (hereinafter “GDPR”),

Having regard to the EEA Agreement and in particular to Annex XI and Protocol 37 thereof, as amended by the Decision of the EEA joint Committee No 154/2018 of 6 July 2018¹,

Having regard to Article 12 and Article 22 of its Rules of Procedure,

HAS ADOPTED THE FOLLOWING GUIDELINES

1 INTRODUCTION

1. Symbol of the 20th century economy, the automobile is one of the mass consumer products that has impacted society as a whole. Commonly associated with the notion of freedom, cars are often considered as more than just a means of transportation. Indeed, they represent a private area in which people can enjoy a form of autonomy of decision, without encountering any external interferences. Today, as connected vehicles move into the mainstream, such a vision no longer corresponds to the reality. In-vehicle connectivity is rapidly expanding from luxury models and premium brands to high-volume midmarket models, and vehicles are becoming massive data hubs. Not only vehicles, but drivers and passengers are also becoming more and more connected. As a matter of fact, many models launched over the past few years on the market integrate sensors and connected on-board equipment, which may collect and record, among other things, the engine performance, the driving habits, the locations visited, and potentially even the driver’s eye movements, his or her pulse, or biometric data for the purpose of uniquely identifying a natural person.²
2. Such data processing is taking place in a complex ecosystem, which is not limited to the traditional players of the automotive industry, but is also shaped by the emergence of new players belonging to the digital economy. These new players may offer infotainment services such as online music, road condition and traffic information, or provide driving assistance systems and services, such as autopilot software, vehicle condition updates, usage-based insurance or dynamic mapping. Moreover, since vehicles are connected via electronic communication networks, road infrastructure managers and telecommunications operators involved in this process also play an important role with respect to the potential processing operations applied to the drivers’ and passengers’ personal data.
3. In addition, connected vehicles are generating increasing amounts of data, most of which can be considered personal data since they will relate to drivers or passengers. Even if the

¹ References to “Member States” made throughout this document should be understood as references to “EEA Member States”.

² Infographic “Data and the connected car” by the Future of Privacy Forum; https://fpf.org/wp-content/uploads/2017/06/2017_0627-FPF-Connected-Car-Infographic-Version-1.0.pdf

data collected by a connected car are not directly linked to a name, but to technical aspects and features of the vehicle, it will concern the driver or the passengers of the car. As an illustration, data relating to the driving style or the distance covered, data relating to the wear and tear on vehicle parts, location data or data collected by cameras may concern driver behaviour as well as information about other people who could be inside or data subjects that pass by. Such technical data are produced by a natural person, and permit his/her direct or indirect identification, by the data controller or by another person. The vehicle can be considered as a terminal that can be used by different users. Therefore, as for a personal computer, this potential plurality of users does not affect the personal nature of the data.

4. In 2016, the Fédération Internationale de l'Automobile (FIA) ran a campaign across Europe called "My Car My Data" to get a sentiment on what Europeans think about connected cars.³ While it showed the high interest of drivers for connectivity, it also highlighted the vigilance that must be exercised with regard to the use of the data produced by vehicles as well as the importance of complying with personal data protection legislation. Thus, the challenge is, for each stakeholder, to incorporate the "protection of personal data" dimension from the product design phase, and to ensure that car users enjoy transparency and control in relation to their data in accordance with recital 78 GDPR. Such an approach helps to strengthen user confidence, and thus the long-term development of those technologies.

1.1 Related works

5. Connected vehicles have become a substantial subject for regulators over the last decade, with a major increase in the last couple of years. Various works have thus been published at the national and international levels concerning the security and privacy of connected vehicles. Those regulations and initiatives aim at complementing the existing data protection and privacy frameworks with sector specific rules or providing guidance to professionals.

1.1.1 European-level and international initiatives

6. Since 31 March 2018, a 112-based eCall in-vehicle system is mandatory on all new types of M1 and N1 vehicles (passenger cars and light duty vehicles).^{4,5} In 2006, the Article 29 Working Party had already adopted a working document on data protection and privacy implications in eCall initiative.⁶ In addition, as previously discussed, the Article 29 Working Party also adopted an opinion in October 2017 regarding the processing of personal data in the context of Cooperative Intelligent Transport Systems (C-ITS).
7. In January 2017, the European Union Agency for Network and Information Security (ENISA) published a study focused on cyber security and resilience of smart cars listing the sensitive assets as well as the corresponding threats, risks, mitigation factors and possible security

³ Campaign "My Car My Data"; <http://www.mycarmydata.eu/>.

⁴ The interoperable EU-wide eCall; https://ec.europa.eu/transport/themes/its/road/action_plan/ecall_en.

⁵ Decision No 585/2014/EU of the European Parliament and of the Council of 15 May 2014 on the deployment of the interoperable EU-wide eCall service Text with EEA relevance; <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014D0585>.

⁶ Working document on data protection and privacy implications in eCall initiative; http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2006/wp125_en.pdf.

measures to implement.⁷ In September 2017, the International Conference of Data Protection and Privacy Commissioners (ICDPPC) adopted a resolution on connected vehicles.⁸ Finally, in April 2018, the International Working Group on Data Protection in Telecommunications (IWGDPT), also adopted a working paper on connected vehicles.⁹

1.1.2 National initiatives of European Data Protection Board (EDPB) members

8. In January 2016, the Conference of the German Federal and State Data Protection Authorities and the German Association of the Automotive Industry (VDA) published a common declaration on the principles of data protection in connected and not-connected vehicles.¹⁰ In August 2017, the UK Centre for Connected and Autonomous Vehicles (CCAV) released a guide stating principles of cyber security for connected and automated vehicles in order to raise awareness on the matter within the automotive sector.¹¹ In October 2017, the French data protection authority, the Commission Nationale de l'Informatique et des Libertés (CNIL), released a compliance package for connected cars in order to provide assistance to stakeholders on how to integrate data protection by design and by default, enabling data subjects to have effective control over their data.¹²

1.2 Applicable law

9. The relevant EU legal framework is the GDPR. It applies in any case where data processing in the context of connected vehicles involves processing personal data of individuals.
10. Additionally to the GDPR, directive 2002/58/EC as revised by 2009/136/EC (hereinafter – “ePrivacy directive”), **sets a specific standard for all actors that wish to store or access information stored in the terminal equipment of a subscriber or user in the European Economic Area (EEA).**
11. Indeed, if most of the ePrivacy directive provisions (art. 6, art. 9, etc.) only apply to providers of publicly available electronic communication services and providers of public communication networks, art. 5(3) ePrivacy directive is a general provision. It does not only apply to electronic communication services but also to every entity, private or public, that places on or reads information from a terminal equipment without regard to the nature of the data being stored or accessed.

⁷ Cyber security and resilience of smart cars; <https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars>.

⁸ Resolution on data protection in automated and connected vehicles; https://edps.europa.eu/sites/edp/files/publication/resolution-on-data-protection-in-automated-and-connected-vehicles_en_1.pdf.

⁹ Working paper on connected vehicles; <https://www.datenschutz-berlin.de/infothek-und-service/veroeffentlichungen/working-paper/>.

¹⁰ Data protection aspects of using connected and non-connected vehicles; https://www.lda.bayern.de/media/dsk_joint_statement_vda.pdf.

¹¹ Principles of cyber security for connected and automated vehicles; <https://www.gov.uk/government/publications/principles-of-cyber-security-for-connected-and-automated-vehicles>.

¹² Compliance package for a responsible use of data in connected cars; <https://www.cnil.fr/en/connected-vehicles-compliance-package-responsible-use-data>.

12. Regarding the notion of “terminal equipment”, the definition is given by directive 2008/63/CE¹³. Art. 1 (a) defines the terminal equipment as an “*equipment directly or indirectly connected to the interface of a public telecommunications network to send, process or receive information; in either case (direct or indirect), the connection may be made by wire, optical fibre or electromagnetically; a connection is indirect if equipment is placed between the terminal and the interface of the network; (b) satellite earth station equipment*”.
13. As a result, provided that the aforementioned criteria are met, the connected vehicle and device connected to it should be considered as a “terminal equipment” (just like a computer, a smartphone or a smart TV) and provisions of art. 5(3) ePrivacy directive apply where relevant.
14. As outlined by the EDPB in its opinion 5/2019 on the interplay between the ePrivacy directive and the GDPR,¹⁴ art. 5(3) ePrivacy directive provides that, as a rule, and subject to the exceptions to that rule mentioned in paragraph 17 below, prior consent is required for the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user. To the extent that the information stored in the end-user’s device constitutes personal data, art. 5(3) ePrivacy directive shall take precedence over art. 6 GDPR with regards to the activity of storing or gaining access to this information.¹⁵ Any processing operations of personal data following the aforementioned processing operations, including processing personal data obtained by accessing information in the terminal equipment, must have a legal basis under art. 6 GDPR in order to be lawful.¹⁶
15. Since the controller, when seeking consent for the storing or gaining of access to information pursuant to art. 5(3) ePrivacy directive, will have to inform the data subject about all the purposes of the processing – including any processing following the aforementioned operations (meaning the “subsequent processing”) – consent under art. 6 GDPR will generally be the most adequate legal basis to cover the processing of personal data following such operations (as far as the purpose of the following processing is comprehended by the data subject’s consent, see paragraphs 53-54 below). Hence, consent will likely constitute the legal basis both for the storing and gaining of access to information already stored and the subsequent processing of personal data¹⁷. Indeed, when assessing compliance with art. 6 GDPR, one should take into account that the processing as a whole involves specific activities for which the EU legislature has sought to provide additional protection.¹⁸ Moreover, controllers must take into account the impact on data subjects’

¹³ Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment (Codified version) (Text with EEA relevance); <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32008L0063>.

¹⁴ European Data Protection Board, Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities, adopted on 12 March 2019 (hereinafter - “Opinion 5/2019”), paragraph 40.

¹⁵ Ibid, paragraph 40.

¹⁶ Ibid, paragraph 41.

¹⁷ Consent required by art. 5(3) of the “ePrivacy” directive and consent needed as a legal basis for the processing of data (art. 6 GDPR) for the same specific purpose can be collected at the same time (for example, by checking a box clearly indicating what the data subject is consenting to).

¹⁸ Opinion 5/2019, paragraph 41.

rights when identifying the appropriate lawful basis in order to respect the principle of fairness.¹⁹ The bottom line is that art. 6 GDPR cannot be relied upon by controllers in order to lower the additional protection provided by art. 5(3) ePrivacy directive.

16. The EDPB recalls that the notion of consent in the ePrivacy directive remains the notion of consent in the GDPR and must meet all the requirements of the consent as provided by art. 4(11) and 7 GDPR.
17. However, while consent is the principle, art. 5(3) ePrivacy directive allows the storing of information or the gaining of access to information that is already stored in the terminal equipment to be exempted from the requirement of informed consent, if it satisfies one of the following criteria:
 - **Exemption 1:** for the sole purpose of carrying out the transmission of a communication over an electronic communications network;
 - **Exemption 2:** when it is strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.
18. In such cases, the processing of personal data including personal data obtained by accessing information in the terminal equipment is based on one of the legal bases as provided by art. 6 GDPR. For example, consent is not needed when data processing is necessary to provide GPS navigation services requested by the data subject when such services can be qualified as information society services.

1.3 Scope

19. The EDPB would like to point out that these guidelines are intended to facilitate compliance of the processing of personal data carried out by a wide range of stakeholders working in this environment. However, they are not intended to cover all use cases possible in this context or to provide guidance for every possible specific situation.
20. The scope of this document focuses in particular on the personal data processing in relation to the non-professional use of connected vehicles by data subjects: e.g., drivers, passengers, vehicle owners, other road users, etc. More specifically, it deals with the personal data: (i) processed inside the vehicle, (ii) exchanged between the vehicle and personal devices connected to it (e.g., the user's smartphone) or (iii) collected locally in the vehicle and exported to external entities (e.g., vehicle manufacturers, infrastructure managers, insurance companies, car repairers) for further processing.
21. The connected vehicle definition has to be understood as a broad concept in this document. It can be defined as a vehicle equipped with many electronic control units (ECU) that are linked together via an in-vehicle network as well as connectivity facilities allowing it to share information with other devices both inside and outside the vehicle. As such, data can be exchanged between the vehicle and personal devices connected to it, for instance allowing the mirroring of mobile applications to the car's in-dash information and entertainment unit. Also, the development of standalone mobile applications, meaning independent of the vehicle (for example, relying on the sole use of the smart phone) to assist drivers is included

¹⁹ European Data Protection Board, Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0, 8 October 2019, paragraph 1.

in the scope of this document since they contribute to the vehicle's connectivity capacities even though they may not effectively rely on the transmission of data with the vehicle *per*

se. Applications for connected vehicles are multiple and diverse and can include²⁰:

22. *Mobility management*: functions that allow drivers to reach a destination quickly, and in a cost-efficient manner, by providing timely information about GPS navigation, potentially dangerous environmental conditions (e.g., icy roads), traffic congestion or road construction work, parking lot or garage assistance, optimised fuel consumption or road pricing.
23. *Vehicle management*: functions that are supposed to aid drivers in reducing operating costs and improving ease of use, such as notification of vehicle condition and service reminders, transfer of usage data (e.g., for vehicle repair services), customised “Pay As/How You Drive” insurances, remote operations (e.g., heating system) or profile configurations (e.g., seat position).
24. *Road safety*: functions that warn the driver of external hazards and internal responses, such as collision protection, hazard warnings, lane departure warnings, driver drowsiness detection, emergency call (eCall) or crash investigation “black-boxes” (event data recorder).
25. *Entertainment*: functions providing information to and involving the entertainment of the driver and passengers, such as smart phone interfaces (hands free phone calls, voice generated text messages), WLAN hot spots, music, video, Internet, social media, mobile office or “smart home” services.
26. *Driver assistance*: functions involving partially or fully automated driving, such as operational assistance or autopilot in heavy traffic, in parking, or on highways,
27. *Well-being*: functions monitoring the driver's comfort, ability and fitness to drive such as fatigue detection or medical assistance.
28. Hence, vehicles can be natively connected or not and personal data can be collected through several means, including: (i) vehicle sensors, (ii) telematics boxes or (iii) mobile applications (e.g. accessed from a device belonging to a driver). In order to fall within the scope of this document, mobile applications need to be related to the environment of driving. For example, GPS navigation applications are in-scope. Applications whose functionalities only suggest places of interest (restaurants, historic monument, etc.) to drivers fall, however, outside the scope of these guidelines.
29. Much of the data that is generated by a connected vehicle relate to a natural person that is identified or identifiable and thus constitute personal data. For instance, data include directly identifiable data (e.g., the driver's complete identity), as well as indirectly identifiable data such as the details of journeys made, the vehicle usage data (e.g., data relating to driving style or the distance covered), or the vehicle's technical data (e.g., data relating to the wear and tear on vehicle parts), which, by cross-referencing with other files and especially the vehicle identification number (VIN), can be related to a natural person. Personal data in connected vehicles can also include metadata, such as vehicle maintenance status. In other words, any data that can be associated with a natural person therefore fall into the scope of this document.

²⁰ PwC Strategy 2014. “In the fast lane. The bright future of connected cars”:
https://www.strategyand.pwc.com/media/file/Strategyand_In-the-Fast-Lane.pdf.

30. The connected vehicle ecosystem covers a wide spectrum of stakeholders. This ecosystem more precisely includes traditional actors of the automotive industry as well as emerging players from the digital industry. Hence, these guidelines are directed towards vehicle manufacturers, equipment manufacturers and automotive suppliers, car repairers, automobile dealerships, vehicle service providers, fleet managers, motor insurance companies, entertainment providers, telecommunication operators, road infrastructure managers and public authorities as well as data subjects. The EDPB underlines that the categories of data subjects will differ from one service to another (e.g., drivers, owners, passengers, etc.). This is a non-exhaustive list as the ecosystem entails a wide variety of services, including services for which a direct authentication or identification is needed and services for which this is not needed.
31. Some data processing performed by natural persons within the vehicle fall within “*the course of a purely personal or household activity*” and are consequently out of the scope of the GDPR²¹. In particular, this concerns the use of personal data within the vehicles by the sole data subjects who provided such data into the vehicle’s dashboard. However, the EDPB recalls that according to its recital 18 the GDPR “*applies to controllers or processors which provide the means for processing personal data for such personal or household activities*”.

1.3.1 Out of scope of this document

32. Employers providing company cars to members of their staff might want to monitor their employee’s actions (e.g., in order to ensure the safety of the employee, goods or vehicles, to allocate resources, to track and bill a service or to check working time). Data processing carried out by employers in this context raises specific considerations to the employment context, which might be regulated by labour laws at the national level that cannot be detailed in these guidelines²².
33. While the data processing in the context of commercial vehicles used for professional purposes (such as public transport) and shared transport and MaaS solution may raise specific considerations which fall out of the scope of these general guidelines, many of the principles and recommendations set out here will also be applicable to those types of processing.
34. Connected vehicles being radio-enabled systems, they are subject to passive tracking such as Wi-Fi or Bluetooth tracking. In that sense they do not differ from other connected devices and fall in the scope of the ePrivacy directive which is currently being revised. This therefore excludes also large-scale tracking of Wi-Fi equipped vehicles²³ by a dense network of bystanders who use common smartphone location services. These routinely report all visible Wi-Fi networks to central servers. Since built-in Wi-Fi can be considered a secondary vehicle

²¹ See GDPR, Article 2(2)(c).

²² The Article 29 Working Party elaborated on this in its WP249 Opinion 2/2017 on data processing at work; https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169.

²³ See for details: <https://www.datenschutzzentrum.de/artikel/1269-Location-Services-can-Systematically-Track-Vehicles-with-WiFi-Access-Points-at-Large-Scale.html>.

identifier²⁴, this risks a systematic ongoing collection of complete vehicle movement profiles.

35. Vehicles are increasingly equipped with image recording devices (e.g., car parking camera systems or dashcams). Since this deals with the issue of filming public places, which requires an assessment of the relevant legislative framework which is specific to each Member State, this data processing is out of the scope of these guidelines.
36. The processing of data enabling Cooperative Intelligent Transport Systems (C-ITS) – as defined in the directive 2010/40/EU²⁵ has been dealt with in a specific opinion by the Article 29 Working Party²⁶. While the definition of the C-ITS concept in the directive does not bear any technical specifications, the Article 29 Working Party focuses in its opinion on short-range communications, i.e. that do not involve the intervention of a network operator. More specifically, it provides analysis for specific use cases built for initial deployment and committed to assess at a later stage the new issues that will be undoubtedly raised when higher level of automation will be implemented. Since the data protection implications in the context of C-ITS are very specific (unprecedented amounts of location data, continuous broadcasting of personal data, exchange of data between vehicles and other road infrastructural facilities, etc.) and that it is still being discussed at the European level, the processing of personal data in that context is not covered by these guidelines.
37. Finally, this document does not aim to address all possible issues and questions raised by connected vehicles and can therefore not be considered as exhaustive.

1.4 Definitions

38. The **processing** of personal data encompasses any operation that involves personal data such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, etc.²⁷
39. The **data subject** is the natural person to whom the data covered by the processing relate. In the context of connected vehicles, it can, in particular, be the driver (main or occasional), the passenger, or the owner of the vehicle.²⁸
40. The **data controller** is the person who determines the purposes and means of processing that take place in connected vehicles.²⁹ Data controllers can include

service providers that process vehicle data to send the driver traffic-information, eco-driving messages or alerts

²⁴ Markus Ullmann, Tobias Franz, and Gerd Nolden, Vehicle Identification Based on Secondary Vehicle Identifier - Analysis, and Measurements, in Proceedings, VEHICULAR 2017, The Sixth International Conference on Advances in Vehicular Systems, Technologies and Applications, Nice, France, July 23 to 27, 2017, p. 32-37.

²⁵ Directive 2010/40/EU of 7 July 2020 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport; <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32010L0040>.

²⁶ Article 29 Working Party - Opinion 03/2017 on Processing personal data in the context of Cooperative Intelligent Transport Systems (C-ITS); http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171.

²⁷ See GDPR, Article 4 (2).

²⁸ See GDPR, Article 4 (1).

²⁹ See GDPR, Article 4 (7) and the European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR (hereinafter - "Guidelines 07/2020").

regarding the functioning of the vehicle, insurance companies offering “*Pay As You Drive*” contracts, or vehicle manufacturers gathering data on the wear and tear affecting the vehicle’s parts to improve its quality. Pursuant to art. 26 GDPR, two or more controllers can jointly determine the purposes and means of the processing and thus be considered as joint controllers. In this case, they have to clearly define their respective obligations, especially as regards the exercising of the rights of data subjects and the provision of information as referred to in art. 13 and 14 GDPR.

41. The **data processor** is any person who processes personal data for and on behalf of the data controller.³⁰ The data processor collects and processes data on instruction from the data controller, without using those data for its own purposes. As an example, in a number of cases, equipment manufacturers and automotive suppliers may process data on behalf of vehicle manufacturers (which does not imply they cannot be a data controller for other purposes). In addition to requiring data processors to implement appropriate technical and organisational measures in order to guarantee a security level that is adapted to risk, art. 28 GDPR sets out data processors’ obligations.
42. The **recipient** means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.³¹ As an example, a commercial partner of the service provider that receives from the service provider personal data generated from the vehicle is a recipient of personal data. Whether they act as a new data controller or as a data processor, they shall comply with all the obligations imposed by the GDPR.
43. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients³²; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing. As an example, law enforcement authorities are authorised third parties when they request personal data as part of an investigation in accordance with European Union or Member State law.

³⁰ See GDPR, Article 4 (8) and the Guidelines 07/2020.

³¹ See GDPR, Article 4 (9) and the Guidelines 07/2020.

³² GDPR, Article 4 (9) and Recital 31.

1.5 Privacy and data protection risks

44. Article 29 Working Party has already expressed several concerns about Internet of Things (IoT) systems that can also apply to connected vehicles.³³ The issues relating to data security and control already stressed regarding IoT are even more sensitive in the context of connected vehicles, since it entails road safety concerns – and can impact the physical integrity of the driver – in an environment traditionally perceived as isolated and protected from external interferences.
45. Also, connected vehicles raises significant data protection and privacy concerns regarding the processing of location data as its increasingly intrusive nature can put a strain on the current possibilities to remain anonymous. The EDPB wants to place particular emphasis and raise stakeholders’ awareness to the fact that the use of location technologies requires the implementation of specific safeguards in order to prevent surveillance of individuals and misuse of the data.

1.5.1 Lack of control and information asymmetry

46. Vehicle drivers and passengers may not always be adequately informed about the processing of data taking place in or through a connected vehicle. The information may be given only to the vehicle owner, who may not be the driver, and may also not be provided in a timely fashion. Thus, there is a risk that there are insufficient functionalities or options offered to exercise the control necessary for affected individuals to avail themselves of their data protection and privacy rights. This point is of importance since, during their lifetime, vehicles may belong to more than one owner either because they are sold or because they are being leased rather than purchased.
47. Also, communication in the vehicle can be triggered automatically as well as by default, without the individual being aware of it. In the absence of the possibility to effectively control how the vehicle and its connected equipment interact, it is bound to become extraordinarily difficult for the user to control the flow of data. It will be even more difficult to control its subsequent use, and thereby prevent potential function creep.

1.5.2 Quality of the user’s consent

48. The EDPB underlines that, when the data processing is based on consent, all elements of valid consent have to be met which means that consent shall be free, specific and informed and constitutes an unambiguous indication of the data subject's wishes as interpreted in EDPB guidelines on consent.³⁴ Data controllers need to pay careful attention to the modalities of obtaining valid consent from different participants, such as car owners or car users. Such consent must be provided separately, for specific purposes and may not be bundled with the contract to buy or lease a new car. Consent must be as easily withdrawn as it is given.
49. The same has to be applied when consent is required to comply with the ePrivacy directive, for example if there is a storing of information or the gaining of access to information already stored in the vehicle as required in certain cases by art. 5(3) of the ePrivacy directive. Indeed, as outlined above, consent in this context has to be interpreted in light of the GDPR.

³³ Article 29 Working Party – Opinion 8/2014 on the Recent Developments on the Internet of Things; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.

³⁴ European Data Protection Board, Guidelines 05/2020 on consent under Regulation 2016/679, Version 1.1, 4 May 2020 (hereinafter - “Guidelines 05/2020”).

50. In many cases, the user may not be aware of the data processing carried out in his/her vehicle. Such lack of information constitutes a significant barrier to demonstrating valid consent under the GDPR, as the consent must be informed. In such circumstances, consent cannot be relied upon as a legal basis for the corresponding data processing under the GDPR.
51. Classic mechanisms used to obtain individuals' consent may be difficult to apply in the context of connected vehicles, resulting in a "low-quality" consent based on a lack of information or in the factual impossibility to provide fine-tuned consent in line with the preferences expressed by individuals. In practice, consent might also be difficult to obtain for drivers and passengers who are not related to the vehicle's owner in the case of secondhand, leased, rented or borrowed vehicles.
52. When the ePrivacy directive does not require the data subject consent, the controller nonetheless has the responsibility of choosing the legal basis under art. 6 GDPR that is most appropriate to the case for the processing of personal data.

1.5.3 Further processing of personal data

53. When data is collected on the basis of consent as required by art. 5(3) of the ePrivacy directive or on one of the exemptions of art. 5(3), and subsequently processed in accordance with art. 6 GDPR, it can only be further processed either if the controller seeks additional consent for this other purpose or if the data controller can demonstrate that it is based on a Union or Member State law to safeguard the objectives referred to in art. 23 (1) GDPR³⁵. The EDPB considers that further processing on the basis of a compatibility test according to art. 6(4) GDPR is not possible in such cases, since it would undermine the data protection standard of the ePrivacy directive. Indeed, consent, where required under the ePrivacy directive, needs to be specific and informed, meaning that data subjects must be aware of each data processing purpose and entitled to refuse specific ones³⁶. Considering that further processing on the basis of a compatibility test according to art. 6(4) of the GDPR is possible would circumvent the very principle of the consent requirements set forth by the current directive.
54. The EDPB recalls that the initial consent will never legitimise further processing as consent needs to be informed and specific to be valid.
55. For instance, telemetry data, which is collected during use of the vehicle for maintenance purposes may not be disclosed to motor insurance companies without the users consent for the purpose of creating driver profiles to offer driving behaviour-based insurance policies.
56. Furthermore, data collected by connected vehicles may be processed by law enforcement authorities to detect speeding or other infractions if and when the specific conditions in the law enforcement directive are fulfilled. In this case, such data will be considered as relating to criminal convictions and offences under the conditions laid down by art. 10 GDPR and any applicable national legislation. Manufacturers may provide the law enforcement authorities with such data if the specific conditions for such processing are fulfilled. The EDPB points out that processing of personal data for the sole purpose of fulfilling requests made by law enforcement authorities does not constitute a specified, explicit and legitimate purpose within the meaning of art. 5(1)(b) GDPR. When law enforcement authorities are authorized bylaw, they could be third parties within the meaning of art. 4(10) GDPR, in this case

³⁵ See also European Data Protection Board, Guidelines 10/2020 on restrictions under Article 23 GDPR.

manufacturers would be entitled to provide them with any data at their disposal subject to compliance with the relevant legal framework in each Member State.

1.5.4 Excessive data collection

57. With the ever-increasing number of sensors being deployed in connected vehicles there is a very high risk of excessive data collection compared to what is necessary to achieve the purpose.

58. The development of new functionalities and more specifically those based on machine learning algorithms may require a large amount of data collected over a long period of time.

1.5.5 Security of personal data

59. The plurality of functionalities, services and interfaces (e.g., web, USB, RFID, Wi-Fi) offered by connected vehicles increases the attack surface and thus the number of potential vulnerabilities through which personal data could be compromised. Unlike most IoT devices, connected vehicles are critical systems where a security breach may endanger the life of its users and people around. The importance of addressing the risk of hackers attempting to exploit connected vehicles' vulnerabilities is thus heightened.

60. In addition, personal data stored on vehicles and/or at external locations (e.g., in cloud computing infrastructures) must be adequately secured against unauthorized access. For instance, during maintenance, a vehicle has to be handed to a technician who will require access to some of the vehicle's technical data. While the technician needs to have access to the technical data, there is a possibility that the technician could attempt to access all the data stored in the vehicle.

2 GENERAL RECOMMENDATIONS

61. In order to mitigate the risks for data subjects identified above, the following general recommendations should be followed by vehicle and equipment manufacturers, service providers or any other stakeholder who may act as data controller or data processor in relation to connected vehicles.

2.1 Categories of data

62. As noted in the introduction, most data associated with connected vehicles will be considered personal data to the extent that it is possible to link it to one or more identifiable individuals. This includes technical data concerning the vehicle's movements (e.g., speed, distance travelled) as well concerning the vehicle's condition (e.g., engine coolant temperature, engine RPM, tyre pressure). Certain data generated by connected vehicles may also warrant special attention given their sensitivity and/or potential impact on the rights and interests of data subjects. At present, the EDPB has identified three categories of personal data warranting special attention, by vehicle and equipment manufacturers, service providers and other data controllers: location data, biometric data (and any special category of data as defined in art. 9 GDPR) and data that could reveal offences or traffic violations.

2.1.1 Location data

63. When collecting personal data, vehicle and equipment manufacturers, service providers and other data controllers should keep in mind that location data are particularly revealing of the life habits of data subjects. The journeys carried out are very characteristic in that they

enable one to infer the place of work and of residence, as well as a driver's centres of interest (leisure), and may possibly reveal sensitive information such as religion through the place of worship, or sexual orientation through the places visited. Accordingly, the vehicle and equipment manufacturer, service provider and other data controller should be particularly vigilant not to collect location data except if doing so is absolutely necessary for the purpose of processing. As an example, when the processing consists in detecting the vehicle's movement, the gyroscope is sufficient to fulfil that function, without there being a need to collect location data.

64. In general, collecting location data is also subject to compliance with the following principles:

- adequate configuration of the frequency of access to, and of the level of detail of, location data collected relative to the purpose of processing. For example, a weather application should not be able to access the vehicle's location every second, even with the consent of the data subject;
- providing accurate information on the purpose of processing (e.g., is location history stored? If so, what is its purpose?);
- when the processing is based on consent, obtaining valid (free, specific and informed) consent that is distinct from the general conditions of sale or use, for example on the on-board computer;
- activating location only when the user launches a functionality that requires the vehicle's location to be known, and not by default and continuously when the car is started;
- informing the user that location has been activated, in particular by using icons (e.g., an arrow that moves across the screen);
- the option to deactivate location at any time;
- defining a limited storage period.

2.1.2 Biometric data

65. In the context of connected vehicles, biometric data used for the purpose of uniquely identifying a natural person may be processed, within the remit of art. 9 GDPR and the national exceptions, among other things, to enable access to a vehicle, to authenticate the driver/owner, and/or to enable access to a driver's profile settings and preferences. When considering the use of biometric data, guaranteeing the data subject full control over his or her data involves, on the one hand, providing for the existence of a non-biometric alternative (e.g., using a physical key or a code) without additional constraint (that is, the use of biometrics should not be mandatory), and, on the other hand, storing and comparing the biometric template in encrypted form only on a local basis, with biometric data not being processed by an external reading/comparison terminal.

66. In the case of biometric data³⁷, it is important to ensure that the biometric authentication solution is sufficiently reliable, in particular by complying with the following principles:

³⁷ The prohibition principle set out in article 9.1 GDPR only relates to “*biometric data for the purpose of uniquely identifying a natural person*”.

- the adjustment of the biometric solution used (e.g., the rate of false positives and false negatives) is adapted to the security level of the required access control;
- the biometric solution used is based on a sensor that is resistant to attacks (such as the use of a flat-printed print for fingerprint recognition);
- the number of authentication attempts is limited;
- the biometric template/model is stored in the vehicle, in an encrypted form using a cryptographic algorithm and key management that comply with the state of the art;
- the raw data used to make up the biometric template and for user authentication are processed in real time without ever being stored, even locally.

2.1.3 Data revealing criminal offenses or other infractions

67. In order to process data that relate to potential criminal offences within the meaning of art. 10 GDPR, the EDPB recommends to resort to the local processing of the data where the data subject has full control over the processing in question (see discussion on local processing in section 2.4). Indeed – except for some exceptions (see the case study on accidentology studies presented below in section 3.3) – external processing of data revealing criminal offences or other infractions is forbidden. Thus, according to the sensitivity of the data, strong security measures such as those described in section 2.7 must be put in place in order to offer protection against the illegitimate access, modification and deletion of those data.
68. Indeed, some categories of personal data from connected vehicles could reveal that a criminal offence or other infraction has been or is being committed (“offence-related data”) and therefore be subject to special restrictions (e.g., data indicating that the vehicle crossed a white line, the instantaneous speed of a vehicle combined with precise location data). Notably, in the event that such data would be processed by the competent national authorities for the purposes of criminal investigation and prosecution of criminal offence, the safeguards provided for in art. 10 GDPR would apply.

2.2 Purposes

69. Personal data may be processed for a wide variety of purposes in relation to connected vehicles, including driver safety, insurance, efficient transportation, entertainment or information services. In accordance with the GDPR, data controllers must ensure that their purposes are “specified, explicit and legitimate”, not further processed in a way incompatible with those purposes and that there is a valid legal basis for the processing as required in art. 5 GDPR. Some concrete examples of purposes that may be pursued by data controllers operating in the context of connected vehicles are discussed in Part III of these guidelines, along with specific recommendations for each type of processing.

2.3 Relevance and data minimisation

70. To comply with the data minimization principle³⁸, vehicle and equipment manufacturers, service providers and other data controllers should pay special attention to the categories of data they need from a connected vehicle, as they shall only collect personal data that are relevant and necessary for the processing. For instance, location data are particularly intrusive and can reveal many life habits of

the data subjects. Accordingly, industry participants should be particularly vigilant not to collect location data except if doing so is

³⁸ GDPR, Article 5(1)(c).

absolutely necessary for the purpose of processing (see discussion on location data above, in section 2.1).

2.4 Data protection by design and by default

71. Taking into account the volume and diversity of personal data produced by connected vehicles, the EDPB notes that data controllers are required to ensure that technologies deployed in the context of connected vehicles are configured to respect the privacy of individuals by applying the obligations of data protection by design and by default as required by art. 25 GDPR. Technologies should be designed to minimize the collection of personal data, provide privacy-protective default settings and ensure that data subjects are well informed and have the option to easily modify configurations associated with their personal data. Specific guidance on how manufacturers and service providers can comply with data protection by design and by default could be beneficial for the industry and third party application providers.
72. Certain general practices, described below, can also help mitigate the risks to the rights and freedoms of natural persons associated with connected vehicles³⁹.

2.4.1 Local processing of personal data

73. In general, vehicle and equipment manufacturers, service providers and other data controllers should, wherever possible, use processes that do not involve personal data or transferring personal data outside of the vehicle (i.e., the data is processed internally). The nature of connected vehicles however does present risks, such as the possibility of attacks on local processing by outside actors or local data being leaked by selling parts of the vehicle. Therefore, adequate attention and security measures should be taken into account to ensure that local processing shall remain local. This scenario offers the advantage of guaranteeing to the user the sole and full control of his/her personal data and, as such, it presents, “by design”, less privacy risks especially by prohibiting any data processing by stakeholders without the data subject knowledge. It also enables the processing of sensitive data such as biometric data or data relating to criminal offenses or other infractions, as well as detailed location data which otherwise would be subject to stricter rules (see below). In the same vein, it presents fewer cybersecurity risks and involves little latency, which makes it particularly suited to automated driving-assistance functions. Some examples of this type of solution could include:
 - eco-driving applications that process data in the vehicle in order to display eco-driving advice
in real time on the on-board screen;
 - applications that involve a transfer of personal data to a device such as a smartphone under the user’s full control (via, for example, Bluetooth or Wi-Fi), and where the _____ vehicle’s data are not transmitted to the application providers or the vehicle manufacturers; this would include, for instance, coupling of smartphones to use the car’s display, multimedia systems, microphone (or other sensors) for phone calls, etc., to the extent that the data collected remain under the control of the data subject and is exclusively used to provide the service he or she has

requested;

- in-vehicle safety enhancing applications such as those that provide audible signals or vibrations of the steering wheel when a driver overtakes a car without indicating or straying over white

³⁹ See as well European Data Protection Board, Guidelines 4/2019 on Article 25 Data Protection by Design and by Default, Version 2.0, adopted on 20 October 2020 (hereinafter - “Guidelines 4/2019”).

Adopted

18

lines or which provides alerts as to the state of the vehicle (e.g., an alert on the wear and tear affecting brake pads);

- applications for unlocking, starting, and/or activating certain vehicle commands using the driver's biometric data that is stored within the vehicle (such as a face or voice models or fingerprint minutiae).

74. Applications such as the above involve processing carried out for the performance of purely personal activities by a natural person (i.e., without the transfer of personal data to a data controller or data processor). Therefore, in accordance with art. 2(2) GDPR, **these applications fall outside the scope of the GDPR.**

75. However, if the GDPR does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity, it does apply to controllers or processors, which provide the means for processing personal data for such personal or household activities (car manufacturers, service provider, etc.) in accordance with recital 18 GDPR. Hence, when they are acting as data controller or data processor, they must develop secure in-car application and with due respect to the principle of privacy by design and by default. In any case, according to recital 78 GDPR, *"When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfil their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations"*.⁴⁰ On the one hand, it will enhance the development of user-centric services and, on the other hand, it will facilitate and secure any further uses in the future which could fall back within the scope of the GDPR. More specifically, the EDPB recommends developing a secure in-car application platform, physically divided from safety relevant car functions so that the access to car data does not depend on unnecessary external cloud capabilities.

76. Local data processing should be considered by car manufacturers and service providers, whenever possible, to mitigate the potential risks of cloud processing, as they are underlined in the opinion on Cloud Computing released by the Article 29 Working Party.⁴¹

77. In general users should be able to control how their data are collected and processed in the vehicle:

- information regarding the processing must be provided in the driver's language (manual, settings, etc.);

-the EDPB recommends that only data strictly necessary for the functioning of the vehicle are

processed by default. Data subjects should have the possibility to activate or deactivate the data processing for each other purpose and controller/processor and have the possibility to delete the data concerned, taking into account the purpose and the legal

_____basis of the data processing;

⁴⁰ For more recommendations on privacy by design and privacy by default see also Guidelines 4/2019.

⁴¹ Article 29 Working Party – Opinion 5/2012 on Cloud Computing; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

- data should not be transmitted to any third parties (i.e., the user has sole access to the data);
- data should be retained only for as long as is necessary for the provision of the service or otherwise required by Union or Member State law;
- data subjects should be able to delete permanently any personal data before the vehicles are put up for sale;
- data subjects should, where feasible, have a direct access to the data generated by these applications.

78. Finally, while it may not always be possible to resort to local data processing for every use-case, “hybrid processing” can often be put in place. For instance, in the context of usage-based insurance, personal data regarding driving behaviour (such as the force exerted on the brake pedal, mileage driven, etc.) could either be processed inside the vehicle or by the telematics service provider on behalf of the insurance company (the data controller) to generate numerical scores that are transferred to the insurance company on a defined basis (e.g. on a monthly basis). In this way, the insurance company does not gain access to the raw behavioural data but only to the aggregate score that is the result of the processing. This ensures that principles of data minimization are satisfied by design. This also means that users must have the ability to exercise their right when data are stored by other parties: for example, a user should have the ability to delete data stored in the systems of a car maintenance shop or dealership under the conditions of art.17 GDPR.

2.4.2 Anonymization and pseudonymisation

79. If the transmission of personal data outside the vehicle is envisaged, consideration should be given to anonymize them before being transmitted. When anonymising the controller should take into account all processing involved which could potentially lead to re-identification of data, such as the transmission of locally anonymised data. The EDPB recalls that the principles of data protection do not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable⁴². Once a dataset is truly anonymised and individuals are no longer identifiable, European data protection law no longer applies. As a consequence, anonymisation, where relevant, may be a good strategy to keep the benefits and to mitigate the risks in relation to connected vehicles.

80. As detailed in the opinion by the Article 29 Working Party on anonymization techniques, various methods can be used – sometimes in combination – in order to reach data anonymisation.⁴³

81. Other techniques such as pseudonymisation⁴⁴ can help minimize the risks generated by the data processing, taking into account that in most cases, directly identifiable data are not necessary to achieve the purpose of the processing. Pseudonymisation, if reinforced by security safeguards, improves the protection of personal data by reducing the risks of

⁴² See GDPR, Article 4 (1) and Recital 26.

⁴³ WP29 - Opinion 05/2014 on Anonymisation Techniques; https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf.

⁴⁴ GDPR, Article 4 (5). Enisa report on December 03, 2019: <https://www.enisa.europa.eu/publications/pseudonymisation-techniques-and-best-practices>.

misuse. Pseudonymisation is reversible, unlike anonymisation, and pseudonymised data are considered as personal data subject to the GDPR.

2.4.3 Data protection impact assessments

82. Given the scale and sensitivity of the personal data that can be generated *via* connected vehicles; it is likely that processing – particularly in situations where personal data are processed outside of the vehicle - will often result in a high risk to the rights and freedoms of individuals. Where this is the case, industry participants will be required to perform a data protection impact assessment (DPIA) to identify and mitigate the risks as detailed in art. 35 and 36 GDPR. Even in the cases where a DPIA is not required, it is a best practice to conduct one as early as possible in the design process. This will allow industry participants to factor the results of this analysis into their design choices prior to the roll-out of new technologies.

2.5 Information

83. Prior to the processing of personal data, the data subject shall be informed of the identity of the data controller (e.g., the vehicle and equipment manufacturer or service provider), the purpose of processing, the data recipients, the period for which data will be stored, and the data subject's rights under the GDPR⁴⁵.

84. In addition, the vehicle and equipment manufacturer, service provider or other data controller should also provide the data subject with the following information, in clear, simple, and easily-accessible terms:

- the contact details of the data protection officer;
- the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;
- the explicit mention of the legitimate interests pursued by the data controller or by a third party, when such legitimate interests constitute the legal basis for processing;
- the recipients or categories of recipients of the personal data, if any;
- the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
- the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
- the existence of the right to withdraw consent at any time without affecting the lawfulness of processing based on consent before its withdrawal where the processing is based on consent;
- where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and safeguards used to transfer them;

- whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

⁴⁵ GDPR, Article 5 (1) (a) and 13. See also Article 29 Working Party, Guidelines on Transparency under Regulation 2016/679 (wp260rev.01), endorsed by the EDPB.

- the existence of automated decision-making, including profiling that produces legal effects concerning the data subject or similarly significantly affects the data subject, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. This could particularly be the case in relation to the provision of usage-based insurance to individuals;
- the right to lodge a complaint with a supervisory authority;
- information about further processing;
- In case of joint data controllership, clear and complete information about the responsibilities of each data controller.

85. In some cases, personal data is not collected directly from the individual concerned. For instance, a vehicle and equipment manufacturer may rely on a dealer to collect information about the owner of the vehicle in order to offer an emergency road side assistance service. When data have not been collected directly, the vehicle and equipment manufacturer, service provider or other data controller shall, in addition to the information mentioned above, also indicate the categories of personal data concerned, the source from which the personal data originate, and, if applicable, whether those data came from publicly accessible sources. That information must be provided by the controller within a reasonable period after obtaining the data, and **no later than the first of the following dates** in accordance with art. 14 (3) GDPR: (i) one month after the data are obtained, having regard to the specific circumstances in which the personal data are processed, (ii) upon first communication with the data subject, or (iii) if those data are transmitted to a third party, before the transmission of the data.

86. New information may also need to be provided to data subjects when they are taken care of by new data controller. A roadside assistance service that interacts with connected vehicles can be provided by different data controllers depending in which country or region the assistance is required. New data controllers should provide data subjects with the required information when data subjects cross borders and services that interact with connected vehicles are provided by new data controllers.

87. The information directed to the data subjects may be provided in layers⁴⁶, i.e. by separating two levels of information: on the one hand, first-level information, which is the most important for the data subjects, and, on the other hand, information that presumably is of interest at a later stage. The essential first-level information includes, in addition to the identity of the data controller, the purpose of the processing and a description of the data subject's rights, as well as any additional information on the processing which has the most impact on the data subject and processing which could surprise them. The EDPB recommends that, in the context of connected vehicles, the data subject should be made aware of all the recipients in the first layer of information. As stated in the WP29 guidelines on transparency, controllers should provide information on the recipients that is most meaningful for data subjects. In practice, this will generally be the named recipients, so that data subjects know exactly who has _____ their personal data. If controllers cannot provide the names of the recipients, the information should be as specific as possible by indicating the

⁴⁶ See Article 29 Working Party, Guidelines on Transparency under Regulation 2016/679 (wp260rev.01), endorsed by the EDPB.

type of recipient (i.e. by reference to the activities it carries out), the industry, sector and sub-sector, and the location of the recipients.

88. The data subjects may be informed by concise and easily understandable clauses in the contract of sale of the vehicle, in the contract for the provision of services, and/or in any written medium, by using distinct documents (e.g., the vehicle's maintenance record book or manual) or the on-board computer.
89. Standardised icons could be used in addition to the information necessary, as required under art. 13 and 14 GDPR, to enhance transparency by potentially reducing the need for vast amounts of written information to be presented to a data subject. It should be visible in vehicles in order to provide, in relation to the planned processing, a good overview that is understandable, and clearly legible. The EDPB emphasises the importance of standardising those icons, so that the user finds the same symbols regardless of the make or model of the vehicle. For example, when certain types of data are being collected, such as location, the vehicles could have a clear signal on-board (such as a light inside the vehicle) to inform passengers about data collection.

2.6 Rights of the data subject

90. Vehicle and equipment manufacturers, service providers and other data controllers should facilitate data subjects' control over their data during the entire processing period, through the implementation of specific tools providing an effective way to exercise their rights, in particular their right of access, rectification, erasure, their right to restrict the processing and, depending on the legal basis of the processing, their right to data portability and their right to object.
91. To facilitate settings modifications, a profile management system should be implemented in order to store the preferences of known drivers and help them to change easily their privacy settings anytime. The profile management system should centralize every data setting for each data processing, especially to facilitate the access, deletion, removal and portability of personal data from vehicle systems at the request of the data subject. Drivers should be enabled to stop the collection of certain types of data, temporarily or permanently, at any moment, unless there is a specific legal ground that the controller can rely on to continue the collection of specific data. In case of a contract that provides a personalized offer based on driving behaviour this may mean that the user as a result should be reverted to the standard conditions of that contract. These features should be implemented inside the vehicle, although it could also be provided to data subjects through additional means (e.g., dedicated application). Furthermore, in order to allow data subjects to quickly and easily remove personal data that can be stored on the car's dashboard (for example, GPS navigation history, web browsing, etc.), the EDPB recommends that manufacturers provide a simple functionality (such as a delete button).
92. The sale of a connected vehicle and the ensuing change of ownership should also trigger the deletion of any personal data, which is no longer needed for the previous specified purposes and the data subject should be able to exercise his or her right to portability.

2.7 Security

93. Vehicle and equipment manufacturers, service providers and other data controllers should put in place measures that guarantee the security and confidentiality of processed data and

take all useful precautions to prevent control being taken by an unauthorised person. In particular, industry participants should consider adopting the following measures:

- encrypting the communication channels by means of a state-of-the-art algorithm;
- putting in place an encryption-key management system that is unique to each vehicle, not to each model;
- when stored remotely, encrypting data by means of state-of-the-art algorithms;
- regularly renewing encryption keys;
- protecting encryptions keys from any disclosure;
- authenticating data-receiving devices;
- ensuring data integrity (e.g., by hashing);
- make access to personal data subject to reliable user authentication techniques (password, electronic certificate, etc.);

94. Concerning more specifically vehicle manufacturers, the EDPB recommends the implementation of the following security measures:

- partitioning the vehicle's vital functions from those always relying on telecommunication capacities (e.g., "infotainment");
- implementing technical measures that enable vehicle manufacturers to rapidly patch security vulnerabilities during the entire lifespan of the vehicle;
- for the vehicle's vital functions, give priority as much as possible to using secure means of communications that are specifically dedicated to transportation;
- setting up an alarm system in case of attack on the vehicle's systems, with the possibility of operating in downgraded mode⁴⁷;
- storing a log history of any access to the vehicle's information system, e.g. going back six months as a maximum period, in order to enable the origin of any potential attack to be understood and periodically carry out a review of the logged information to detect possible anomalies.

95. These general recommendations should be completed by specific requirements taking into account the characteristics and purpose of each data processing.

2.8 Transmitting personal data to third parties

96. In principle, only the data controller and the data subject have access to the data generated by a connected vehicle. However, the data controller may transmit personal data to a commercial partner (recipient), to the extent that such transmission lawfully relies on one of the legal bases stated in art. 6 GDPR.

⁴⁷ Downgraded mode is a vehicle operating mode ensuring that the functions essential for the safe operation of the vehicle (i.e., minimum safety requirements) would be guaranteed, even if other less important functionalities would be deactivated (e.g., the operation of the geo-guidance device can be considered as non-essential, as opposed to the braking system).

97. In view of the possible sensitivity of the vehicle-usage data (e.g., journeys made, driving style), the EDPB recommends that the data subject's consent be systematically obtained before their data are transmitted to a commercial partner acting as a data controller (e.g., by ticking a box that is not pre-ticked, or, where technically possible, by using a physical or logical device that the person can access from the vehicle). The commercial partner in turn becomes responsible for the data that it receives, and is subject to all the provisions of the GDPR.
98. The vehicle manufacturer, service provider or other data controller can transmit personal data to a data processor selected to play a part in providing the service to the data subject, provided the data processor shall not use those data for its own purpose. Data controllers and data processors shall draw up a contract or other legal document specifying the obligations of each party and setting out the provisions of art. 28 GDPR.

2.9 Transfer of personal data outside the EU/EEA

99. When personal data is transferred outside the European Economic Area, special safeguards are foreseen to ensure that the protection travels with the data.
100. As a consequence, the data controller may transfer personal data to a recipient only to the extent that such transfer is in accordance with the requirements laid down in Chapter V GDPR.

2.10 Use of in-vehicle Wi-Fi technologies

101. Advances in cellular technology have made it possible to easily use the Internet on the road. While it is possible to get Wi-Fi connectivity in a vehicle through a smartphone hotspot or a dedicated device (OBD-II dongle, wireless modem or router, etc.), most manufacturers offer nowadays models that include a built-in cellular data connection and are also capable of creating Wi-Fi networks. Depending on the case, various aspects must be considered:

-The Wi-Fi connectivity is offered as a service by a road professional, such as a taxi driver for its customers. In this case, the professional or his/her company might be considered as an internet service provider (ISP), hence be subject to specific obligations and restrictions regarding the processing of his / her clients' personal data.

-The Wi-Fi connectivity is put in place for the sole use of the driver (at the exclusion of the driver and his/her passengers). In this case, the processing of personal data is considered to be purely personal or household activity in accordance with art. 2(2)(c) and recital 18 GDPR.

102. In general, the proliferation of Internet connection interfaces via Wi-Fi poses greater risks to the privacy of individuals. Indeed, through their vehicles, users become continuous broadcasters, and can therefore be identified and tracked. In order to prevent tracking, easy to operate opt-out options ensuring the service set identifier (SSID) of the on-board Wi-Fi network is not collected should therefore be put in place by the vehicle and equipment manufacturers.

3 CASE STUDIES

103. This section addresses five specific examples of processing in the context of connected vehicles, which correspond to scenarios likely to be encountered by stakeholders in the sector. The examples cover data processing that requires calculating power which cannot be mobilised locally in the vehicle, and/or the sending of personal data to a third party to carry out further analysis or to provide further functionality remotely. For each type of processing, this document specifies the intended purposes, the categories of data collected, the retention period of such data, the rights of data subjects, the security measures to be implemented, and the recipients of the information. In the case some of these fields are not described in the following, the general recommendations described in the previous part apply.
104. The examples chosen are non-exhaustive and are meant to be indicative of the variety of types of processing, legal bases, actors, etc. that might be engaged in the context of connected vehicles.

3.1 Provision of a service by a third party

105. Data subjects may contract with a service provider in order to obtain added-value services relating to their vehicle. For example, a data subject may enter into a usage-based insurance contract that offers reduced insurance premiums for less driving ("Pay As You Drive") or good driving behaviour ("Pay How You Drive") and which necessitates monitoring of driving habits by the insurance company. A data subject could also contract with a company that offers roadside assistance in the event of a breakdown and which entails the transmission of the vehicle's location to the company or with a service provider in order to receive

messages or alerts relating to the vehicle's functioning (e.g., an alert on the state of brake wear, or a reminder of the technical-inspection date).

3.1.1 Usage-based insurance

106. "Pay as you drive" is a type of usage-based insurance that tracks the driver's mileage and/or driving habits to differentiate and reward "safe" drivers by giving them lower premiums. The insurer will require the driver to install a built-in telematics service, a mobile application or activate a built-in module from manufacturing that tracks the miles covered and/or the driving behaviour (braking pattern, rapid acceleration, etc.) of the policy holder. The information gathered by the telematic device will be used to assign the driver scores in order to analyse what risks he/she may pose to the insurance company.
107. As usage-based insurance requires consent under art. 5(3) of the ePrivacy directive, the EDPB outlines that the policy holder must have the choice to subscribe to a non-usage-based insurance policy. Otherwise, consent would not be considered freely given, as the performance of the contract would be conditional on the consent. Further, art. 7(3) GDPR requires that a data subject must have the right to withdraw consent.

3.1.1.1 Legal basis

108. When the data is collected through a publicly available electronic communication service (for example *via* the SIM card contained in the telematics device), consent will be needed in order to gain access to information that is already stored in the vehicle as provided by art. 5(3) ePrivacy directive. Indeed, none of the exemptions provided by those provisions can apply in this context: the processing is not for the sole purpose of carrying out the transmission of a communication over an electronic communications network nor does it relate to an information society service explicitly requested by the subscriber or user. Consent could be collected at the time of the conclusion of the contract.
109. As regards the processing of personal data following the storage or access to the end-user's terminal equipment, the insurance company can rely on art. 6(1)(b) GDPR in this specific context provided it can establish both that the processing takes place in the context of a valid contract with the data subject and that processing is necessary in order that the particular contract with the data subject can be performed. Insofar as the processing is objectively necessary for the performance of the contract with the data subject, the EDPB considers that reliance upon art. 6(1)(b) GDPR would not have the effect of lowering the additional protection provided by art. 5(3) of the ePrivacy directive in this specific instance. That legal basis is materialised by the data subject signing a contract with the insurance company.

3.1.1.2 Data collected

110. There are two types of personal data to be considered:
 - **commercial and transactional data:** data subject's identifying information, transaction-related data, data relating to means of payment, etc.;
 - **usage data:** personal data generated by the vehicle, driving habits, location, etc.
111. The EDPB recommends that, as far as possible, and given that there is a risk that the data collected via the telematics-box could be misused to create a precise profile of the driver's movements, raw data regarding driving behaviour should be either processed:

- inside the vehicle in telematics boxes or in the user's smartphone so that the insurer only accesses the results data (e.g., a score relating to driving habits), not detailed raw data (see section 2.1);
 - or by the telematics service provider on behalf of the controller (the insurance company) to generate numerical scores that are transferred to the insurance company on a defined basis. In this case, raw data and data directly relating to the identity of the driver must be separated. This means that the telematics service provider receives the real-time data, but does not know the names, licence plates, etc. of the policy holders. On the other hand, the insurer knows the names of policyholders, but only receives the scores and the total kilometres and not the raw data used to produce such scores.
112. Moreover, it has to be noted that if only the mileage is necessary for the performance of the contract, location data shall not be collected.

3.1.1.3 Retention period

113. In the context of data processing taking place for the performance of a contract (i.e. provision of a service), it is important to distinguish between two types of data before defining their respective retention periods:
- **commercial and transactional data:** those data can be retained in an active database for the full duration of the contract. At the end of the contract, they can be archived physically (on a separate medium: DVD, etc.) or logically (by authorisation management) in the event of possible litigation. Thereafter, at the end of the statutory limitation periods, the data shall be deleted or anonymised;
 - **usage data:** usage data can be classified as raw data and aggregated data. As stated above, if possible, data controllers or processors should not process raw data. If it is necessary, raw data should be kept only as long as they are required to elaborate the aggregated data and to check the validity of that aggregation process. Aggregated data should be kept as long as it is necessary for the provision of the service or otherwise requested by a Union or Member State law.

3.1.1.4 Information and rights of data subjects

114. Prior to the processing of personal data, the data subject shall be informed according to art. 13 GDPR, in a transparent and understandable way. In particular, he or she must be informed of the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period. In this last case, the EDPB recommends to adopt a pedagogic approach to emphasize the difference between raw data and the score produced on this basis, stressing, when it is the case, that the insurer will only collect the result of the score where appropriate.
115. Where data are not processed inside the vehicle but by a telematics provider on behalf of the controller (the insurance company), the information could usefully mention that, in this case, the provider will not have access to data directly relating to the identity of the driver (such as names, licence plates, etc.). Also, considering the importance of informing data subjects as to the consequences of processing of their personal data and the fact that data subjects should not be taken by surprise by the processing of their personal data, the EDPB recommends that data subject should be informed of the existence of profiling and the consequences of such profiling even if it does not involve any automated decision-making as referred to in art. 22 GDPR.

116. Regarding the right of data subjects, they shall be specifically informed of the available means to exercise his or her right of access, rectification, restriction and erasure. Since raw data collected in this context are provided by the data subject (through specific forms or through his or her activity) and processed on the basis of art. 6(1)(b) GDPR (performance of a contract), the data subject is entitled to exercise his or her right to data portability. As emphasized in the guidelines on the right to data portability, the EDPB strongly recommends “that data controllers clearly explain the difference between the types of data that a data subject can receive through the rights of subject access and data portability”.⁴⁸
117. The information can be provided when the contract is signed.

3.1.1.5 Recipient:

118. The EDPB recommends that, as far as possible, the vehicle’s usage data should be processed directly in telematics boxes, so that the insurer only accesses the results data (e.g. a score), not detailed raw data.
119. If a telematics service provider collects the data on behalf of the controller (the insurance company) to generate numerical scores, it does not need to know the identity of the driver (such as names, licence plates, etc.) of the policy holders.

3.1.1.6 Security:

120. General recommendations apply. See section 2.7.

3.1.2 Renting and booking a parking space

121. The owner of a parking place may want to rent it. For this, he/she lists a spot and sets a price for it on a web application. Then, once the parking spot is listed, the application notifies the owner when a driver wants to book it. The driver can select a destination and check for available parking spots based on multiple criteria. After the approval of the owner, the transaction is confirmed and the service provider handles the payment transaction then uses navigation to drive to the location.

3.1.2.1 Legal basis

122. When the data is collected through a publicly available electronic communication, art. 5(3) of the ePrivacy directive applies.
123. Because this is an information society service, art. 5(3) of the ePrivacy directive does not require consent for gaining access to information that is already stored in the vehicle when such a service is explicitly requested by the subscriber.
124. For the processing of personal data and only for data necessary for the performance of the contract to which the data subject is party, art. 6(1)(b) GDPR will be the legal basis.

3.1.2.2 Data collected

125. Data processed includes the driver contact details (name, email, telephone number, vehicle type (e.g. car, truck, motorcycle), license plate number, parking period, payment details (e.g. credit card info) as well as navigation data.

⁴⁸ Article 29 Working Party, Guidelines on the right to data portability under Regulation 2016/676, WP242 rev.01, endorsed by EDPB, p. 13.

3.1.2.3 Retention period

126. Data should be retained only as long as it is necessary to fulfil the parking contract or otherwise as provided by Union or Member State law. After that data is either anonymised or deleted.

3.1.2.4 Information and rights of data subjects

127. Prior to the processing of personal data, the data subject should be informed according to art. 13 GDPR, in a transparent and understandable way.
128. The data subject should be specifically informed of the available means to exercise his or her right of access, rectification, restriction and erasure. Since the data collected in this context are provided by the data subject (through specific forms or through his or her activity) and processed on the basis of art. 6(1)(b) GDPR (performance of a contract), the data subject is entitled to exercise his or her right to data portability. As emphasized in the guidelines on the right to data portability, the EDPB strongly recommends *“that data controllers clearly explain the difference between the types of data that a data subject can receive through the rights of subject access and data portability”*.

3.1.2.5 Recipient:

129. In principle, only the data controller and the data processor have access to the data.

3.1.2.6 Security:

130. General recommendations apply. See section 2.7.

3.2 eCall

131. In the event of a serious accident in the European Union, the vehicle automatically triggers an eCall to 112, the EU-wide emergency number (see section 1.1 for further details) which allows an ambulance to be sent the place of the accident promptly according to Regulation (EU) 2015/758 of 29 April 2015 concerning type-approval requirements for the deployment of the eCall in-vehicle system based on the 112 service, and amending Directive 2007/46/EC (hereinafter - “Regulation (EU) 2015/758”).
132. Indeed, the eCall generator installed inside the vehicle, which enables transmission via a public mobile wireless communications network initiates an emergency call, which is either triggered automatically by vehicle sensors or manually by the vehicle occupants only in the event of an accident. In addition to activation of the audio channel, the second event triggered automatically as a result of an accident consists in generating the Minimum Set of Data (MSD) and sending it to the public safety answering point (PSAP).

3.2.1 Legal basis

133. Regarding the application of the ePrivacy directive, two provisions have to be considered:
 - art. 9 regarding location data other than traffic data which only applies to electronic communication services;
 - art. 5(3) for the gaining access to information stored in the generator installed inside the vehicle.
134. Despite the fact that, in principle, those provisions require the consent of the data subject, Regulation (EU) 2015/758 constitutes a legal obligation to which the data controller is subject (the data subject has no genuine or free choice and will be unable to refuse the

processing of his/her data). Hence, Regulation (EU) 2015/758 overrides the need of the driver's consent for the processing of location data and the MSD.⁴⁹

135. The legal basis of the processing of those data will be compliance with a legal obligation as provided for in art. 6(1)(c) GDPR (i.e., Regulation (EU) 2015/758).

3.2.2 Data collected

136. Regulation (EU) 2015/578 provides that data sent by the 112-based eCall in-vehicle system shall include only the minimum information as referred to in the standard EN 15722:2015 'Intelligent transport systems — eSafety — eCall minimum set of data (MSD)' including:

- the indication if eCall has been manually or automatically triggered;
- the vehicle type;
- the vehicle identification number (VIN);
- the propulsion type of the vehicle;
- the timestamp of the initial data message generation within the current eCall incident event;
- the last known vehicle latitude and longitude position determined at the latest moment possible before message generation;
- the vehicle's last known real direction of travel determined at the latest moment possible before message generation (only the last three locations of the vehicle).

3.2.3 Retention period

137. Regulation (EU) 2015/758 stipulates that data shall not be retained for longer than is needed for processing emergency situations. Those data shall be completely deleted when they are no longer needed for that purpose. Furthermore, in the internal memory of the eCall system, data shall be automatically and constantly deleted. Only the vehicle's last three positions can be stored, insofar as it is strictly necessary to specify the current position of the vehicle and the direction of travel at the time of the event.

3.2.4 Information and rights of data subjects

138. Art. 6 of the Regulation (EU) 2015/758 stipulates that manufacturers shall provide clear and complete information on data processing done using the eCall system. This information shall be provided in the owner's manual separately for the 112-based eCall in-vehicle system and any third-party service supported eCall systems prior to the use of the system. It includes:

- the reference to the legal basis for the processing;
 - the fact that the 112-based eCall in-vehicle system is activated by default;
 - the arrangements for data processing that the 112-based eCall in-vehicle system
-
- performs;

⁴⁹ It has to be noted that Article 8-1-f of the Council negotiation mandate for the proposal for an "ePrivacy" regulation does provide a specific exemption for eCall as consent is not needed when *"it is necessary to locate terminal equipment when an end-user makes an emergency communication either to the single European emergency number '112' or a national emergency number, in accordance with Article 13(3)."*

- the specific purpose of the eCall processing, which shall be limited to the emergency situations referred to in the first subparagraph of Art. 5(2) Regulation (EU) 2015/758;
 - the types of data collected and processed and the recipients of that data;
 - the time limit for the retention of data in the 112-based eCall in-vehicle system;
 - the fact that there is no constant tracking of the vehicle;
 - the arrangements for exercising data subjects' rights as well as the contact service responsible for handling access requests;
 - any necessary additional information regarding traceability, tracking and processing of personal data in relation to the provision of a third-party service (TPS) eCall and/or other added value services, which shall be subject to explicit consent by the owner and in compliance with the GDPR. Particular account shall be taken of the fact that differences may exist between the data processing carried out through the 112-based eCall in-vehicle system and the TPS eCall in-vehicle systems or other added value services.
139. Furthermore, the service provider shall also provide the data subjects with information in accordance with art. 13 GDPR in a transparent and understandable way. In particular, he or she must be informed of the purposes of the processing for which the personal data are intended as well as the fact that the processing of personal data is based on a legal obligation to which the controller is subject.
140. In addition, taking into account the nature of the processing, the information about the recipients or categories of recipients of the personal data should be clear and the data subjects should be informed that the data are not be available outside the 112-based eCall in-vehicle system to any entities before the eCall is triggered.
141. Regarding rights of data subjects, it has to be noted that since the processing is based on a legal obligation, the right to object and the right to portability will not apply.

3.2.5 Recipient:

142. The data shall not be available outside the 112-based eCall in-vehicle system to any entities before the eCall is triggered.
143. When it is triggered (either manually by vehicle occupants or automatically as soon as an in-vehicle sensor detects a serious collision), the eCall system establishes a voice connection with the relevant PSAP and the MSD is sent to the PSAP operator.
144. Furthermore, data transmitted via the 112-based eCall in-vehicle system and processed by the PSAPs can be transferred to the emergency service and service partners referred to in Decision No 585/2014/EU only in the event of incidents related to eCalls and under the conditions set out in that Decision and are used exclusively for the attainment of the objectives of that Decision. Data processed by the PSAPs through the 112-based eCall in-vehicle system are not transferred to any other third parties without the explicit prior consent of the data subject.

3.2.6 Security

145. Regulation (EU) 2015/758 stipulates the requirements to incorporate into the eCall system technologies that strengthen the protection of privacy, in order to offer users the appropriate level of protection of privacy, as well as the guarantees needed to prevent

surveillance and abusive uses. In addition, manufacturers should ensure that the eCall system based on the number 112, as well as any other system providing an eCall that is handled by third-party services or an added-value service, are so designed that it is impossible for personal data to be exchanged between those systems.

146. Regarding PSAPs, Member States should ensure that personal data are protected against misuse, including unlawful access, alteration or loss, and that protocols concerning personal data storage, retention duration, processing and protection are established at the appropriate level and properly observed.

3.3 Accidentology studies

147. Data subjects may voluntarily agree to take part in accidentology studies aimed at better understanding the causes of road accidents and more generally scientific purposes.

3.3.1 Legal basis

148. When the data are collected through a public electronic communication service, the data controller will have to collect the consent of the data subject for the gaining of access to information that is already stored in the vehicle as provided by art. 5(3) of the ePrivacy directive. Indeed, none of the exemptions provided by those provisions can apply in this context: the processing is not for the sole purpose of carrying out the transmission of a communication over an electronic communications network nor does it relate to an information society service explicitly requested by the subscriber or user.
149. Regarding the processing of personal data and taking into account the variety and amount of personal data needed for accidentology studies, the EDPB recommends the processing to be based on the prior consent of the data subject according to art. 6 GDPR. Such prior consent must be provided on a specific form, through which the data subject volunteers to take part to the study and have his or her personal data processed for that purpose. Consent shall be an expression of the free, specific, and informed will of the person whose data are being processed (e.g., ticking a box that is not pre-ticked, or configuring the onboard computer to activate a function in the vehicle). Such consent must be provided separately, for specific purposes, may not be bundled with the contract to buy or lease a new car and the consent must be as easily withdrawn as it is given. Withdrawal of consent shall lead to the processing being stopped. The data shall then be deleted from the active database, or anonymised.
150. Consent required by art. 5(3) of the ePrivacy directive and consent needed as a legal basis for the processing of data can be collected at the same time (for example by checking a box clearly indicating what the data subject is consenting to).
151. It has to be noted that, depending on the conditions of the processing (nature of the data controller, etc.), another legal basis can be lawfully chosen as long as it does not lower the additional protection provided by art. 5(3) ePrivacy directive (see paragraph 15). If the processing is based on another legal basis such as the performance of a task carried out in the public interest (art. 6(1)(e) GDPR), the EDPB recommends that the data subjects are included in the study on a voluntary basis.

3.3.2 Data collected

152. The data controller shall only collect personal data that are strictly necessary for the processing.

153. There are two types of data to be considered:

- **data relating to participants and vehicles;**
- **technical data from vehicles** (instantaneous speed, etc.).

154. Scientific research linked to accidentology justifies the collection of the instantaneous speed, including by legal persons who do not administer a public service in the strict sense.

155. Indeed, as noted above, the EDPB considers that instantaneous speed collected in the context of an accidentology study is not offence-related data by destination (i.e., it is not being collected for the purpose of investigating or prosecuting an offence), which justifies its collection by legal persons who do not administer a public service in the strict sense.

3.3.3 Retention period

156. It is important to distinguish between two types of data. First, the data relating to participants and vehicles can be retained for the duration of the study. Second, the technical data from vehicles should be retained for as short as possible for the purpose. In this regard, five years from the end date of the study appears to be a reasonable period. At the end of that period, the data shall be deleted or anonymised.

3.3.4 Information and rights of data subjects

157. Prior to the processing of personal data, the data subject shall be informed according to art. 13 GDPR, in a transparent and understandable way. In particular, in the case of collecting instantaneous speed, the data subjects should be specifically informed of the data collection. Since the data processing is based on consent, the data subject must be specifically informed of the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal. Moreover, because the data collected in this context are provided by the data subject (through specific forms or through his or her activity) and processed on the basis of art. 6(1)(a) GDPR (consent), the data subject is entitled to exercise his or her right to data portability. As emphasized in the guidelines on the right to data portability, the EDPB strongly recommends “that data controllers clearly explain the difference between the types of data that a data subject can receive through the rights of subject access and data portability”. Consequently, the data controller should provide an easy way to withdraw his consent, freely and at any time, as well as develop tools to be able to answer data portability requests.

158. That information can be given upon signing the form to agree to take part in the accidentology study.

3.3.5 Recipient

159. In principle, only the data controller and the data processor have access to the data.

3.3.6 Security

160. As noted above, the security measures put in place shall be adapted to the level of data sensitivity. For instance, if instantaneous speed (or any other data related to criminal convictions and offences) is collected as part of the accidentology study, the EDPB strongly recommends putting in place strong security measures, such as:

- implementing pseudonymisation measures (e.g., secret-key hashing of data like the surname/first name of the data subject and the serial number);

- storing data relating to instantaneous speed and to location in separate databases (e.g., using a state-of-the-art encryption mechanism with distinct keys and approval mechanisms);
- and/or deleting location data as soon as the reference event or sequence is qualified (e.g., the type of road, day/night), and the storage of directly-identifying data in a separate database that can only be accessed by a small number of people.

3.4 Tackle auto theft

161. Data subjects may wish, in the case of theft, to attempt to find their vehicle using location. Using location data is limited to the strict needs of the investigation and to the case assessment by the competent legal authorities.

3.4.1 Legal basis

162. When the data is collected through a publicly available electronic communication service, art. 5(3) of the ePrivacy directive applies.
163. Because this is an information society service, art. 5(3) of the ePrivacy directive does not require consent for gaining access to information that is already stored in the vehicle when such a service is explicitly requested by the subscriber.
164. Regarding the processing of personal data, the legal basis for processing the location data will be the consent of the vehicle's owner, or, if applicable, the performance of a contract (only for data necessary for the performance of the contract to which the vehicle's owner is party).
165. Consent shall be an expression of the free, specific, and informed will of the person whose data are being processed (e.g. ticking a box that is not pre-ticked, or configuring the on-board computer to activate a function in the vehicle). Freedom to give consent involves the option of withdrawing consent at any time, of which the data subject should be expressly informed. Withdrawal of consent shall lead to the processing being stopped. The data should then be deleted from the active database, anonymised, or archived.

3.4.2 Data collected

166. Location data can only be transmitted as of the declaration of theft, and cannot be collected continuously the rest of the time.

3.4.3 Retention period

167. Location data can only be retained for the period during which the case is assessed by the competent legal authorities, or until the end of a procedure to dispel doubt that does not end with confirmation of the theft of the vehicle.

3.4.4 Information of the data subjects

168. Prior to the processing of personal data, the data subject should be informed according to art. 13 GDPR, in a transparent and understandable way. More specifically, the EDPB recommends that the data controller emphasizes that there is no constant tracking of the vehicle and that location data can only be collected and transmitted as of the declaration of theft. Moreover, the controller must provide the data subject with information relating to the fact that only approved officers of the remote-surveillance platform and legally approved authorities have access to the data.
169. Regarding the rights of the data subjects, when the data processing is based on consent, the data subject should be specifically informed of the existence of the right to withdraw

consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal. Besides, when the data collected in this context are provided by them (through specific forms or through his or her activity) and processed on the basis of art. 6(1)(a) (consent) or art. 6(1)(b) GDPR (performance of a contract), the data subject is entitled to exercise his or her right to data portability. As emphasized in the guidelines on the right to data portability, the EDPB strongly recommends “that data controllers clearly explain the difference between the types of data that a data subject can receive through the rights of subject access and data portability”.

170. Consequently, the data controller should provide an easy way to withdraw his consent (only when consent is the legal basis), freely and at any time, as well as develop tools to be able to answer data portability requests.

171. The information can be provided when the contract is signed.

3.4.5 Recipients

172. In the event of a theft declaration, location data can be passed on the (i) approved officers of the remote-surveillance platform, and (ii) to the legally approved authorities.

3.4.6 Security

173. General recommendations apply. See section 2.7

AUTOMATED DRIVING SYSTEMS

A Vision for Safety



U.S. Department of Transportation

Adopted

36



INTRODUCTORY MESSAGE

Today, our country is on the verge of one of the most exciting and important innovations in transportation history—the development of Automated Driving Systems (ADSs), commonly referred to as automated or self-driving vehicles.

The future of this new technology is so full of promise. It's a future where vehicles increasingly help drivers avoid crashes. It's a future where the time spent commuting is dramatically reduced, and where millions more—including the elderly and people with disabilities—gain access to the freedom of the open road. And, especially important, it's a future where highway fatalities and injuries are significantly reduced.

Since the Department of Transportation was established in 1966, there have been more than 2.2 million motor-vehicle-related fatalities in the United States. In addition, after decades of decline, motor vehicle fatalities spiked by more than 7.2 percent in 2015, the largest single-year increase since 1966. The major factor in 94 percent of all fatal crashes is human error. So ADSs have the potential to significantly reduce highway fatalities by addressing the root cause of these tragic crashes.

The U.S. Department of Transportation has a role to play in building and shaping this future by developing a regulatory framework that encourages, rather than hampers, the safe development, testing and deployment of automated vehicle technology.

Accordingly, the Department is releasing *A Vision for Safety* to promote improvements in safety, mobility, and efficiency through ADSs.

A Vision for Safety replaces the Federal Automated Vehicle Policy released in 2016. This updated policy framework offers a path forward for the safe deployment of automated vehicles by:

- Encouraging new entrants and ideas that deliver safer vehicles;
- Making Department regulatory processes more nimble to help match the pace of private sector innovation; and
- Supporting industry innovation and encouraging open communication with the public and with stakeholders.

Thanks to a convergence of technological advances, the promise of safer automated driving systems is closer to becoming a reality. From reducing crash-related deaths and injuries, to improving access to transportation, to reducing traffic congestion and vehicle emissions, automated vehicles hold significant potential to increase productivity and improve the quality of life for millions of people. *A Vision for Safety* seeks to facilitate the integration of ADS technology by helping to ensure its safe testing and deployment, as well as encouraging the development of systems that guard against cyber-attacks and protect consumer privacy.

Our goal at the Department of Transportation is to be good stewards of the future by helping to usher in this new era of transportation innovation and safety, and ensuring that our country remains a global leader in autonomous vehicle technology.



Secretary Elaine L. Chao
U.S. Department of Transportation

EXECUTIVE SUMMARY

The world is facing an unprecedented emergence of automation technologies. In the transportation sector, where 9 out of 10 serious roadway crashes occur due to human behavior, automated vehicle technologies possess the potential to save thousands of lives, as well as reduce congestion, enhance mobility, and improve productivity. The Federal Government wants to ensure it does not impede progress with unnecessary or unintended barriers to innovation. Safety remains the number one priority for the U.S. Department of Transportation (DOT) and is the specific focus of the National Highway Traffic Safety Administration (NHTSA).

NHTSA's mission is to save lives, prevent injuries, and reduce the economic costs of roadway crashes through education, research, safety standards, and enforcement activity. As automated vehicle technologies advance, they have the potential to dramatically reduce the loss of life each day in roadway crashes. To support industry innovators and States in the deployment of this technology, while informing and educating the public, and improving roadway safety through the safe introduction of the technology, NHTSA presents *Automated Driving Systems: A Vision for Safety*. It is an important part of DOT's multimodal efforts to support the safe introduction of automation technologies.

In this document, NHTSA offers a nonregulatory approach to automated vehicle technology safety. *Section 1: Voluntary Guidance for Automated Driving Systems (Voluntary Guidance)* supports the automotive industry and other key stakeholders as they consider and design best practices for the testing and safe deployment of Automated Driving Systems (ADSs - SAE Automation Levels 3 through 5 – Conditional, High, and Full Automation Systems). It contains 12 priority safety design elements for consideration, including vehicle cybersecurity, human machine interface, crashworthiness, consumer education and training, and post-crash ADS behavior.

Given the developing state of the technology, this *Voluntary Guidance* provides a flexible framework for industry to use in choosing how to address a given safety design element. In addition, to help support public trust and confidence, the *Voluntary Guidance* encourages entities engaged in testing and deployment to publicly disclose Voluntary Safety Self-Assessments of their systems in order to demonstrate their varied approaches to achieving safety.

Vehicles operating on public roads are subject to both Federal and State jurisdiction, and States are beginning to draft legislation to safely deploy emerging ADSs. To support the State work, NHTSA offers *Section 2: Technical Assistance to States, Best Practices for Legislatures Regarding Automated Driving Systems (Best Practices)*. The section clarifies and delineates Federal and State roles in the regulation of ADSs. NHTSA remains responsible for regulating the safety design and performance aspects of motor vehicles and motor vehicle equipment; States continue to be responsible for regulating the human driver and vehicle operations.

The section also provides *Best Practices for Legislatures*, which incorporates common safety-related components and significant elements regarding ADSs that States should consider incorporating in legislation. In addition, the section provides *Best Practices for State Highway Safety Officials*, which offers a framework for States to develop procedures and conditions for ADSs' safe operation on public roadways. It includes considerations in such areas as applications and permissions to test, registration and titling, working with public safety officials, and liability and insurance.

Together, the *Voluntary Guidance* and *Best Practices* sections serve to support industry, Government officials, safety advocates, and the public. As our Nation and the world embrace technological advances in motor vehicle transportation through ADSs, safety must remain the top priority.

Over the coming months and years, NHTSA, along with other Federal agencies, where relevant, will continue to take a leadership role in encouraging the safe introduction of automated vehicle technologies into the motor vehicle fleet and on public roadways in the areas of policy, research, safety standards, freight and commercial use, infrastructure, and mass transit.

The **Office of the Under Secretary for Policy (OST-P)** is the office responsible for serving as a principal advisor to the Secretary and provides leadership in the development of policies for the Department, generating proposals and providing advice regarding legislative and regulatory initiatives across all modes of transportation. The Under Secretary coordinates the Department's budget development and policy development functions. The Under Secretary also directs transportation policy development and works to ensure that the Nation's transportation resources function as an integrated national system. See www.transportation.gov/policy.

The **Office of the Assistant Secretary for Research and Technology (OST-R)** is the lead office responsible for coordinating DOT's research and for sharing advanced technologies with the transportation system. Technical and policy research on these technologies occurs through the Intelligent Transportation Systems (ITS) Research Program, the University Transportation Centers, and the Volpe National Transportation Research Center, which make investments in technology initiatives, exploratory studies, pilot deployment programs and evaluations in intelligent vehicles, infrastructure, and multi-modal systems. See www.its.dot.gov and www.transportation.gov/research-technology.

The **Federal Motor Carrier Safety Administration (FMCSA)** is the lead Federal Government agency responsible for regulating and providing operational safety oversight (for instance, hours of service regulations, drug and alcohol testing, hazardous materials safety, vehicle inspections) for motor carriers operating commercial motor vehicles (CMVs), such as trucks and buses, and CMV drivers. FMCSA partners with industry, safety advocates, and State and local governments to keep our Nation's roadways safe and improve CMV safety through financial assistance, regulation, education, enforcement, research, and technology. See www.fmcsa.dot.gov.

The **Federal Highway Administration (FHWA)** supports State and local governments in the design, construction, and maintenance of the Nation's highway system (Federal Aid Highway Program) and various Federal and tribal lands (Federal Lands Highway Program). Through financial and technical assistance to State and local governments, FHWA is responsible for ensuring that America's roads and highways continue to be among the safest and most technologically sound in the world. See www.fhwa.dot.gov.

The **Federal Transit Administration (FTA)** provides financial and technical assistance to local public transit systems, including buses, subways, light rail, commuter rail, trolleys, and ferries. FTA also oversees safety measures and helps develop next-generation technology research. See www.transit.dot.gov.

TABLE OF CONTENTS

Section 1: Voluntary Guidance

Overview	1
Scope and Purpose.....	2
ADS Safety Elements.....	5
System Safety.....	5
Operational Design Domain	6
Object and Event Detection and Response	7
Fallback (Minimal Risk Condition)	8
Validation Methods.....	9
Human Machine Interface.....	10
Vehicle Cybersecurity	11
Crashworthiness	12
Post-Crash ADS Behavior	13
Data Recording	14
Consumer Education and Training	15
Federal, State, and Local Laws.....	15
Voluntary Safety Self-Assessment	16

Section 2: Technical Assistance to States

Overview	19
Federal and State Regulatory Roles.....	20
Best Practices for Legislatures.....	21
Best Practices for State Highway Safety Officials	22
Conclusion.....	25
Endnotes.....	26

SECTION 1: VOLUNTARY GUIDANCE

For Automated Driving Systems

OVERVIEW

The U.S. Department of Transportation (DOT) through the National Highway Traffic Safety Administration (NHTSA) is fully committed to reaching an era of crash-free roadways through deployment of innovative lifesaving technologies. Recent negative trends in automotive crashes underscore the urgency to develop and deploy lifesaving technologies that can dramatically decrease the number of fatalities and injuries on our Nation's roadways. NHTSA believes that Automated Driving Systems (ADSs), including those contemplating no driver at all, have the potential to significantly improve roadway safety in the United States.

The purpose of this Voluntary Guidance is to support the automotive industry, the States, and other key stakeholders as they consider and design best practices relative to the testing and deployment of automated vehicle technologies. It updates the Federal Automated Vehicles Policy released in September 2016 and serves as NHTSA's current operating guidance for ADSs.

The Voluntary Guidance contains 12 priority safety design elements.¹ These elements were selected based on research conducted by the Transportation Research Board (TRB), universities, and NHTSA. Each element contains safety goals and approaches that could be used to achieve those safety goals. Entities are encouraged to consider each safety element in the design of their systems and have a self-documented process for assessment, testing, and validation of the various elements. As automated driving technologies evolve at a rapid pace, no single standard exists by which an entity's methods of considering a safety design element can be measured. Each entity is free to be creative and innovative when developing the best method for its system to appropriately mitigate the safety risks associated with their approach.

In addition, to help support public trust and confidence in the safety of ADSs, this Voluntary Guidance encourages entities to disclose Voluntary Safety Self-Assessments demonstrating their varied approaches to achieving safety in the testing and deployment of ADSs.²

Entities are encouraged to begin using this Voluntary Guidance on the date of its publication. NHTSA plans to regularly update the Voluntary Guidance to reflect lessons learned, new data, and stakeholder input as technology continues to be developed and refined.

For overall awareness and to ensure consistency in taxonomy usage, NHTSA adopted SAE International's Levels of Automation and other applicable terminology.³

NHTSA'S MISSION

Save lives, prevent injuries, and reduce economic costs due to road traffic crashes, through education, research, safety standards, and enforcement activity.

SCOPE AND PURPOSE

Through this Voluntary Guidance, NHTSA is supporting entities that are designing ADSs for use on public roadways in the United States. This includes traditional vehicle manufacturers as well as other entities involved with manufacturing, designing, supplying, testing, selling, operating, or deploying ADSs, including equipment designers and suppliers; entities that outfit any vehicle with automated capabilities or equipment for testing, for commercial sale, and/or for use on public roadways; transit companies; automated fleet operators; “driverless” taxi companies; and any other individual or entity that offers services utilizing ADS technology (referred to collectively as “entities” or “industry”).

This Voluntary Guidance applies to the design aspects of motor vehicles and motor vehicle equipment under NHTSA’s jurisdiction, including low-speed vehicles, motorcycles, passenger vehicles, medium-duty vehicles, and heavy-duty CMVs such as large trucks and buses. These entities are subject to NHTSA’s defect, recall, and enforcement authority.⁴ For entities seeking to request regulatory action (e.g., petition for exemption or interpretation) from NHTSA, an informational resource is available on the Agency’s website at www.nhtsa.gov/technology-innovation/automated-vehicles, along with other associated references and resources.

Interstate motor carrier operations and CMV drivers fall under the jurisdiction of FMCSA and are not within the scope of this Voluntary Guidance. Currently, per the Federal Motor Carrier Safety Regulations (FMCSRs), a trained commercial driver must be behind the wheel at all times, regardless of any automated driving technologies available on the CMV, unless a petition for a waiver or exemption has been granted. For more information regarding CMV operations and automated driving technologies, including guidance on FMCSA’s petition process, see www.fmcsa.dot.gov.

This Voluntary Guidance focuses on vehicles that incorporate SAE Automation Levels 3 through 5 – Automated Driving Systems (ADSs). ADSs may include systems for which there is no human driver or for which the human driver can give control to the ADS and would not be expected to perform any driving-related tasks for a period of time.⁵ It is an entity’s responsibility to determine its system’s automation level in conformity with SAE International’s published definitions.

The purpose of this Voluntary Guidance is to help designers of ADSs analyze, identify, and resolve safety considerations prior to deployment using their own, industry, and other best practices. It outlines 12 safety elements, which the Agency believes represent the consensus across the industry, that are generally considered to be the most salient design aspects to consider and address when developing, testing, and deploying ADSs on public roadways. Within each safety design element, entities are encouraged to consider and document their use of industry standards, best practices, company policies, or other methods they have employed to provide for increased system safety in real-world conditions. The 12 safety design elements apply to both ADS original equipment and to replacement equipment or updates (including software updates/upgrades) to ADSs.

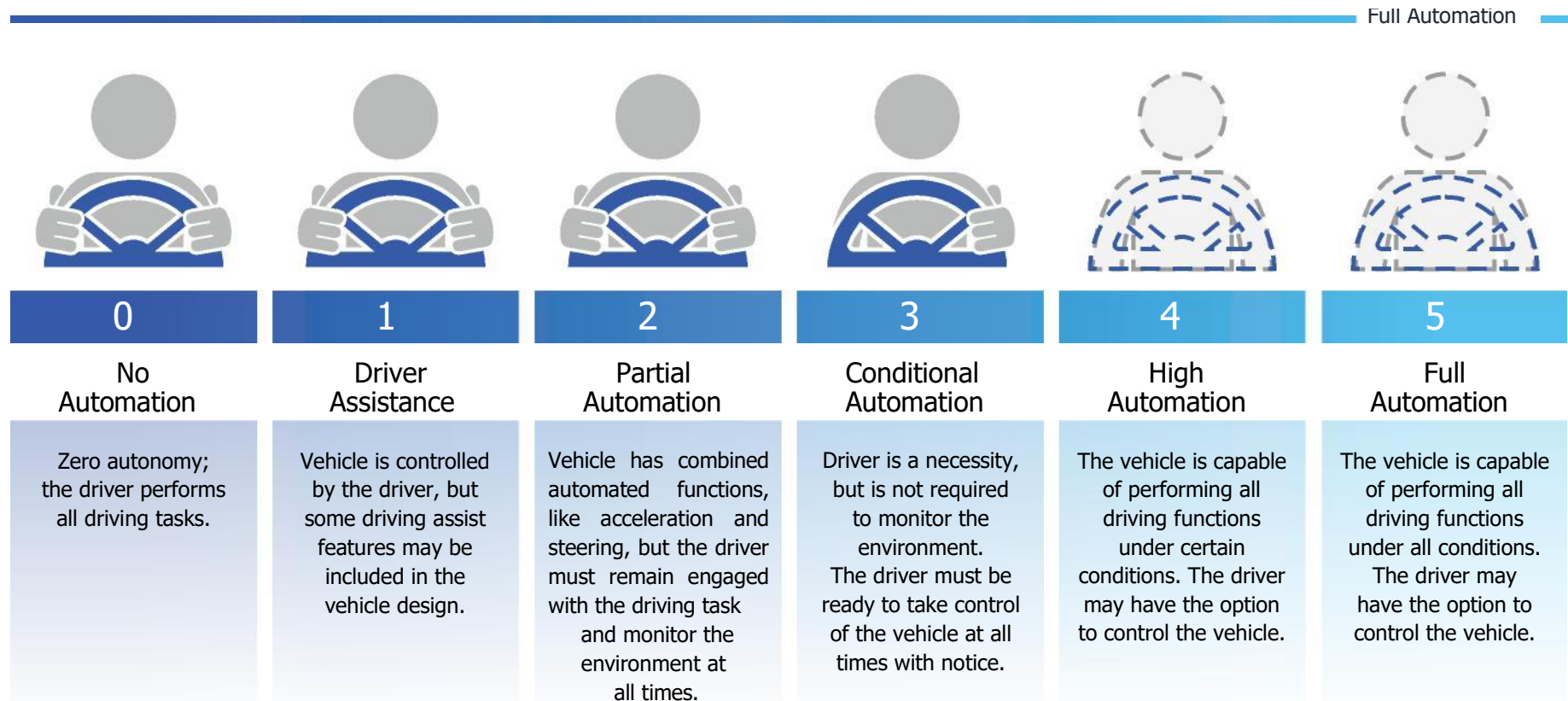
This Voluntary Guidance provides recommendations and suggestions for industry’s consideration and discussion. This Guidance is entirely voluntary, with no compliance requirement or enforcement mechanism. The sole purpose of this Guidance is to support the industry as it develops best practices in the design, development, testing, and deployment of automated vehicle technologies.

NHTSA'S ENFORCEMENT AUTHORITY

Several States have sought clarification of NHTSA's enforcement authority with respect to ADSs. As DOT is asking States to maintain the delineation of Federal and State regulatory authority, NHTSA understands that States are looking for reassurance that the Federal Government has tools to keep their roadways safe.

NHTSA has broad enforcement authority to address existing and new automotive technologies and equipment. The Agency is commanded by Congress⁵ to protect the safety of the driving public against unreasonable risks of harm that may arise because of the design, construction, or performance of a motor vehicle or motor vehicle equipment, and to mitigate risks of harm, including risks that may arise in connection with ADSs. Specifically, NHTSA's enforcement authority concerning safety-related defects in motor vehicles and motor vehicle equipment extends and applies equally to current and emerging ADSs. As NHTSA has always done, when evaluating new automotive technologies, it will be guided by its statutory mission, the laws it is obligated to enforce, and the benefits

SAE AUTOMATION LEVELS



ADS SAFETY ELEMENTS

1. System Safety

Entities are encouraged to follow a robust design and validation process based on a systems-engineering approach with the goal of designing ADSs free of unreasonable safety risks. The overall process should adopt and follow industry standards, such as the functional safety⁷ process standard for road vehicles, and collectively cover the entire operational design domain (i.e., operating parameters and limitations) of the system. Entities are encouraged to adopt voluntary guidance, best practices, design principles, and standards developed by established and accredited standards-developing organizations (as applicable) such as the International Standards Organization (ISO) and SAE International, as well as standards and processes available from other industries such as aviation, space, and the military⁸ and other applicable standards or internal company processes as they are relevant and applicable. See NHTSA's June 2016 report, *Assessment of Safety Standards for Automotive Electronic Control Systems*⁹, which provides an evaluation of the strengths and limitations of such standards.

The design and validation process should also consider including a hazard analysis and safety risk assessment for ADSs, for the overall vehicle design into which it is being integrated, and when applicable, for the broader transportation ecosystem. Additionally, the process shall describe design redundancies and safety strategies for handling ADS malfunctions. Ideally, the process should place significant emphasis on software development, verification, and validation. The software development process is one that should be well-planned, well-controlled, and well-documented to detect and correct unexpected results from software updates. Thorough and measurable software testing should complement a structured and documented software development and change management process and should be part of each software version release. Industry is encouraged to monitor the evolution, implementation,

and safety assessment of artificial intelligence and other relevant software technologies and algorithms to improve the effectiveness and safety of ADSs.

Design decisions should be linked to the assessed risks that could impact safety-critical system functionality. Design safety considerations should include design architecture, sensors, actuators, communication failure, potential software errors, reliability, potential inadequate control, undesirable control actions, potential collisions with environmental objects and other road users, potential collisions that could be caused by actions of an ADS, leaving the roadway, loss of traction or stability, and violation of traffic laws and deviations from normal (expected) driving practices.

All design decisions should be tested, validated, and verified as individual subsystems and as part of the entire vehicle architecture. Entities are encouraged to document the entire process; all actions, changes, design choices, analyses, associated testing, and data should be traceable and transparent.



2. Operational Design Domain

Entities are encouraged to define and document the Operational Design Domain (ODD) for each ADS available on their vehicle(s) as tested or deployed for use on public roadways, as well as document the process and procedure for assessment, testing, and validation of ADS functionality with the prescribed ODD. The ODD should describe the specific conditions under which a given ADS or feature is intended to function. The ODD is the definition of where (such as what roadway types and speeds) and when (under what conditions, such as day/night, weather limits, etc.) an ADS is designed to operate.



The ODD would include the following information at a minimum to define each ADS's capability limits/boundaries:

- Roadway types (interstate, local, etc.) on which the ADS is intended to operate safely;
- Geographic area (city, mountain, desert, etc.);
- Speed range;
- Environmental conditions in which the ADS will operate (weather, daytime/nighttime, etc.); and
- Other domain constraints.

An ADS should be able to operate safely within the ODD for which it is designed. In situations where the ADS is outside of its defined ODD or in which conditions dynamically change to fall outside of the ADS's ODD, the vehicle should transition to a minimal risk condition.¹⁰ For a Level 3 ADS, transitioning to a minimal risk condition could entail transitioning control to a receptive, fallback-ready user.¹¹ In cases the ADS does not have indications that the user is receptive and fallback-ready, the system should continue to mitigate manageable risks, which may include slowing the vehicle down or bringing the vehicle to a safe stop. To support the safe introduction of ADSs on public roadways and to speed deployment, the ODD concept provides the flexibility for entities to initially limit the complexity of broader driving challenges in a confined ODD.

3. Object and Event Detection and Response

Object and Event Detection and Response (OEDR)¹² refers to the detection by the driver or ADS of any circumstance that is relevant to the immediate driving task, as well as the implementation of the appropriate driver or system response to such circumstance. For the purposes of this Guidance, an ADS is responsible for performing OEDR while it is engaged and operating in its defined ODD.

Entities are encouraged to have a documented process for assessment, testing, and validation of their ADS's OEDR capabilities. When operating within its ODD, an ADS's OEDR functions are expected to be able to detect and respond to other vehicles (in and out of its travel path), pedestrians, bicyclists, animals, and objects that could affect safe operation of the vehicle.

An ADS's OEDR should also include the ability to address a wide variety of foreseeable encounters, including emergency vehicles, temporary work zones, and other unusual conditions (e.g., police manually directing traffic or other first responders or construction workers controlling traffic) that may impact the safe operation of an ADS.

Normal Driving

Entities are encouraged to have a documented process for the assessment, testing, and validation of a variety of behavioral competencies for their ADSs. Behavioral competency refers to

the ability of an ADS to operate in the traffic conditions that it will regularly encounter, including keeping the vehicle in a lane, obeying traffic laws, following reasonable road etiquette, and responding to other vehicles or hazards.¹³ While research conducted by California PATH¹⁴ provided a set of minimum behavioral competencies for ADSs,¹⁵ the full complement of behavioral competencies a particular ADS would be expected to demonstrate and routinely perform will depend upon the individual ADS, its ODD, and the designated fallback (minimal risk condition) method. Entities are encouraged to consider all known behavioral competencies in the design, test, and validation of their ADSs.

Crash Avoidance Capability – Hazards

Entities are encouraged to have a documented process for assessment, testing, and validation of their crash avoidance capabilities and design choices. Based on the ODD, an ADS should be able to address applicable pre-crash scenarios¹⁶ that relate to control loss; crossing-path crashes; lane change/merge; head-on and opposite-direction travel; and rear-end, road departure, and low-speed situations such as backing and parking maneuvers.¹⁷ Depending on the ODD, an ADS may be expected to handle many of the pre-crash scenarios that NHTSA has identified previously.¹⁸

The Federal Government wants to ensure it does not impede progress with unnecessary or unintended barriers to innovation. Safety remains the number one priority for U.S. DOT and is the specific focus of NHTSA.

4. Fallback (Minimal Risk Condition)

Entities are encouraged to have a documented process for transitioning to a minimal risk condition when a problem is encountered or the ADS cannot operate safely. ADSs operating on the road should be capable of detecting that the ADS has malfunctioned, is operating in a degraded state, or is operating outside of the ODD. Furthermore, ADSs should be able to notify the human driver of such events in a way that enables the driver to regain proper control of the vehicle or allows the ADS to return to a minimal risk condition independently.

Fallback strategies should take into account that, despite laws and regulations to the contrary, human drivers may be inattentive, under the influence of alcohol or other substances, drowsy, or otherwise impaired.

Fallback actions are encouraged to be administered in a manner that will facilitate safe operation of the vehicle and minimize erratic driving behavior. Such fallback actions should also consider minimizing the effects of errors in human driver recognition and decision-making during and after transition to manual control.

In cases of higher automation in which a human driver may not be available, the ADS must be able to fallback into a minimal risk condition without the need for driver intervention.

A minimal risk condition will vary according to the type and extent of a given failure, but may include automatically bringing the vehicle to a safe stop, preferably outside of an active lane of traffic. Entities are encouraged to have a documented process for assessment, testing, and validation of their fallback approaches.

The purpose of this Voluntary Guidance is to help designers of ADSs analyze, identify, and resolve safety considerations prior to deployment using their own, industry, and other best practices. It outlines 12 safety elements, which the Agency believes represent the consensus across the industry, that are generally considered to be the most salient design aspects to consider and address when developing, testing, and deploying ADSs on public roadways.

5. Validation Methods

Given that the scope, technology, and capabilities vary widely for different automation functions, entities are encouraged to develop validation methods to appropriately mitigate the safety risks associated with their ADS approach. Tests should demonstrate the behavioral competencies an ADS would be expected to perform during normal operation, the ADS's performance during crash avoidance situations, and the performance of fallback strategies relevant to the ADS's ODD.

To demonstrate the expected performance of an ADS for deployment on public roads, test approaches may include a combination of simulation, test track, and on-road testing.

Prior to on-road testing, entities are encouraged to consider the extent to which simulation and track testing may be necessary. Testing may be performed by the entities themselves, but could also be performed by an independent third party.

Entities should continue working with NHTSA and industry standards organizations (SAE, International Organization for Standards [ISO], etc.) and others to develop and update tests that use innovative methods as well as to develop performance criteria for test facilities that intend to conduct validation tests.



6. Human Machine Interface

Understanding the interaction between the vehicle and the driver, commonly referred to as “human machine interface” (HMI), has always played an important role in the automotive design process. New complexity is introduced to this interaction as ADSs take on driving functions, in part because in some cases the vehicle must be capable of accurately conveying information to the human driver regarding intentions and vehicle performance. This is particularly true for ADSs in which human drivers may be requested to perform any part of the driving task. For example, in a Level 3 vehicle, the driver always must be receptive to a request by the system to take back driving responsibilities. However, a driver’s ability to do so is limited by their capacity to stay alert to the driving task and thus capable of quickly taking over control, while at the same time not performing the actual driving task until prompted by the vehicle. Entities are encouraged to consider whether it is reasonable and appropriate to incorporate driver engagement monitoring in cases where drivers could be involved in the driving task so as to assess driver awareness and readiness to perform the full driving task.

Entities are also encouraged to consider and document a process for the assessment, testing, and validation of the vehicle’s HMI design. Considerations should be made for the human driver, operator, occupant(s), and external actors with whom the ADS may have interactions, including other vehicles (both traditional and those with

ADSs), motorcyclists, bicyclists, and pedestrians. HMI design should also consider the need to communicate information regarding the ADS’s state of operation relevant to the various interactions it may encounter and how this information should be communicated.

In vehicles that are anticipated not to have driver controls, entities are encouraged to design their HMI to accommodate people with disabilities (e.g., through visual, auditory, and haptic displays).¹⁹

In vehicles where an ADS may be intended to operate without a human driver or even any human occupant, the remote dispatcher or central control authority, if such an entity exists, should be able to know the status of the ADS at all times. Examples of these may include unoccupied SAE Automation Level 4 or 5 vehicles, automated delivery vehicles, last-mile special purpose ground drones, and automated maintenance vehicles.

Given the ongoing research and rapidly evolving nature of this field, entities are encouraged to consider and apply voluntary guidance, best practices, and design principles published by SAE International, ISO, NHTSA, the American National Standards Institute (ANSI), the International Commission on Illumination (CIE), and other relevant organizations, based upon the level of automation and expected level of driver engagement.

AT MINIMUM

An ADS should be capable of informing the human operator or occupant through various indicators that the ADS is:

- Functioning properly;
- Currently engaged in ADS mode;
- Currently “unavailable” for use;
- Experiencing a malfunction; and/or
- Requesting control transition from the ADS to the operator.

7. Vehicle Cybersecurity

Entities are encouraged to follow a robust product development process based on a systems engineering approach to minimize risks to safety, including those due to cybersecurity threats and vulnerabilities. This process should include a systematic and ongoing safety risk assessment for each ADS, the overall vehicle design into which it is being integrated, and when applicable, the broader transportation ecosystem.²⁰

Entities are encouraged to design their ADSs following established best practices for cyber vehicle physical systems. Entities are encouraged to consider and incorporate voluntary guidance, best practices, and design principles published by National Institute of Standards and Technology (NIST²¹), NHTSA, SAE International, the Alliance of Automobile Manufacturers, the Association of Global Automakers, the Automotive Information Sharing and Analysis Center (Auto-ISAC),²² and other relevant organizations, as appropriate.

NHTSA encourages entities to document how they incorporated vehicle cybersecurity considerations into ADSs, including all actions, changes, design choices, analyses, and associated testing, and ensure that data is traceable within a robust document version control environment.

Industry sharing of information on vehicle cybersecurity facilitates collaborative learning and helps prevent industry members from experiencing the same cyber vulnerabilities. Entities are encouraged

to report to the Auto-ISAC all discovered incidents, exploits, threats and vulnerabilities from internal testing, consumer reporting, or external security research as soon as possible, regardless of membership. Entities are further encouraged to establish robust cyber incident response plans and employ a systems engineering approach that considers vehicle cybersecurity in the design process. Entities involved with ADSs should also consider adopting a coordinated vulnerability reporting/disclosure policy.



8. Crashworthiness

Occupant Protection

Given that a mix of vehicles with ADSs and those without will be operating on public roadways for an extended period of time, entities still need to consider the possible scenario of another vehicle crashing into an ADS-equipped vehicle and how to best protect vehicle occupants in that situation. Regardless of whether the ADS is operating the vehicle or the vehicle is being driven by a human driver, the occupant protection system should maintain its intended performance level in the event of a crash.

Entities should consider incorporating information from the advanced sensing technologies needed for ADS operation into new occupant protection systems that provide enhanced protection to occupants of all ages and sizes. In addition to the seating configurations evaluated in current standards, entities are encouraged to evaluate and consider additional countermeasures that will protect all occupants in any alternative planned seating or interior configurations during use.²³

Compatibility

Unoccupied vehicles equipped with ADSs should provide geometric and energy absorption crash compatibility with existing vehicles on the road.²⁴ ADSs intended for product or service delivery or other unoccupied use scenarios should consider appropriate vehicle crash compatibility given the potential for interactions with vulnerable road users and other vehicle types.

Entities are not required to submit a Voluntary Safety Self-Assessment, nor is there any mechanism to compel entities to do so. While these assessments are encouraged prior to testing and deployment, NHTSA does not require that entities provide disclosures nor are they required to delay testing or deployment. Assessments are not subject to Federal approval.

9. Post-Crash ADS Behavior

Entities engaging in testing or deployment should consider methods of returning ADSs to a safe state immediately after being involved in a crash. Depending upon the severity of the crash, actions such as shutting off the fuel pump, removing motive power, moving the vehicle to a safe position off the roadway (or safest place available), disengaging electrical power, and other actions that would assist the ADSs should be considered. If communications with an operations center, collision notification center, or vehicle communications technology exist, relevant data is encouraged to be communicated and shared to help reduce the harm resulting from the crash.

Additionally, entities are encouraged to have documentation available that facilitates the maintenance and repair of ADSs before they can be put back in service. Such documentation would likely identify the equipment and the processes necessary to ensure safe operation of the ADSs after repairs.



10. Data Recording

Learning from crash data is a central component to the safety potential of ADSs. For example, the analysis of a crash involving a single ADS could lead to safety developments and subsequent prevention of that crash scenario in other ADSs. Paramount to this type of learning is proper crash reconstruction. Currently, no standard data elements exist for law enforcement, researchers, and others to use in determining why an ADS-enabled vehicle crashed. Therefore, entities engaging in testing or deployment are encouraged to establish a documented process for testing, validating, and collecting necessary data related to the occurrence of malfunctions, degradations, or failures in a way that can be used to establish the cause of any crash. Data should be collected for on-road testing and use, and entities are encouraged to adopt voluntary guidance, best practices, design principles, and standards



issued by accredited standards developing organizations such as SAE International.²⁵ Likewise, these organizations are encouraged to be actively engaged in the discussion and regularly update standards as necessary and appropriate.

To promote a continual learning environment, entities engaging in testing or deployment should collect data associated with crashes involving: (1) fatal or nonfatal personal injury or (2) damage that requires towing, including damage that prevents a motor vehicle involved from being driven under its own power in its customary manner or damage that prevents a motor vehicle involved from being driven without resulting in further damage or causing a hazard to itself, other traffic elements, or the roadway.

For crash reconstruction purposes (including during testing), it is recommended that ADS data be stored, maintained, and readily available for retrieval as is current practice, including applicable privacy protections, for crash event data recorders.²⁶ Vehicles should record, at a minimum, all available information relevant to the crash, so that the circumstances of the crash can be reconstructed. These data should also contain the status of the ADS and whether the ADS or the human driver was in control of the vehicle leading up to, during, and immediately following a crash. Entities should have the technical and legal capability to share with government authorities the relevant recorded information as necessary for crash reconstruction purposes. Meanwhile, for consistency and to build public trust and acceptance, NHTSA will continue working with SAE International to begin the work necessary to establish uniform data elements for ADS crash reconstruction.

11. Consumer Education and Training

Education and training is imperative for increased safety during the deployment of ADSs.²⁷ Therefore, entities are encouraged to develop, document, and maintain employee, dealer, distributor, and consumer education and training programs to address the anticipated differences in the use and operation of ADSs from those of the conventional vehicles that the public owns and operates today.²⁸ Such programs should consider providing target users the necessary level of understanding to utilize these technologies properly, efficiently, and in the safest manner possible.

Entities, particularly those engaging in testing or deployment, should also ensure that their own staff, including their marketing and sales forces, understand the technology and can educate and train their dealers, distributors, and consumers.²⁹

Consumer education programs are encouraged to cover topics such as ADSs' functional intent, operational parameters, system capabilities and limitations, engagement/disengagement methods, HMI, emergency fallback scenarios, operational design domain parameters (i.e., limitations), and mechanisms that could alter ADS behavior while in service. They should also include explicit information on what the ADS is capable and not capable of in an effort to minimize potential risks from user system abuse or misunderstanding.

As part of their education and training programs, ADS dealers and distributors should consider including an on-road or on-track experience demonstrating ADS operations and HMI functions prior to consumer release. Other innovative approaches (e.g., virtual reality or onboard vehicle systems) may also be considered, tested, and employed. These programs should be continually evaluated for their effectiveness and updated on a routine basis, incorporating feedback from dealers, customers, and other sources.

12. Federal, State, and Local Laws

Entities are also encouraged to document how they intend to account for all applicable Federal, State, and local laws in the design of their vehicles and ADSs. Based on the operational design domain(s), the development of ADSs should account for all governing traffic laws when operating in automated mode for the region of operation.³⁰ For testing purposes, an entity may rely on an ADS test driver or other mechanism to manage compliance with the applicable laws.

In certain safety-critical situations (such as having to cross double lines on the roadway to travel safely past a broken-down vehicle on the road) human drivers may temporarily violate certain State motor vehicle driving laws. It is expected that ADSs have the capability of handling such foreseeable events safely; entities are encouraged to have a documented process for independent assessment, testing, and validation of such plausible scenarios.

Given that laws and regulations will inevitably change over time, entities should consider developing processes to update and adapt ADSs to address new or revised legal requirements.

NHTSA encourages collaboration and communication between Federal, State, and local governments and the private sector as the technology evolves, and the Agency will continue to coordinate dialogue among all stakeholders. Collaboration is essential as our Nation embraces the many technological developments affecting our public roadways.

VOLUNTARY SAFETY SELF-ASSESSMENT

Entities engaged in ADS testing and deployment may demonstrate how they address – via industry best practices, their own best practices, or other appropriate methods – the safety elements contained in the Voluntary Guidance by publishing a Voluntary Safety Self-Assessment. The Voluntary Safety Self-Assessment is intended to demonstrate to the public (particularly States and consumers) that entities are: (1) considering the safety aspects of ADSs; (2) communicating and collaborating with DOT; (3) encouraging the self-establishment of industry safety norms for ADSs; and (4) building public trust, acceptance, and confidence through transparent testing and deployment of ADSs. It also allows companies an opportunity to showcase their approach to safety, without needing to reveal proprietary intellectual property.

To facilitate this process and as an example of the type of information an entity might provide as part of its Voluntary Safety Self-Assessment, NHTSA has assembled an illustrative template for one of the safety elements within the Voluntary Guidance. This template is available on NHTSA's website. However, the information submitted could vary beyond the template when information is limited or unavailable (e.g., testing activities) or if the entity wishes to provide supplemental information.

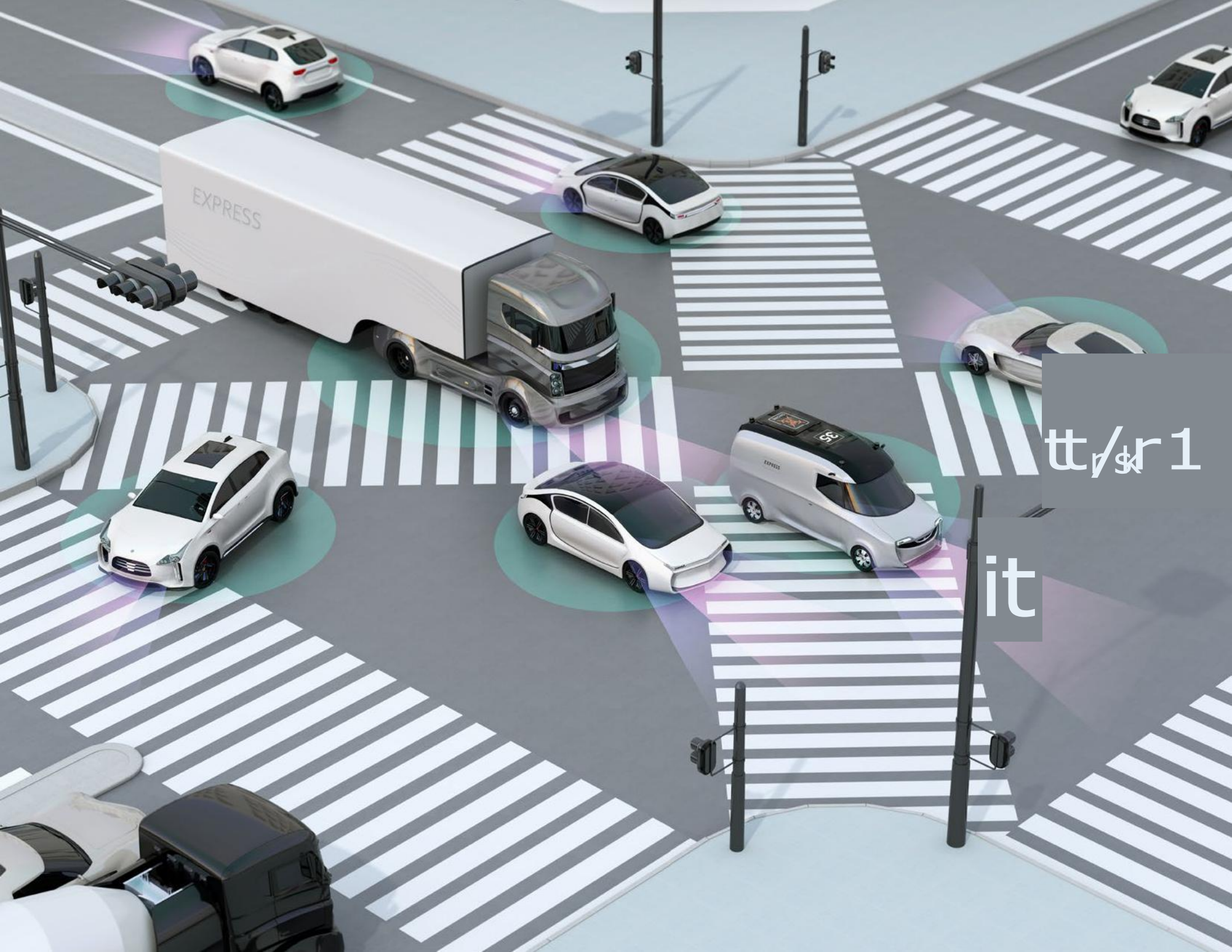
Entities should ensure that Voluntary Safety Self-Assessments do not contain confidential business information (CBI), as it would be information available to the public. Entities will presumably wish to update these documents over time.

For each safety element laid out by the Voluntary Guidance, entities are encouraged to include an acknowledgment within the Voluntary Safety Self-Assessment that indicates one of the following:

- This safety element was considered during product development efforts for the subject feature; or
- This safety element is not applicable to the subject product development effort.

NHTSA envisions that the Voluntary Safety Self-Assessments would contain concise information on how entities are utilizing the Voluntary Guidance and/or their own processes to address applicable safety elements identified in the Voluntary Guidance. The Voluntary Safety Self-Assessment should not serve as an exhaustive recount of every action the entity took to address a particular safety element.

Entities are not required to submit a Voluntary Safety Self-Assessment, nor is there any mechanism to compel entities to do so. While these assessments are encouraged prior to testing and deployment, NHTSA does not require that entities provide submissions nor are they required to delay testing or deployment. Assessments are not subject to Federal approval.



$\pi_r 1$

it

THE FEDERAL AND STATE ROLES

NHTSA strongly encourages States not to codify this Voluntary Guidance (that is, incorporate it into State statutes) as a legal requirement for any phases of development, testing, or deployment of ADSs. Allowing NHTSA alone to regulate the safety design and performance aspects of ADS technology will help avoid conflicting Federal and State laws and regulations that could impede deployment.

SECTION 2: TECHNICAL ASSISTANCE TO STATES

Best Practices for Legislatures Regarding Automated Driving Systems

OVERVIEW

The National Highway Traffic Safety Administration (NHTSA) of the U.S. Department of Transportation (DOT) is prepared to assist with challenges that States face regarding the safe integration of SAE Level 3 and above Automated Driving Systems (ADSs) on public roads. Given that vehicles operating on public roads are subject to both Federal and State jurisdictions and States are beginning to regulate ADSs, NHTSA has developed this section. It is designed to clarify and delineate the Federal and State roles in the regulation of ADSs and lay out a framework that the States can use as they write their laws and regulations surrounding ADSs to ensure a consistent, unified national framework.

NHTSA is working to bring ADSs safely onto the Nation's roadways in a way that encourages ADS entities (manufacturers, suppliers, transit operators, automated fleet operators, or any entity that offers services utilizing ADSs), consumer advocacy organizations, State legislatures, and other interested parties to work together in a shared environment. As the technology grows and the horizon of ADS changes rapidly, it is essential for each of these entities and interested parties to exercise due diligence in staying ahead of activity in a proactive—rather than reactive—manner.

States have begun to propose and pass legislation concerning ADSs. Public comments to NHTSA suggest that these proposals present several disparate approaches for adding and amending State authority over ADSs. Public comments and some State officials have asked NHTSA to provide guidance (and eventually regulations) that would support a more national approach to testing and deploying ADSs.

Further, in a prior collaborative effort between States and the Federal Government, NHTSA entered a 2-year cooperative agreement (beginning in September 2014) with the American Association of Motor

Vehicle Administrators (AAMVA) under which the Autonomous Vehicle Best Practices Working Group was created. The working group was chartered to organize and share information related to the development, design, testing, use, and regulation of ADSs and other emerging vehicle technology. Based on the working group's research, a report is currently being developed to assist jurisdictions in enhancing their current ADS regulations or considering developing new legislation.³¹ The goal of the report is to promote uniformity amongst jurisdictions and provide a baseline safety approach to possible challenges to the regulation of ADS and testing the drivers who operate them.

Coinciding with the development of AAMVA's report, NHTSA has continued to work with State stakeholders including the National Conference of State Legislatures (NCSL) and the Governors Highway Safety Association (GHSA) to identify emerging challenges in the integration of ADSs and conventional motor vehicles.

Based on public input and the Agency's ongoing work with partners such as NCSL, GHSA, and AAMVA, NHTSA offers these Best Practices and specific legal components States should consider as we all work toward the shared goal of advancing safe ADS integration. The objective is to assist States in developing ADS laws, if desired, and creating consistency in ADS regulation across the country.

While technology is evolving and new State legislative language is still being drafted and reviewed, States can proactively evaluate current laws and regulations so as not to unintentionally create barriers to ADS operation, such as a requirement that a driver have at least one hand on the steering wheel at all times.

NHTSA encourages States to review others’ draft ADS policies and legislation and work toward consistency. The goal of State policies in this realm need not be uniformity or identical laws and regulations across all States. Rather, the aim should be sufficient consistency of laws and policies to promote innovation and the swift, widespread, safe integration of ADSs.

States are encouraged to maintain a good state of infrastructure design, operation, and maintenance that supports ADS deployment and to adhere to the Manual on Uniform Traffic Control Devices (MUTCD), the existing national standard for traffic control devices as required by law. For example, items that may be considered a low priority now because of the presence of a human driver may be considered a higher priority as vehicle systems begin to rely more on machine vision and other techniques to detect where they are in a given lane. In addition, States are urged to continue to work with the Federal Highway Administration (FHWA) and the American Association of State Highway and Transportation Officials (AASHTO)³² to support uniformity and consensus in infrastructure standards setting. This will support the safe operation of ADSs and ensure the safety of human drivers, who will continue to operate vehicles on the roads for years to come.

FEDERAL AND STATE REGULATORY ROLES

In consideration of State activity regarding ADSs, as well as NHTSA’s activity at the Federal level, it is important to delineate Federal and State regulatory responsibility for motor vehicle operation.

These general areas of responsibility should remain largely unchanged for ADSs. NHTSA is responsible for regulating motor vehicles and motor vehicle equipment, and States are responsible for regulating the human driver and most other aspects of motor vehicle operation.

Further DOT involvement includes safety, evaluation, planning, and maintenance of the Nation’s infrastructure through FHWA as well as regulation of the safe operation of interstate motor carriers and commercial vehicle drivers, along with registration and insurance requirements through the Federal Motor Carrier Safety Administration (FMCSA).

DOT strongly encourages States to allow DOT alone to regulate the safety design and performance aspects of ADS technology. If a State does pursue ADS performance-related regulations, that State should consult with NHTSA.

NHTSA’S RESPONSIBILITIES	STATES’ RESPONSIBILITIES
<ul style="list-style-type: none">• Setting Federal Motor Vehicle Safety Standards (FMVSSs) for new motor vehicles and motor vehicle equipment (with which manufacturers must certify compliance before they sell their vehicles)³³• Enforcing compliance with FMVSSs• Investigating and managing the recall and remedy of noncompliances and safety-related motor vehicle defects nationwide• Communicating with and educating the public about motor vehicle safety issues	<ul style="list-style-type: none">• Licensing human drivers and registering motor vehicles in their jurisdictions• Enacting and enforcing traffic laws and regulations• Conducting safety inspections, where States choose to do so• Regulating motor vehicle insurance and liability

BEST PRACTICES FOR LEGISLATURES

As States act to ensure the safety of road users in their jurisdictions, NHTSA continually monitors and reviews language to stay informed on State legislation. In reviewing draft State legislation, the Agency has identified common components and has highlighted significant elements regarding ADSs that States should consider including in legislation. As such, NHTSA recommends the following safety-related best practices when crafting legislation for ADSs:

- **Provide a “technology-neutral” environment.**

States should not place unnecessary burdens on competition and innovation by limiting ADS testing or deployment to motor vehicle manufacturers only. For example, no data suggests that experience in vehicle manufacturing is an indicator of the ability to safely test or deploy vehicle technology. All entities that meet Federal and State law prerequisites for testing or deployment should have the ability to operate in the State.

- **Provide licensing and registration procedures.**

States are responsible for driver licensing and vehicle registration procedures. To support these efforts, NHTSA recommends defining “motor vehicle” under ADS laws to include any vehicle operating on the roads and highways of the State; licensing ADS entities and test



operators for ADSs; and registering all vehicles equipped with ADSs and establishing proof of financial responsibility requirements in the form of surety bonds or self-insurance. These efforts provide States with the same information as that collected for conventional motor vehicles and improve State recordkeeping for ADS operation.

- **Provide reporting and communications methods for Public Safety Officials.**

States can take steps to monitor safe ADS operation through reporting and communications mechanisms so that entities can coordinate with public safety agencies. The safety of public safety

officials, other road users, and ADS passengers will be improved with greater understanding of the technology, capabilities, and functioning environment. States should develop procedures for entities to report crashes and other roadway incidents involving ADSs to law enforcement and first responders.

- **Review traffic laws and regulations that may serve as barriers to operation of ADSs.**

States should review their vehicle codes, applicable traffic laws, and similar items to determine if there are unnecessary regulatory barriers that would prevent the testing and deployment of ADSs on public roads. For example, some States require a human operator to have one hand on the steering wheel at all times – a law that would pose a barrier to Level 3 through Level 5 ADSs.

BEST PRACTICES FOR STATE HIGHWAY SAFETY OFFICIALS

States have a general responsibility to reduce traffic crashes and the resulting deaths, injuries, and property damage for all road users in their jurisdictions. States use this authority to establish and maintain highway safety programs addressing: driver education and testing; licensing; pedestrian safety; law enforcement; vehicle registration and inspection; traffic control; highway design and maintenance; crash prevention, investigation, and recordkeeping; and emergency services. This includes any legal components States may wish to consider upon drafting legislation on ADSs.

The following sections describe a framework for States looking for assistance in developing procedures and conditions for ADSs' introduction onto public roadways. NHTSA and AAMVA's collaborative partnership on a Model State Policy is the foundation of the following discussion; however, it has been upgraded to incorporate additional concerns of State stakeholders, the clarification of roles, and an emphasis on the States' consideration of the information—rather than a directive for action. NHTSA does not expect that States will necessarily need to create any new processes or requirements in order to support ADS activities. Instead, the references below are intended as guidance for those States that may be looking to incorporate ADSs into existing processes or requirements or States who are considering such processes or requirements.

1. Administrative: States may want to consider new oversight activities on an administrative level to support States' roles and activities as they relate to ADSs. NHTSA does not expect that States will need to create any particular new entity in order to support ADS activities, but States may decide to create some of these entities if the State determines that they will be useful. The references below are intended as examples of those that may be appropriate for participation.

- a. Consider identifying a lead agency responsible for deliberation of any ADS testing.

- b. Consider creating a jurisdictional ADS technology committee that is launched by the designated lead agency and includes representatives from the governor's office, the motor vehicle administration, the State department of transportation, the State law enforcement agency, the State Highway Safety Office, State office of information technology, State insurance regulator, the State office(s) representing the aging and disabled communities, toll authorities, trucking and bus authorities, and transit authorities.
- c. To encourage open communication, the designated lead agency may choose to inform the State automated safety technology committee of the requests from entities to test in their State and the status of the designated agency's response to companies.
- d. In an effort to implement a framework for policies and regulations, the designated lead agency could take steps to use or establish statutory authority. This preparation would involve examination of laws and regulations in order to address unnecessary barriers to ADS operation on public roadways.
- e. Consider developing an internal process to include an application for entities to test in their State.
- f. Consider establishing an internal process for issuing test ADS vehicle permits.

2. Application for Entities to Test ADSs on Public Roadways:

For those States with an existing application process for test vehicles, the following are considerations for applications involving testing of an ADS on public roadways. It is recommended that the application for testing remain at the State level; however, if a State chooses to request applications at a local level, these considerations would carry to those jurisdictions.

- a. States could request that an entity submit an application to the designated lead agency in each State in which it plans to test ADSs. A process should be considered for application submission in those situations in which multiple entities are involved in the testing of an ADS.
- b. States could request the following information from entities to ensure accurate recordkeeping:
 - Name, corporate physical and mailing addresses, in-State physical and mailing addresses (if applicable), and the program administrator/director's name and contact information;
 - Identification of each ADS that will be used on public roadways by VIN, vehicle type, or other unique identifiers such as the year, make, and model; and
 - Identification of each test operator, the operator's driver license number, and the State or country in which the operator is licensed.
- c. Inclusion of the entity's safety and compliance plan for the ADS could provide increased safety assurance to the State.
- d. Inclusion of evidence of the entity's ability to satisfy a judgment or judgments for damages for personal injury, death, or property damage caused by an ADS in the form of an instrument of insurance, a surety bond, or proof of self-insurance could provide increased safety assurance to the State.³⁴
- e. Inclusion of a summary of the training provided to the employees, contractors, or other users designated by the entity as test operators of the ADS could provide increased safety assurance to the State.

3. Permission for Entities to Test ADSs on Public Roadways:

For States that grant permission for testing of vehicles, the following are considerations for granting permission for ADS testing on public roadways. It is recommended that permission to test remain at the State level; however, State and local governments should coordinate. If a State chooses to request applications at a local level, these considerations would carry to those jurisdictions.

- a. For greater public safety, it is recommended that a State's lead agency involve law enforcement agencies before responding to the application for testing from the entity.
- b. It would be appropriate to suspend permission to test if the entity fails to comply with the State insurance or driver requirements.



- f. It would be appropriate for the lead agency to request additional information or require an entity to modify its application before granting approval.
- g. If a State requires an application, it should consider notification to the entity indicating permission to test that ADS in the State. A State may choose to request that entity's test vehicles carry a copy of proof of permission to test that ADS in those vehicles.

4. Specific Considerations for ADS Test Drivers and Operations:

Considerations for States providing access for test-ADSs as they are operated under designated circumstances and with entity-based operators.

- a. If a State is concerned about the training of an ADS test driver, the State could request a summary of the training provided to the test driver.
- b. For test vehicles, the test driver should follow all traffic rules and report crashes as appropriate for the State.
- c. States regulate human drivers. Licensed drivers are necessary to perform the driving functions for motor vehicles equipped with automated safety technologies that are less than fully automated (SAE Levels 3 and lower). A licensed driver has responsibility to operate the vehicle, monitor the operation, or be immediately available to perform the driving task when requested or the lower level automated system disengages.
- d. Fully automated vehicles are driven entirely by the vehicle itself and require no licensed human driver (SAE levels 4 and 5), at least in certain environments or under certain conditions.³⁵ The entire driving operation (under specified conditions) is performed by a motor vehicle automated system from origin to destination.

5. Considerations for Registration and Titling: Specific considerations regarding identification and records for ADS deployed for consumer use and operation.

- a. Consider identification of an ADS on the title and registration. This could apply to all ADSs or only those capable of operating without a human driver.
- b. Consider requiring notification of ADS upgrades if the vehicle has been significantly upgraded post-sale. Applicable State forms could be adjusted to reflect the upgrade.

6. Working With Public Safety Officials: General considerations as public safety officials begin to understand vehicles and needs.

- a. States could consider training public safety officials in conjunction with ADS deployments in their jurisdictions to improve understanding of ADS operation and potential interactions.
- b. Coordination among States would be beneficial for developing policies on human operator behaviors, as to monitor behavior changes—if any—in the presence of ADSs when the vehicle is in control.

7. Liability and Insurance: Initial considerations for State relegation of liability during an incident and insurance of the driver, entity, and/ or ADS. These considerations may take time and broad discussion of incident scenarios, understanding of technology, and knowledge of how the ADSs are being used (personal use, rental, ride share, corporate, etc.). Additionally, determination of the operator of an ADS, in a given circumstance, may not necessarily determine liability for crashes involving the ADS.

- a. Begin to consider how to allocate liability among ADS owners, operators, passengers, manufacturers, and other entities when a crash occurs.
- b. For insurance purposes, determine who (owner, operator, passenger, manufacturer, other entity, etc.) must carry motor vehicle insurance.
- c. States could begin to consider rules and laws allocating tort liability.

CONCLUSION

Public trust and confidence in the evolution of ADSs has the potential to advance or inhibit the testing and deployment of ADSs on public roadways. NHTSA is committed to supporting the safety of these emerging and evolutionary technological advancements, which have the potential to significantly improve roadway safety. The Voluntary Guidance, highlighting the 12 priority safety elements, and its associated Voluntary Safety Self-Assessment offer public reassurance that safety remains NHTSA's top priority. The States' Best Practices section reinforces NHTSA's willingness to assist States with the challenges they face regarding ADSs now and in the pivotal years ahead.

This document will be updated periodically to reflect advances in technology, increased presence of ADSs on public roadways, and any regulatory action or statutory changes that could occur at both the Federal and State levels. In the meantime, the information provided herein serves to aid industry as it moves forward with testing and deploying ADSs and States with drafting legislation and developing plans and policies regarding ADSs. NHTSA encourages collaboration and communication between Federal, State, and local governments and the private sector as the technology evolves, and the Agency will continue to coordinate dialogue among all stakeholders. Collaboration is essential as our Nation embraces the many technological developments affecting our public roadways. Together, we can use lessons learned to make any necessary course corrections, to prevent or mitigate unintended consequences or safety risks, and to positively transform American mobility safely and efficiently.

RESOURCES

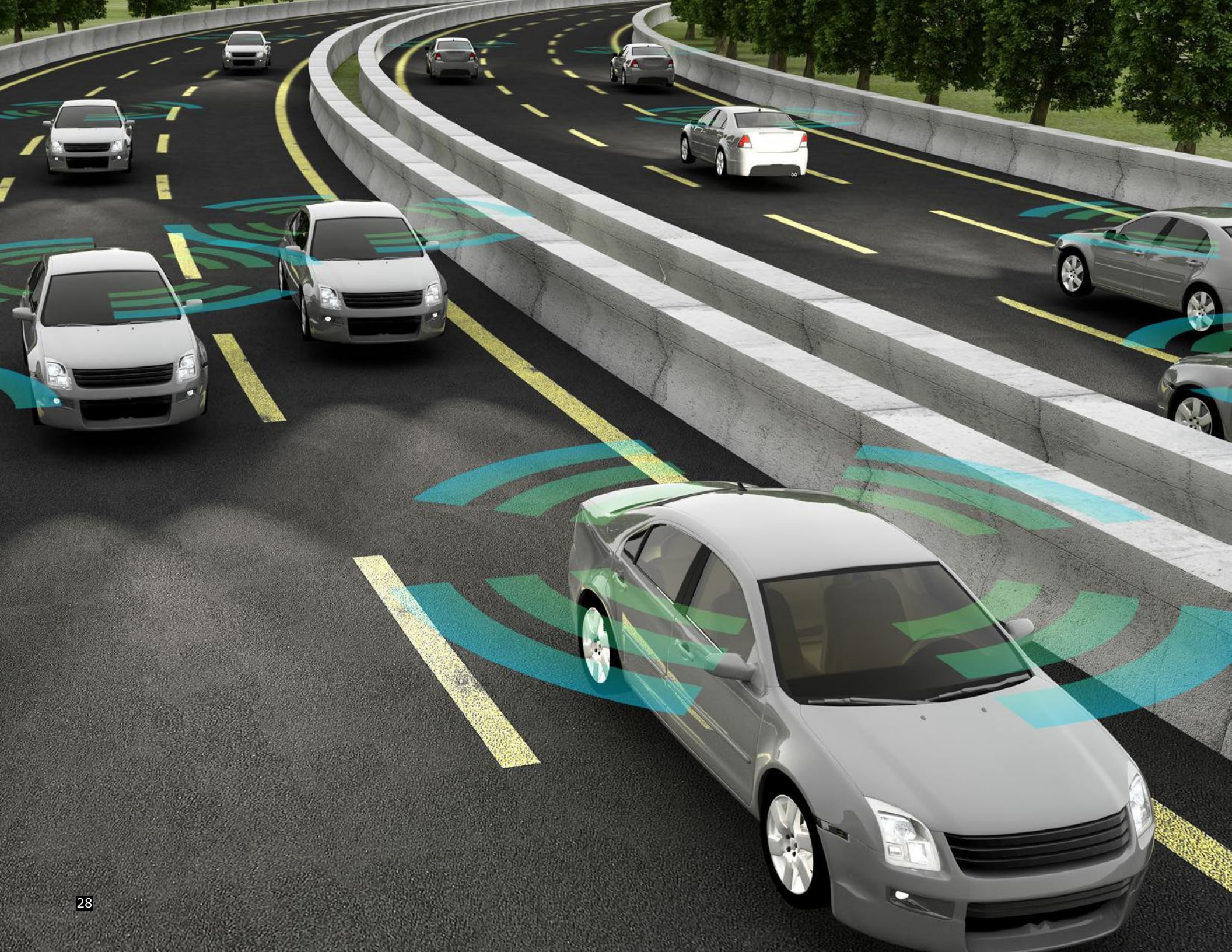
A central repository of associated references to this and other NHTSA ADS resources will be maintained at www.nhtsa.gov/technology-innovation/automated-vehicles.

This includes an informational resource to support manufacturers and other entities interested in requesting regulatory action from NHTSA.

ENDNOTES

- 1 NHTSA acknowledges that Privacy and Ethical Considerations are also important elements for entities to deliberate. See www.nhtsa.gov/AVforIndustry for NHTSA's approach on each.
- 2 NHTSA completed the Paperwork Reduction Act (PRA) process and received clearance from the Office of Management and Budget (OMB) on the Federal Automated Vehicles Policy Voluntary Guidance's information collection through August 31, 2018, 81 FR 65709. However, pursuant to PRA, NHTSA is again seeking public comment on an updated Information Collection Request (ICR) that covers the information included in Automated Driving Systems: A Vision for Safety. The ICR identified in this document will not be effective until the ICR process is completed.
- 3 SAE International J3016, International Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles (J3016:Sept 2016).
- 4 See, e.g., 49 U.S.C. §§ 30102(a)(8), 30116, 30120.
- 5 Parts of this Voluntary Guidance could be applied to any form of ADS.
- 6 The National Traffic and Motor Vehicle Safety Act, as amended ("Safety Act"), 49 U.S.C. 30101 et seq., provides the basis and framework for NHTSA's enforcement authority over motor vehicle and motor vehicle equipment defects and non-compliances with Federal Motor Vehicle Safety Standards (FMVSS).
- 7 Under ISO 26262 (Road Vehicles: Functional Safety), functional safety refers to the absence of unreasonable safety risks in cases of electrical and electronic failures.
- 8 For example, the U.S. Department of Defense standard practice on system safety, MIL-STD-882E. 11 May 2012. Available at www.system-safety.org/Documents/MIL-STD-882E.pdf.
- 9 See Van Eikema Hommes, Q.D. (2016, June). *Assessment of Safety Standards for Automotive Electronic Control Systems*. (Report No. Dot HS 812 285). Washington, DC: National Highway Traffic Safety Administration. Available at ntl.bts.gov/lib/59000/59300/59359/812285_ElectronicsReliabilityReport.pdf.
- 10 "Minimal risk condition" means low-risk operating condition that an automated driving system automatically resorts to either when a system fails or when the human driver fails to respond appropriately to a request to take over the dynamic driving task. See SAE International J3016, International Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles (J3016:Sept2016).
- 11 "Fallback ready user" means the user of a vehicle equipped with an engaged ADS feature who is able to operate the vehicle and is receptive to ADS-issued requests to intervene and to evident dynamic driving task (DDT) performance-relevant system failures in the vehicle compelling him or her to perform the DDT fallback. See SAE International J3016, International Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles (J3016:Sept2016).
- 12 See Automated Vehicle Research for Enhanced Safety: Final Report. Collision Avoidance Metrics Partnership, Automated Vehicle Research Consortium. June 2016. DTNH22-050H-01277. The report includes detailed functional descriptions for on-road driving automation levels and identifies potential objective test methods that could be used as a framework for evaluating emerging and future driving automation features. Available at www.noticeandcomment.com/Automated-Vehicle-Research-for-Enhanced-Safety-Final-Report-fn-459371.aspx.
- 13 See Nowakowski, C., et al., *Development of California Regulations to Govern the Testing and Operation of Automated Driving Systems*, California PATH Program, University of California, Berkeley, Nov. 14, 2014, pg. 10. Available at <http://docs.trb.org/prp/15-2269.pdf>.
- 14 California Partners for Advanced Transit and Highways (PATH) is a multidisciplinary research and development program of the University of California, Berkeley, with staff, faculty, and students from universities worldwide and cooperative projects with private industry, State and local agencies, and nonprofit institutions. See www.path.berkeley.edu.
- 15 Id., pgs. 10-11. California PATH's work described minimum behavioral competencies for automated vehicles as "necessary, but by no means sufficient, capabilities for public operation." Id. The document's full peer review is available at www.nspe.org/sites/default/files/resources/pdfs/Peer-Review-Report-IntegratedV2.pdf.
- 16 See Rau, P., Yanagisawa, M., and Najm, W. G., *Target Crash Population of Automated Vehicles*, available at www-esv.nhtsa.dot.gov/Proceedings/24/files/Session_21_Written.pdf.

- 17 See Najm, W. G., Smith, J. D., and Yanagisawa, M., "Pre-Crash Scenario Typology for Crash Avoidance Research," DOT HS 810 767, April 2007. Available at www.nhtsa.gov/gov-Final_PDF_Version_5-2-07.pdf.
- 18 Available at http://ntl.bts.gov/lib/55000/55400/55443/AVBenefitFrameworkFinalReport082615_Cover1.pdf.
- 19 Entities are encouraged to seek technical and engineering advice from members of the disabled community and otherwise engage with that community to develop designs informed by its needs and experiences.
- 20 Entities should insist that their suppliers build into their equipment robust cybersecurity features. Entities should also address cybersecurity, but they should not wait to receive equipment from a supplier before doing so.
- 21 www.nist.gov/cyberframework.
- 22 An Information Sharing and Analysis Center (ISAC) is a trusted, sector specific entity that can provide a 24-hour-per-day 7-day-per-week secure operating capability that establishes the coordination, information sharing, and intelligence requirements for dealing with cybersecurity incidents, threats, and vulnerabilities. See McCarthy, C., Harnett, K., Carter, A., and Hatipoglu, C. (2014, October). *Assessment of the information sharing and analysis center model* (Report No. DOT HS 812 076). Washington, DC: National Highway Traffic Safety Administration.
- 23 The tools to demonstrate such due care need not be limited to physical testing but also could include virtual tests with vehicle and human body models.
- 24 In 2003, as part of a voluntary agreement on crash compatibility, the Alliance of Automobile Manufacturers agreed to a geometric compatibility commitment which would provide for alignment of primary energy absorbing structures among vehicles. The European Union recently introduced a new frontal crash test that also requires geometric load distribution similar to the Alliance voluntary agreement.
- 25 The collection, recording, storage, auditing, and deconstruction of data recorded by an entity must be in strict accordance with the entity's consumer privacy and security agreements and notices, as well as any applicable legal requirements.
- 26 See 49 CFR Part 563, Event Data Recorders. Available at www.gpo.gov/fdsys/pkg/CFR-2016-title49-vol6/xml/CFR-2016-title49-vol6-part563.xml.
- 27 Not applicable to ADS testing.
- 28 The training and education programs recommended here are intended to complement and augment driver training and education programs run by States that retain the primary responsibility for training, testing, and licensing human drivers.
- 29 Such training and education programs for employees, dealers, distributors, and consumers may be administered by an entity other than the direct employer, manufacturer, or other applicable entity.
- 30 Traffic laws vary from State to State (and even city to city); ADSs should be able to follow all laws that apply to the applicable operational design domain. This includes speed limits, traffic control devices, one-way streets, access restrictions (crosswalks, bike lanes), U-turns, right-on-red situations, metering ramps, and other traffic circumstances and situations.
- 31 Future updates to AAMVA's guide may integrate commercial vehicle ADS operational aspects brought forth by the Commercial Vehicle Safety Alliance (CVSA).
- 32 AASHTO is an international leader in setting technical standards for all phases of highway system development. Standards are issued for design, construction of highways and bridges, materials, and many other technical areas. See www.transportation.org/home/organization/.
- 33 NHTSA does not expressly regulate motor vehicle (or motor vehicle equipment) in-use performance after first sale. However, because the FMVSSs apply to the vehicle or equipment when first manufactured and because taking a vehicle or piece of equipment out of compliance with an applicable standard can be a violation of the Safety Act, the influence of the FMVSSs extends throughout the life of the vehicle even if NHTSA is not directly regulating it. At the same time, States have the authority to regulate a vehicle's in-use performance (through safety inspection laws), but as the text here states, State regulations cannot conflict with applicable FMVSSs. Additionally, NHTSA continues to have broad enforcement authority to evaluate and address safety risks as they arise.
- 34 AAMVA experts recommended a minimum insurance requirement of \$5 million; however, that is subject to State considerations.
- 35 Some vehicles may be capable of being entirely "driven" either by the vehicle itself or by a human driver. For such dual-capable vehicles, the States would have jurisdiction to regulate (license, etc.) the human driver.



DOT HS 812 442
September 2017



O

U.S. Department of Transportation



APPLYING DATA MINIMIZATION TO CONSUMER REQUESTS

SUMMARY

- Data minimization is a foundational principle in the CCPA. Many aspects of the CCPA's implementing regulations underscore this principle.
- Businesses must apply 11 CCR § 7002(d)—in coordination with other applicable sections of the CCPA and its implementing regulations—for each purpose for which businesses collect, use, retain, and share personal information.
- Data minimization principles apply to the processing of consumers' CCPA requests.

ENFORCEMENT OBSERVATIONS

Data minimization is a foundational principle in the CCPA. Businesses should apply this principle to every purpose for which they collect, use, retain, and share consumers' personal information.

Data minimization serves important functions. For example, data minimization reduces the risk that unintended persons or entities will access personal information, such as through data breaches. Data minimization likewise supports good data governance, including through potentially faster responses to consumers' requests to exercise their CCPA rights. Businesses reduce their exposure to these risks and improve their data governance by periodically assessing their collection, use, retention, and sharing of personal information from the perspective of data minimization.

The Enforcement Division is observing, however, that certain businesses are asking consumers to provide excessive and unnecessary personal information in response to requests that consumers make under the CCPA. The Enforcement Division reminds businesses to apply the data minimization principle to each purpose for which they collect, use, retain, and share consumers' personal information—including information that businesses collect when processing consumers' CCPA requests.

ENFORCEMENT ADVISORIES GENERALLY

Enforcement Advisories address select provisions of the California Consumer Privacy Act and its implementing regulations. Advisories do not cover all potentially applicable laws or enforcement circumstances; the Enforcement Division will make case-by-case enforcement determinations. Advisories do not implement, interpret, or make specific the law enforced or administered by the California Privacy Protection Agency, establish substantive policy or rights, constitute legal advice, or reflect the views of the Agency's Board.



Advisories do not provide any options for alternative relief or safe harbor from potential violations. The statutes and regulations control in the event of any conflicting interpretation. The Advisory provides the questions that follow as hypothetical examples of how a business might review its practices. Businesses should consult the statute, regulation, and/or an attorney before taking any action to ensure compliance with the law.

WHAT THE LAW AND REGULATIONS SAY ABOUT DATA MINIMIZATION

The CCPA's data minimization principle stems from the law's general purpose and intent that businesses should collect consumers' personal information only to the extent that it is relevant and limited to what is necessary in relation to the purposes for which it is being collected, used, and shared. See Prop 24, § 3(B)(3).

The CCPA states:

"A business' collection, use, retention, and sharing of a consumer's personal information **shall be reasonably necessary and proportionate** to achieve the purposes for which the personal information was collected or processed, **or for another disclosed purpose that is compatible** with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes."

Civil Code § 1798.100(c) (emphasis added).

Underscoring this principle, the regulations explain:

"[W]hether a business's collection, use, retention, and/or sharing of a consumer's personal information is **reasonably necessary and proportionate** to achieve the purpose identified ... shall be based on the following:

(1) The minimum personal information that is necessary to achieve the purpose identified For example, to complete an online purchase and send an email confirmation of the purchase to the consumer, an online retailer may need the consumer's order information, payment and shipping information, and email address.

(2) The possible negative impacts on consumers posed by the business's collection or processing of the personal information. For example, a possible negative impact of collecting precise geolocation information is that it may reveal other sensitive personal information about the consumer, such as health information based on visits to healthcare providers.



CALIFORNIA PRIVACY PROTECTION AGENCY

ENFORCEMENT DIVISION

ENFORCEMENT ADVISORY NO. 2024-01

Additional CCPA regulations reflect the concept

(3) **The existence of additional safeguards** for the personal information to **specifically address the possible negative impacts on consumers** For example, a business may consider encryption or automatic deletion of personal information within a specific window of time as potential safeguards.”

11 CCR § 7002(d) (emphasis added).

of data minimization, as shown in bold below:

- **Opt-out Preference Signals.** “The business shall not require a consumer to provide additional information **beyond what is necessary** to send the signal.” 11 CCR § 7025(c)(2).
- **Requests to Opt-out of Sale/Sharing.** “A business shall not require a consumer submitting a request to opt-out of sale/sharing to create an account or provide additional information **beyond what is necessary** to direct the business not to sell or share the consumer’s personal information.” 11 CCR § 7026(c).
- **Requests to Limit Use and Disclosure of Sensitive Personal Information.** “A business shall not require a consumer submitting a request to limit to create an account or provide additional information **beyond what is necessary** to direct the business to limit the use or disclosure of the consumer’s sensitive personal information.” 11 CCR § 7027(d).
- **General Rules Regarding Verification.** In determining the method by which the business will verify the consumer’s identity, the business shall:

(1) “Whenever feasible, **match the identifying information provided by the consumer to the personal information of the consumer already maintained** by the business, or use a third-party identity verification service that complies with this section.

(2) **Avoid collecting** the types of personal information identified in Civil Code section 1798.81.5, subdivision (d) [such as Social Security number, driver’s license number, financial account numbers, or unique biometric data], **unless necessary** for the purpose of verifying the consumer...”

11 CCR § 7060(c) (examples added); and:



requesting additional information from the consumer for purposes of verification. If, however, the business cannot verify the identity of the consumer from the information already maintained by the business, the business may request additional information from the consumer, which shall **only be used for the purposes of verifying the identity of the consumer seeking to exercise their rights under the CCPA, security, or fraud-prevention**. The business shall delete any new personal information collected for the purposes of verification as soon as practical after processing the consumer's request, except as required to comply with section 7101."

11 CCR § 7060(d).

FACTUAL SCENARIOS

Businesses should carefully review whether they are applying the data minimization principle in their collection, use, retention, and sharing of consumers' personal information. Below are two illustrative scenarios in which a business might encounter the data minimization principle: (1) responding to a consumer's CCPA request to opt-out of the sale/sharing of personal information; and (2) verifying a consumer's identity in connection with a CCPA request to delete personal information.

SCENARIO ONE: RESPONDING TO A REQUEST TO OPT-OUT OF SALE/SHARING

As a hypothetical example, Business A—which is covered by the CCPA—receives requests from consumers seeking to opt-out of the sale/sharing of their personal information. Business A is determining how to comply with those requests, including how much personal information to collect from consumers to process their requests.

The CCPA and its regulations speak directly to the right to opt-out of sale/sharing (Civil Code §§ 1798.120, 1798.135; 11 CCR §§ 7025, 7026, 7060(b)). Business A applies the data minimization principle as explained in Civil Code § 1798.100(c) and 11 CCR § 7002(d). Importantly, Business A does not require consumers to verify their identity to make a request to opt-out of sale/sharing:

"A business shall not require a consumer to verify their identity to make a request to opt-out of sale/sharing or to make a request to limit. A business may ask the consumer for information necessary to complete the request; however, it shall not be burdensome on the consumer. For example, a business may ask the consumer for their name, but it shall not require the consumer to take a picture of themselves with their driver's license."

11 CCR § 7060(b).



To apply data minimization principles to these requests, Business A could start by asking itself the following questions consistent with 11 CCR § 7002(c)-(d):

- What is the minimum amount of personal information necessary for our business to honor a request to opt-out of sale/sharing?
- We already have certain personal information from this consumer. Do we need to ask for more personal information than we already have?
- What are the possible negative impacts if we collect additional personal information?
- Could we put in place additional safeguards to address the possible negative impacts?

The information necessary to achieve the purpose of completing the consumer's request will depend on **how** Business A sells or shares personal information, as well as **what** information it sells or shares. For example, if Business A sells or shares a consumer's online activities only in the context of cross-context behavioral advertising, then Business A would not need additional information, such as name or email address, to comply with a consumer request to opt-out of sale or sharing made by way of an opt-out preference signal.

By contrast, if Business A sells or shares profiles of consumers that include both online activity and other information (e.g., purchasing history), then Business A might need the consumer to further identify themselves to apply the opt-out to more than just online activity. Relatedly, if Business A sells or shares purchase history, then asking for unrelated personal information, such as a driver's license, might exceed the "minimum personal information" necessary to comply with the request.

SCENARIO TWO: VERIFICATION OF A CONSUMER'S IDENTITY

As a second hypothetical example, Business B—which is covered by the CCPA—receives requests from consumers to delete their personal information. These consumers do not have accounts with Business B. Business B keeps consumers' names and email addresses on file and receives requests to delete personal information from consumers using their email address on file. Business B is determining how to comply with those requests, including how to verify consumers' identities.

Business B must establish, document, and comply with a reasonable method for verifying that the person making the request is the consumer about whom the business has collected information. (11 CCR § 7060(a).) Business B's purpose for processing the consumer's personal information is to verify that the consumer

making the request is the same consumer about whom the business has collected personal information.



**CALIFORNIA PRIVACY
PROTECTION AGENCY**
ENFORCEMENT DIVISION

ENFORCEMENT ADVISORY NO. 2024-01

In reviewing its verification method, Business B evaluates whether it has complied with the data minimization principle, as well as whether the verification method complies with any regulations that speak specifically to verification (e.g., 11 CCR § 7060 (General Rules Regarding Verification) and in this case, 11 CCR § 7062 (Verification for Non-Accountholders)).

To apply data minimization principles to these requests, the business could start by asking itself the following questions, as set forth in 11 CCR § 7002(c)-(d):

- What is the minimum personal information that is necessary to achieve this purpose (*i.e.*, identity verification)?
- We already have certain personal information from this consumer. Do we need to ask for more personal information than we already have?
- What are the possible negative impacts posed if we collect or use the personal information in this manner?
- Are there additional safeguards we could put in place to address the possible negative impacts?

To help answer these questions, the business will look to regulations that explain the general rules regarding verification (specifically 11 CCR § 7060(c)(1)-(3)), and the rules for verification for non-accountholders accountholders (in this case, 11 CCR § 7062(d), which addresses requests to delete). These regulations help inform the § 7002 data minimization analysis.

As noted above, Business B has consumer names and email addresses. Business B could ask itself:

- The information to be deleted is a name plus email. To what degree of certainty (reasonable or reasonably high) do we need to verify the identity of the consumer? How sensitive is the information to be deleted and what is the risk of harm to the consumer posed by unauthorized deletion?
- We have the email on file. Can we rely on the email address, or is it necessary to request a driver's license number or social security number in order to comply with the request? Is asking for this information to verify a request to delete an email address disproportionate and excessive?



**CALIFORNIA PRIVACY
PROTECTION AGENCY**
ENFORCEMENT DIVISION

ENFORCEMENT ADVISORY NO. 2024-01

For another consumer, Business B has a name and email address on file, and also stores photographs and documents associated with the name and email address. Consumers access their photos and documents by logging in with their email and password, and a code is sent to their email, which they then input into Business B's systems. Business B receives a consumer request from the email address on file, asking to delete all personal information.

In reviewing its verification method, Business B will evaluate whether it has complied with the data minimization principle, as well as whether the verification method complies with any

regulations that speak specifically to verification (e.g., 11 CCR § 7060 (General Rules Regarding Verification) and, in this case, 11 CCR § 7061 (Verification for Password-Protected Accounts)). These regulations help inform the § 7002 data minimization analysis.

In this scenario, Business B could ask itself:

- Are the documents and photos we have on file sensitive information that should warrant a more stringent verification process than just asking for an email address? What is the risk of harm to the consumer if we act on an unauthorized request to delete?
 - We have the email on file. Can we rely on the email address, or can it be spoofed? Is it necessary to use a more stringent verification process, such as requesting the consumer's driver's license number or a copy of the license itself? Is asking for this type of information to verify a request to delete disproportionate and excessive?
 - We don't typically have driver's license numbers in our systems. What are the possible negative impacts posed to the consumer if we do collect driver's license numbers? What harm might result if there's a breach and the driver's license numbers are accessed?
-
- Are there additional safeguards we could put in place to address these possible negative impacts? How does our business interact with consumers? Can we have the consumer request and confirm a code in order to verify their identity in connection with their request to delete? Should we have the consumer request and confirm the code as a means of reauthenticating their identity?

ISSUED BY

Enforcement Division
California Privacy Protection Agency
Michael S. Macko, Deputy Director of Enforcement

**UNITED STATES OF AMERICA BEFORE THE FEDERAL TRADE
COMMISSION**

COMMISSIONERS: **Lina M. Khan, Chair**
 Rebecca Kelly Slaughter
 Christine S. Wilson
 Alvaro M. Bedoya

In the Matter of

DRIZLY, LLC, a Limited Liability

Company, and

**JAMES CORY RELLAS, individually, and as an
officer of DRIZLY, LLC.**

DOCKET NO. C-4780

COMPLAINT

The Federal Trade Commission (“FTC”), having reason to believe that Drizly, LLC, a limited liability company, and James Cory Rellas, individually and as an officer of Drizly, LLC (collectively “Respondents”), violated provisions of the Federal Trade Commission Act, 15 U.S.C. § 45(a)(1), and it appearing to the Commission that this proceeding is in the public interest, alleges:

1. Respondent Drizly, LLC (“Drizly”) is a Delaware limited liability company with its principal place of business at 501 Boylston Street, Boston, MA 02216. Until October 13, 2021, Drizly was a subsidiary of The Drizly Group, Inc., a holding company. On October 13, 2021, Drizly, LLC became a wholly-owned subsidiary of Uber Technologies, Inc. (“Uber”).
2. Respondent James Cory Rellas (“Rellas”), is the Chief Executive Officer (“CEO”) of Drizly, LLC. Individually or in concert with others, he had the authority to control, or participated in, the acts and practices alleged in this complaint.
3. Respondents’ acts and practices as alleged in this Complaint have been in or affecting commerce, as “commerce” is defined in Section 4 of the Federal Trade Commission Act.

Summary of the Case

4. Drizly failed to use appropriate information security practices to protect consumers’ personal information. These failures allowed a malicious actor to access Drizly’s consumer database and steal information relating to 2.5 million consumers, as described in greater detail below. Rellas is responsible for this failure, as he did not implement, or

properly delegate the responsibility to implement, reasonable information security practices. Indeed, as CEO of Drizly prior to and during the breach, Rellas hired senior executives dedicated to finance, legal, marketing, retail, human resources, product, and analytics, but failed to hire a senior executive responsible for the security of consumers' personal information collected and maintained by Drizly.

Drizly's Business Model and Operations

5. Drizly operates an e-commerce platform that enables local retailers to sell alcohol online to consumers of legal drinking age. Retailers choose the products to offer and the prices to charge on the platform. When a consumer places an order through Drizly's website or one of Drizly's mobile apps, the retailer accepts the order and facilitates delivery of the purchase.
6. Drizly's platform includes tools to verify a consumer's age; monitor, track, and analyze orders; and support customer service. The platform also collects and stores both personal information that consumers provide and information that it automatically obtains from consumers' computers and mobile devices.
7. Drizly was founded in 2012 and now has more than 360 employees. The company maintains a headquarters in Boston, Massachusetts and an office in Denver, Colorado. It advertises itself as North America's "largest online marketplace for alcohol," partnering with more than 4,000 retailers across 1,600 urban and suburban markets. Drizly claims that it facilitates sales of alcohol for delivery in more than 33 states and the District of Columbia. It also claims that its retail partners saw average growth in 2020 of 350%, with an average monthly number of orders of more than 230 per store.
8. Rellas has been Drizly's Chief Executive Officer since August 2018. He was previously Drizly's Chief Operating Officer and is a co-founder of Drizly. At all times relevant to the allegations in this Complaint, Rellas had the authority to control, or participated in, Drizly's information security practices.

Drizly's Information Technology Infrastructure

9. Drizly uses a third-party service called the Amazon Relational Database Service ("Amazon RDS") to host its production database environment (the software Drizly uses to operate its e-commerce platform). Amazon RDS is a cloud service provided by Amazon Web Services ("AWS").
10. Drizly's production environment includes a variety of applications and databases, some of which store personal information. These databases contain, among other things, names, email addresses, postal addresses, phone numbers, unique device identifiers, order histories, partial payment information, geolocation information, and consumer data (including, *e.g.*, income level, marital status, gender, ethnicity, existence of children, and home value) purchased from third parties. The databases also contain passwords that were hashed—converted into new values so as not to store the password itself in the database. The passwords were hashed using the bcrypt function or MD5, the latter of which is cryptographically broken, and widely considered insecure. This personal

information can be misused to facilitate identity theft and other consumer harm. Drizly's databases contain some or all of this personal information for more than 2.5 million consumers.

11. Drizly also uses the GitHub software platform ("GitHub") for the development, management, and storage of source code that supports the Drizly website and mobile apps. GitHub facilitates collaboration among developers, allowing them to store and share project files, including images, spreadsheets, and data sets, as well as the histories of all source code changes, in "repositories." Through its GitHub account, Drizly maintains a number of repositories that hold company data and projects, and which at one point improperly held AWS credentials, which could be used to access the company's production environment.
12. Drizly employees are required to use their personal GitHub accounts to access Drizly projects and data using GitHub, with the company granting those accounts access to its repositories.

Drizly's Information Security Practices

13. Drizly failed to use reasonable information security practices to protect consumers' personal information. Among other things, Drizly failed to:
 - a. Develop adequate written information security standards, policies, procedures, or practices; assess or enforce compliance with the written standards, policies, procedures, and practices that it did have; and implement training for employees (including engineers) regarding such standards, policies, procedures, and practices;
 - b. Securely store AWS and database login credentials, by including them in GitHub repositories, and failed to use readily available measures to scan these repositories for unsecured credentials (such as usernames, passwords, API keys, secure access tokens, and asymmetric private keys);
 - c. Impose reasonable data access controls such as: (1) requiring unique and complex passwords (*i.e.*, long passwords not used by the individual for any other online service) or multifactor authentication to access source code or databases; (2) enforcing role-based access controls; (3) monitoring and terminating employee and contractor access to source code once they no longer needed such access; (4) restricting inbound connections to known IP addresses; and (5) requiring appropriate authentications between Drizly applications and the production environment;
 - d. Prevent data loss by monitoring for unauthorized attempts to transfer or exfiltrate consumers' personal information outside the company's network boundaries; continually log and monitor its systems and assets to identify data security events; and perform regular assessments as to the effectiveness of protection measures;

- e. Test, audit, assess, or review its products' or applications' security features; and conduct regular risk assessments, vulnerability scans, and penetration testing of its networks and databases; and
- f. Have a policy, procedure, or practice for inventorying and deleting consumers' personal information stored on its network that was no longer necessary.

Drizly's Information Security Statements

- 14. Drizly made explicit representations about its information security practices that led consumers to believe that it used reasonable and appropriate information security practices to protect their personal information.
- 15. For example, Drizly's Privacy Policy in effect from September 1, 2016 until approximately October 1, 2019 included the following statement:

Security. All information we collect is securely stored within our database, and we use standard, industry-wide, commercially reasonable security practices such as 128-bit encryption, firewalls and SSL (Secure Socket Layers).

(Exhibit A, [Drizly.com](https://www.drizly.com/privacy-policy) Privacy Policy)

- 16. Drizly's Privacy Policy in effect after October 1, 2019 contained similar language:

Security. We use standard security practices such as encryption and firewalls to protect the information we collect from you.

(Exhibit B, [Drizly.com](https://www.drizly.com/privacy-policy) Privacy Policy)

2020 Breach of Personal Information

- 17. Drizly's failures, as described in Paragraph 13, led to a breach in or around July 2020 of its production environment, and the exfiltration of the personal information of 2.5 million consumers.
- 18. In April 2018, Drizly granted a company executive access to its GitHub repositories so that he could participate in a one-day hackathon (a collaborative programming event). Following the event, Drizly failed to monitor and terminate the executive's access, even though such access was no longer needed. The lack of need was underscored by the fact that the executive never accessed the repositories after the hackathon and started employment for a different Drizly subsidiary at the beginning of 2020.
- 19. Drizly failed to require unique and complex passwords or multifactor authentication for personal GitHub accounts that it granted access to its repositories, nor did it leverage Single Sign On for the GitHub organization. Consequently, the executive's GitHub account used a seven-character alphanumeric password that he had used for other personal accounts and did not use multifactor authentication although it was available.

20. In early July 2020, a malicious actor accessed the executive's GitHub account by reusing credentials from an unrelated breach. The malicious actor then used the executive's GitHub account to access one of Drizly's GitHub repositories containing source code, which it could use to find vulnerabilities in Drizly's software. It was also able to access, in those same repositories, AWS and database credentials.
21. Drizly employees stored these credentials in the company's GitHub repository even though GitHub security guidance and numerous publicly-reported security incidents since 2013 have highlighted the dangers of storing passwords and other access keys in GitHub repositories. For example, the Commission's 2018 Complaint against Uber Technologies Inc. specifically publicized and described credential reuse, lack of multifactor authentication, and insecure AWS credentials exposed through GitHub repository code as failures contributing to the breach and exposure of consumers' personal information.
22. The intruder used the compromised credentials from Drizly's GitHub repositories to modify the company's AWS security settings. This modification provided the intruder unfettered access to Drizly's production environment, including databases containing millions of records of user information. The intruder proceeded to exfiltrate Drizly's User Table, comprising more than 2.5 million records.
23. Drizly did not itself detect the breach of its production environment or discover the exfiltration of the personal information of nearly 2.5 million consumers. Drizly only learned of the breach from media and social media reports describing its customers' accounts for sale on dark web forums.
24. The GitHub compromise and breach of Drizly's production environment was not the company's first security incident involving GitHub. In 2018, another Drizly employee posted Drizly AWS credentials to their individual public (personal) GitHub repository. The employee was unable to delete the GitHub posting or rotate the AWS credentials prior to the public exploitation of the credentials; as a result, Drizly's AWS servers were used to mine cryptocurrency until Drizly learned of the exploitation and changed the credentials. Following this incident, Respondents were on notice of the potential dangers of exposing AWS credentials and should have taken appropriate steps to improve GitHub security, including implementation of policies, procedures, and technical measures to address the security practices of employees with access to Drizly's organizational GitHub repositories.
25. Drizly's own post-breach analyses concluded the company's lack of security preparedness, including failures to operate a formal security program or practice basic security hygiene, was exposed as a result of a data breach.

Consumer Injury

26. Respondents' failures to provide reasonable security for consumers' personal information have caused or are likely to cause substantial injury to consumers.
27. Consumers have suffered or are likely to suffer substantial injury in the form of increased exposure to fraud and identity theft, leading to monetary loss and time spent remedying

the problem. Personal information exfiltrated from Drizly's databases was offered for sale on two different, publicly-accessible dark web forums, including raidforums.com, a website where criminals post and offer for sale information from compromised databases. Malicious actors combine such information to perpetrate fraud (for example, by opening fraudulent lines of credit) or obtain additional personal information by impersonating companies with whom the target has previously transacted. The opening of fraudulent accounts will cause consumers financial harm in the form of denied transactions due to damaged credit reflected in consumer reports, and time lost in trying to correct those reports. Moreover, as a result of Respondents' failures to secure consumers' personal information, including in many cases their physical addresses, this information is now in the possession of criminals. Consumers are harmed when criminals know and sell their personal information.

28. These harms were not reasonably avoidable by consumers, as consumers had no way of independently knowing about Respondents' security failures (described in Paragraph 13 above).
29. Respondents could have prevented or mitigated the failures described in Paragraph 13 through well known, readily available, and relatively low-cost measures. For example, Drizly could have required regular review of access permissions, multifactor authentication for all employees with access to code repositories, or scanning of code repositories for unsecured credentials. Any of these measures would likely have prevented the July 2020 breach.

Violations of the FTC Act

30. The acts and practices of Respondents, as alleged in this Complaint, constitute unfair and/or deceptive acts or practices, in or affecting commerce, in violation of Section 5(a) of the Federal Trade Commission Act.

Count I – Drizly's Unfair Information Security Practices

31. As alleged in Paragraphs 13 to 29, Respondents' failure to employ reasonable security measures to protect consumers' personal information caused or is likely to cause substantial injury to consumers that is not outweighed by countervailing benefits to consumers or competition and is not reasonably avoidable by consumers themselves. This practice was, and is, an unfair act or practice.

Count II – Drizly's Deceptive Security Statements

32. Through the means described in Paragraphs 14 to 16, Respondents have represented, directly or indirectly, expressly or by implication, that Drizly used appropriate safeguards to protect consumers' personal information.
33. In truth and in fact, as described in Paragraph 13, Respondents did not maintain appropriate safeguards to protect consumers' personal information. Therefore, the representations set forth in Paragraph 32 are false or misleading.

THEREFORE, the Federal Trade Commission this 9th day of January, 2023, has issued this complaint against Respondents.

By the Commission.

April J. Tabor
Secretary

SEAL:

Exhibit A

[Drizly.com](#) Privacy Policy, September 1, 2016

Security. All information we collect is securely stored within our database, and we use standard, industry-wide, commercially reasonable security practices such as 128-bit encryption, firewalls and SSL (Secure Socket Layers). However, as effective as encryption technology is, no security system is impenetrable. We cannot guarantee the security of our database, nor can we guarantee that information you supply won't be intercepted while being transmitted to us over the Internet, and any information you transmit to Drizly you do so at your own risk. We recommend that you use unique numbers, letters and special characters in your password and not disclose your password to anyone. If you do share your password or personal information with others, you are responsible for all actions taken in the name of your account. Please review our [Terms of Service](#) for additional information. If your password has been compromised for any reason, you should immediately notify Drizly at info@drizly.com and change your password.

Exhibit B

[Drizly.com](https://www.drizly.com/privacy-policy) Privacy Policy, October 1, 2019

Security. We use standard security practices such as encryption and firewalls to protect the information we collect from you. No security system is perfect, and we do not guarantee the security of your information. You are responsible for all actions taken in the name of your account, so use your discretion when providing information and managing your account. Use unique numbers, letters and special characters in your password and do not disclose it to anyone. Please review our [Terms of Service](#) for additional information. If your password is compromised notify us immediately [at info@drizly.com](mailto:info@drizly.com) and change your password. We may store the information we collect on servers in the United States.

**UNITED STATES OF AMERICA
BEFORE THE FEDERAL TRADE COMMISSION**

COMMISSIONERS: **Lina M. Khan, Chair
Rebecca Kelly Slaughter
Christine S. Wilson
Alvaro M. Bedoya**

In the Matter of

DECISION AND ORDER

**DRIZLY, LLC, a Limited Liability Company,
and**

DOCKET NO. C-4780

**JAMES CORY RELLAS, individually, and as an
officer of DRIZLY, LLC.**

DECISION

The Federal Trade Commission (“Commission”) initiated an investigation of certain acts and practices of the Respondents named in the caption. The Commission’s Bureau of Consumer Protection (“BCP”) prepared and furnished to Respondents a draft Complaint. BCP proposed to present the draft Complaint to the Commission for its consideration. If issued by the Commission, the draft Complaint would charge the Respondents with violations of the Federal Trade Commission Act, 15 U.S.C. § 45(a)(1).

Respondents and BCP thereafter executed an Agreement Containing Consent Order (“Consent Agreement”). The Consent Agreement includes: (1) statements by Respondents that they neither admit nor deny any of the allegations in the draft Complaint, except as specifically stated in this Decision and Order, and that only for purposes of this action, they admit the facts necessary to establish jurisdiction; and (2) waivers and other provisions as required by the Commission’s Rules.

The Commission considered the matter and determined that it had reason to believe that Respondents have violated the Federal Trade Commission Act, and that a Complaint should issue stating its charges in that respect. The Commission accepted the executed Consent Agreement and placed it on the public record for a period of 30 days for the receipt and consideration of public comments. The Commission duly considered any comments received from interested persons pursuant to Section 2.34 of its Rules, 16 C.F.R. § 2.34. Now, in further

conformity with the procedure prescribed in Rule 2.34, the Commission issues its Complaint, makes the following Findings, and issues the following Order:

Findings

1. The Respondents are:
 - a. Respondent Drizly, LLC (“Drizly”), a Delaware Limited Liability Company with its principal office or place of business at 501 Boylston Street, Boston, MA 02216.
 - b. Respondent James Cory Rellas, an officer of Corporate Respondent, Drizly, LLC. Individually or in concert with others, he formulates, directs, or controls the policies, acts, or practices of Drizly, LLC. His principal office or place of business is the same as that of Drizly, LLC.
2. The Commission has jurisdiction over the subject matter of this proceeding and over Respondents, and the proceeding is in the public interest.

ORDER

Definitions

For purposes of this Order, the following definitions apply:

1. **“Covered Business”** means: (1) Corporate Respondent; and (2) any business that Corporate Respondent controls, directly or indirectly.
2. **“Corporate Respondent”** means Drizly, LLC, and its successors and assigns.
3. **“Covered Incident”** means any incident that results in a Covered Business notifying, pursuant to a statutory or regulatory requirement, any U.S. federal, state, or local government entity that information of or about an individual consumer was, or is reasonably believed to have been, accessed, acquired, or publicly exposed without authorization.
4. **“Covered Information”** means information from or about an individual consumer, including: (a) a first and last name; (b) a home or physical address; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a mobile or other telephone number; (e) a driver’s license or other government-issued identification number; (f) date of birth; (g) Geolocation information sufficient to identify street name and name of a city or town; (h) credit or debit card information (including a partial credit or debit card number); (i) User identifier, or other persistent identifier that can be used to recognize a User over time and across different devices, websites, or online services; or (j) User account credentials, such as a login name and password (whether plain text, encrypted, hashed, and/or salted).

5. **“Delete” “Deleted” or “Deletion”** means to remove Covered Information such that it is not maintained in retrievable form and cannot be retrieved in the normal course of business.
6. **“Individual Respondent”** means James Cory Rellas.
7. **“Relevant Business”** means any business other than a Covered Business that collects, uses, discloses, or stores Covered Information from 25,000 or more individual consumers.
8. **“Respondents”** means the Corporate Respondent and the Individual Respondent, individually, collectively, or in any combination.
9. **“User”** means an individual consumer from whom Covered Business has obtained information for the purpose of providing access to a Respondent’s products and services.

Provisions

I. Prohibition Against Misrepresentations

IT IS ORDERED that Corporate Respondent and Corporate Respondent’s officers, agents, employees, and attorneys, and all other persons in active concert or participation with any of them, who receive actual notice of this Order, whether acting directly or indirectly, in connection with any product or service, must not misrepresent in any manner, expressly or by implication:

- A. The extent to which Corporate Respondent collects, uses, discloses, maintains, Deletes, or permits or denies access to any Covered Information;
- B. The extent to which Corporate Respondent otherwise protects the privacy, security, availability, confidentiality, or integrity of any Covered Information; or
- C. The extent of any Covered Incident or unauthorized disclosure, misuse, loss, theft, alteration, destruction, or other compromise of Covered Information.

II. Mandated Deletion and Data Minimization

IT IS FURTHER ORDERED that Corporate Respondent must:

- A. Within 60 days after the issuance date of this Order, Delete or destroy all Covered Information that is not being used or retained in connection with providing products or services to Corporate Respondent’s customers, and provide a written statement to the Commission, pursuant to the Provision entitled Compliance Report and Notices, confirming that all such data has been Deleted or destroyed specifically enumerating which types of information were Deleted or destroyed; and

- B. Refrain from collecting or maintaining any Covered Information not necessary for the specific purpose(s) provided in the retention schedule required under Provision III entitled Data Retention Limits.

Provided, however, that any data that Corporate Respondent is required to Delete or destroy pursuant to this Provision may be retained if required by law, regulation, court order, contractual obligations requiring Corporate Respondent to maintain records on behalf of retailers to document the retailers' compliance with state or local liquor regulations, or legal process, including as required by rules applicable to the safeguarding of evidence in pending litigation.

III. Data Retention Limits

IT IS FURTHER ORDERED that Corporate Respondent, in connection with the collection, maintenance, use, or disclosure of, or provision of access to, Covered Information, must:

- A. Within 60 days of issuance of this Order, document, adhere to, and make publicly available on its website(s) or app(s), a retention schedule for Covered Information, setting forth: (1) the purpose or purposes for which each type of Covered Information is collected; (2) the specific business needs for retaining each type of Covered Information; and (3) a set timeframe for Deletion of each type of Covered Information that precludes indefinite retention of any Covered Information; and
- B. Within 60 days after the issuance date of this Order, Corporate Respondent shall provide a written statement to the Commission, pursuant to the Provision entitled Compliance Report and Notices, describing the retention schedule for Covered Information made publicly available on its website(s) or app(s); and
- C. Prior to collecting any new type of information related to consumers that was not being collected as of the issuance date of this Order, and is not described in retention schedules published in accordance with sub-Provision A of this Provision entitled Data Retention Limits, Corporate Respondent must update its retention schedule setting forth: (1) the purpose or purposes for which the new information is collected; (2) the specific business needs for retaining the new information; and (3) a set timeframe for Deletion of the new information that precludes indefinite retention.

IV. Mandated Information Security Program for Covered Businesses

IT IS FURTHER ORDERED that Corporate Respondent and any business that Corporate Respondent controls, directly or indirectly, in connection with the collection, maintenance, use, or disclosure of, or provision of access to, Covered Information, must each, within 60 days of the effective date of this Order, establish and implement, and thereafter maintain, a comprehensive information security program ("Information Security Program") that protects the security, confidentiality, and integrity of such Covered Information. To satisfy this requirement, each Covered Business must, at a minimum:

- A. Document in writing the content, implementation, and maintenance of the Information Security Program;
- B. Provide the written Information Security Program and any evaluations thereof or updates thereto to any Covered Business' board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer of the Covered Business responsible for the business' Information Security Program at least once every 12 months and promptly (not to exceed 30 days) after a Covered Incident;
- C. Designate a qualified employee or employees to coordinate and be responsible for the Information Security Program;
- D. Assess and document, at least once every 12 months and promptly (not to exceed 30 days) following a Covered Incident, internal and external risks to the security, confidentiality, or integrity of Covered Information that could result in the (1) unauthorized collection, maintenance, alteration, use, disclosure of, or provision of access to, Covered Information; or the (2) misuse, loss, theft, alteration, destruction, or other compromise of such information;
- E. Design, implement, maintain, and document safeguards that control for the internal and external risks Covered Businesses identify to the security, confidentiality, or integrity of Covered Information identified in response to sub-Provision D of the Provision entitled Mandated Information Security Program for Covered Businesses. Each safeguard must be based on the volume and sensitivity of the Covered Information that is at risk, and the likelihood that the risk could be realized and result in the (1) unauthorized collection, maintenance, use, disclosure of, or provision of access to, Covered Information; or the (2) misuse, loss, theft, alteration, destruction, or other compromise of such information. Such safeguards must also include:
 - 1. A written information security policy and accompanying written standards and procedures that describe, at a minimum: (a) how each Covered Business implements each of the safeguards identified in this sub-Provision; and (b) how each Covered Business assesses and enforces compliance with these safeguards and any other controls it identifies in the policy and accompanying standards and procedures;
 - 2. Standards, procedures, and policy provisions mandating security education that address internal or external risks each Covered Business identifies under sub-Provision D of this Provision, and that includes, at a minimum: (a) training for each Covered Business' employees about each Covered Business' security policy, standards, and procedures, including the requirements of this Order and the process for submitting complaints and concerns, to be conducted when an employee begins employment or takes on a new role, and on at least an annual basis thereafter; and (b) training in secure software development principles, including secure engineering and defensive programming concepts, for developers, engineers, system administrators, and other employees that design,

implement, and operate a Covered Business' products or services or that are otherwise responsible for the security of Covered Information;

3. Technical measures, standards, procedures, and policy provisions to prevent the storage of unsecured access keys or other unsecured credentials on a Covered Business' network or in any cloud-based services;
4. Policy provisions and, to the extent possible, technical measures requiring employees, contractors, or third parties to secure any accounts with access to a Covered Business' information technology infrastructure by: (a) using strong, unique passwords; and (b) using multi-factor authentication whenever available;
5. Requiring multi-factor authentication methods for all employees, contractors, and affiliates in order to access any assets (including databases) storing Covered Information. Such multi-factor authentication methods for all employees, contractors, and affiliates shall not include telephone or SMS-based authentication methods and must be resistant to phishing attacks. A Covered Business may use widely-adopted industry authentication options that provide at least equivalent security as the multi-factor authentication options required by this sub-provision, if approved in writing by the Commission;
6. Requiring multi-factor authentication methods be provided as an option for consumers. Any information collected from consumers at the time they select to use multi-factor authentication may only be used for authentication purposes and no other purpose;
7. Technical measures, standards, procedures, and policy provisions to: (a) log and monitor access to repositories of Covered Information in the control of a Covered Business; (b) limit access to Covered Information by, at a minimum, limiting employee and service provider access to what is needed to perform that employee's or service provider's job function; (c) grant and audit varying levels of access based on an employee's need to know; and (d) periodically monitor and terminate employee and contractor accounts following inappropriate usage or termination of employment;
8. Technical measures, standards, procedures, and policy provisions to control data access for all assets (including databases) containing Covered Information or resources containing proprietary (*i.e.*, non-open source) source code repositories, including, at a minimum: (a) restrictions of inbound connections to those originating from approved IP addresses; (b) requiring connections to be authenticated and encrypted; and (c) periodic audits of account permissions;
9. Technical measures, standards, procedures, and policy provisions to: (a) monitor and log transfers or exfiltration of Covered Information outside each Covered Business' network boundaries; (b) monitor and log data security events and other anomalous activity; and (c) verify the effectiveness of monitoring and logging;

10. Technical measures to safeguard against unauthorized access, including: (a) an intrusion prevention or detection system; (b) file integrity monitoring tools; (c) data loss prevention tools; (d) properly configured firewalls; and (e) properly configured physical or logical segmentation of networks, systems, and databases;
 11. Technical measures, standards, procedures, and policy provisions to assess the risk posed by source code to Covered Information stored on any Covered Business' network or other assets, including, at least once every 12 months and promptly (not to exceed 30 days) after a Covered Incident involving a vulnerability related to Respondent's source code: (a) software code review; and (b) penetration testing of each Covered Business' software; and
 12. Technical measures, procedures, and policy provisions to systematically inventory Covered Information in each Covered Business' control and Delete Covered Information that is no longer necessary;
- F. Assess, at least once every 12 months and promptly (not to exceed 30 days) following a Covered Incident, the sufficiency of any safeguards in place to address the risks to the security, confidentiality, or integrity of Covered Information, and modify the Information Security Program based on the results;
- G. Test and monitor the effectiveness of the safeguards in place at least once every 12 months and promptly (not to exceed 30 days) following a Covered Incident, and modify the Information Security Program based on the results. Such testing and monitoring must include: (1) vulnerability testing of each Covered Business' network and applications once every 4 months and promptly (not to exceed 30 days) after a Covered Incident; and (2) penetration testing of each Covered Business' network(s) and applications at least once every 12 months and promptly (not to exceed 30 days) after a Covered Incident;
- H. Select and retain service providers capable of safeguarding Covered Information they access through or receive from each Covered Business, and contractually require service providers to implement and maintain safeguards sufficient to address the internal and external risks to the security, confidentiality, or integrity of Covered Information; and
- I. Evaluate and adjust the Information Security Program in light of any changes to a Covered Business' operations or business arrangements, a Covered Incident, new or more efficient technological or operational methods to control for the risks identified in sub-Provision D of the Provision entitled Mandated Information Security Program for Covered Businesses, or any other circumstances that a Covered Business or its officers, agents, or employees know or have reason to know may have an impact on the effectiveness of the Information Security Program or any of its individual safeguards. At a minimum, each Covered Business must evaluate the Information Security Program at least once every 12 months and modify the Information Security Program based on the results.

V. Third Party Information Security Assessments for Covered Businesses

IT IS FURTHER ORDERED that, in connection with compliance with the Provision entitled Mandated Information Security Program for Covered Businesses, Corporate Respondent must obtain initial and biennial assessments (“Assessments”):

- A. The Assessments must be obtained from a qualified, objective, independent third-party professional (“Assessor”), who: (1) uses procedures and standards generally accepted in the profession; (2) conducts an independent review of the Information Security Program; and (3) retains all documents relevant to each Assessment for 5 years after completion of such Assessment and will provide such documents to the Commission within 10 days of receipt of a written request from a representative of the Commission. No documents may be withheld by the Assessor on the basis of a claim of confidentiality, proprietary or trade secrets, work product protection, attorney-client privilege, statutory exemption, or any similar claim.
- B. For each Assessment, Corporate Respondent must provide the Associate Director for Enforcement for the Bureau of Consumer Protection at the Federal Trade Commission with the name, affiliation, and qualifications of the proposed Assessor, whom the Associate Director shall have the authority to approve in their sole discretion.
- C. The reporting period for the Assessments must cover: (1) the first 180 days after the Mandated Information Security Program for Covered Businesses required by Provision IV of this Order has been put in place for the initial Assessment; and (2) each two-year period thereafter for 20 years after issuance of the Order for the biennial Assessments.
- D. Each Assessment must, for the entire assessment period:
 - 1. Determine whether Corporate Respondent has implemented and maintained the Information Security Program required by the Provision entitled Mandated Information Security Program for Covered Businesses;
 - 2. Assess the effectiveness of Corporate Respondent’s implementation and maintenance of sub-Provisions A-I of the Provision entitled Mandated Information Security Program for Covered Businesses;
 - 3. Identify any gaps or weaknesses in, or instances of material noncompliance with, the Information Security Program;
 - 4. Address the status of gaps or weaknesses in, or instances of material non-compliance with, the Information Security Program that were identified in any prior Assessment required by this Order; and
 - 5. Identify specific evidence (including, but not limited to, documents reviewed, sampling and testing performed, and interviews conducted) examined to make such determinations, assessments, and identifications, and explain why the evidence that the Assessor examined is (a) appropriate for assessing an enterprise

of the business's size, complexity, and risk profile; and (b) sufficient to justify the Assessor's findings. No finding of any Assessment shall rely primarily on assertions or attestations by Corporate Respondent's management. The Assessment must be signed by the Assessor, state that the Assessor conducted an independent review of the Information Security Program and did not rely primarily on assertions or attestations by Corporate Respondent's management, and state the number of hours that each member of the assessment team worked on the Assessment. To the extent Corporate Respondent revises, updates, or adds one or more safeguards required under the Provision entitled Mandated Information Security Program for Covered Businesses in the middle of an Assessment period, the Assessment must assess the effectiveness of the revised, updated, or added safeguard(s) for the time period in which it was in effect, and provide a separate statement detailing the basis for each revised, updated, or additional safeguard.

- E. Each Assessment must be completed within 60 days after the end of the reporting period to which the Assessment applies. Unless otherwise directed by a Commission representative in writing, Corporate Respondent must submit an unredacted copy of the initial Assessment and a proposed redacted copy suitable for public disclosure of the initial Assessment to the Commission within 10 days after the Assessment has been completed via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, "*In re* Drizly, LLC and James Cory Rellas, FTC File No. 2023185." Corporate Respondent must retain an unredacted copy of each subsequent biennial Assessment as well as a proposed redacted copy of each subsequent biennial Assessment suitable for public disclosure until the Order is terminated and must provide each such Assessment to the Associate Director for Enforcement within ten (10) days of request. The initial Assessment and any subsequent biennial Assessment provided to the Commission must be marked, in the upper right-hand corner of each page, with the words "DPIP Assessment" in red lettering.

VI. Cooperation with Third-Party Information Security Assessor

IT IS FURTHER ORDERED that Respondents, whether acting directly or indirectly, in connection with any Assessment required by the Provision entitled Third Party Information Security Assessments for Covered Businesses must:

- A. Provide or otherwise make available to the Assessor all information and material in their possession, custody, or control that is relevant to the Assessment for which there is no reasonable claim of privilege;
- B. Provide or otherwise make available to the Assessor information about Corporate Respondent's networks and all of Corporate Respondent's information technology assets so that the Assessor can determine the scope of the Assessment, and visibility to those portions of the networks and information technology assets deemed in scope; and

- C. Disclose all material facts to the Assessor, and not misrepresent in any manner, expressly or by implication, any fact material to the Assessor's: (1) determination of whether Corporate Respondent has implemented and maintained the Mandated Information Security Program for Covered Businesses; (2) assessment of the effectiveness of the Corporate Respondent's implementation and maintenance of sub-Provisions A-I of the required Mandated Information Security Program for Covered Businesses; or (3) identification of any gaps or weaknesses in, or instances of material noncompliance with, the Mandated Information Security Program for Covered Businesses.

VII. Mandated Information Security Program for Certain Businesses of the Individual Respondent

IT IS FURTHER ORDERED that, for 10 years after issuance of this Order, Individual Respondent, for any Relevant Business that he is: 1) majority owner; or 2) employed or functions as a Chief Executive Officer or other senior officer with direct or indirect responsibility for information security, must within 180 days ensure that the business has established and implemented, and thereafter maintains, a comprehensive information security program ("Business ISP") that protects the security, confidentiality, and integrity of Covered Information. To satisfy this requirement, Individual Respondent must ensure that each Relevant Business, at a minimum:

- A. Documents in writing the content, implementation, and maintenance of the Business ISP;
- B. Provides the written Business ISP and any evaluations thereof or updates thereto to any Relevant Business's board of directors or governing body or, if no such board or equivalent governing body exists, to a senior officer of the Relevant Business responsible for the Business ISP at least once every 12 months;
- C. Designates a qualified employee or employees to coordinate and be responsible for the Business ISP;
- D. Assesses and documents, at least once every 12 months, internal and external risks to the security, confidentiality, or integrity of Covered Information that could result in the (1) unauthorized collection, maintenance, alteration, use, disclosure of, or provision of access to, Covered Information; or the (2) misuse, loss, theft, destruction, or other compromise of such information;
- E. Designs, implements, maintains, and documents safeguards that control for the internal and external risks to the security, confidentiality, or integrity of Covered Information identified in response to sub-Provision D of this provision entitled Mandated Information Security Program for Certain Businesses of the Individual Respondent. Each safeguard must be based on the volume and sensitivity of the Covered Information that is at risk, and the likelihood that the risk could be realized and result in the (1) unauthorized collection, maintenance, use, disclosure of, or provision of access to, Covered Information; or the (2) misuse, loss, theft, alteration, destruction, or other compromise of such information;

- F. Assesses, at least once every 12 months, the sufficiency of any safeguards in place to address the risks to the security, confidentiality, or integrity of Covered Information, and modify the Business ISP based on the results;
- G. Tests and monitors the effectiveness of the safeguards in place at least once every 12 months, and modifies the Business ISP based on the results. Such testing and monitoring must include: (1) vulnerability testing of the Relevant Business's network and applications once every 4 months; and (2) penetration testing of the Relevant Business's network(s) and applications at least once every 12 months;
- H. Selects and retains service providers capable of safeguarding Covered Information they access through or receive from the Relevant Business, and contractually require service providers to implement and maintain safeguards sufficient to address the internal and external risks to the security, confidentiality, or integrity of Covered Information; and
- I. Evaluates and adjusts the Business ISP in light of any changes to the Relevant Business's operations or business arrangements, new or more efficient technological or operational methods to control for the risks identified in sub-Provision D of this provision entitled Mandated Information Security Program for Certain Businesses of the Individual Respondent, or any other circumstances that Individual Respondent or the Relevant Business know or have reason to know may have an impact on the effectiveness of the Business ISP or any of its individual safeguards. At a minimum, each Relevant Business must evaluate the Business ISP at least once every 12 months and modify the Business ISP based on the results.

VIII. Annual Certification

IT IS FURTHER ORDERED that Corporate Respondent must:

- A. One year after the issuance date of this Order, and each year thereafter, provide the Commission with a certification from Corporate Respondent's Chief Executive Officer, James Cory Rellas, or if Mr. Rellas no longer serves as Corporate Respondent's Chief Executive Officer, President, or such other officer (regardless of title) that is designated in Corporate Respondent's Bylaws or resolution of the Board of Directors as having the duties of the principal executive officer of Corporate Respondent, then a senior corporate manager, or, if no such senior corporate manager exists, a senior officer responsible for Corporate Respondent's Information Security Program that: (1) each Covered Business has established, implemented, and maintained the requirements of this Order; (2) each Covered Business is not aware of any material noncompliance that has not been (a) corrected or (b) disclosed to the Commission; and (3) includes a brief description of all Covered Incidents that Corporate Respondent verified or confirmed during the certified period. The certification must be based on the personal knowledge of Mr. Rellas, the senior corporate manager, senior officer, or subject matter experts upon whom Mr. Rellas, the senior corporate manager, or senior officer reasonably relies in making the certification.

- B. Unless otherwise directed by a Commission representative in writing, submit all annual certifications to the Commission pursuant to this Order via email to DEbrief@ftc.gov or by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, “*In re* Drizly, LLC and James Cory Rellas, FTC File No. 2023185.”

IX. Covered Incident Reports

IT IS FURTHER ORDERED that, within 10 days of any notification to a United States federal, state, or local entity of a Covered Incident, each Covered Business must submit a report to the Commission. The report must include, to the extent possible:

- A. The date, estimated date, or estimated date range when the Covered Incident occurred;
- B. A description of the facts relating to the Covered Incident, including the causes and scope of the Covered Incident, if known;
- C. A description of each type of information that was affected by the Covered Incident;
- D. The number of consumers whose information was affected by the Covered Incident;
- E. The acts that each Covered Business has taken to date to remediate the Covered Incident and protect Covered Information from further exposure or access, and protect affected individuals from identity theft or other harm that may result from the Covered Incident; and
- F. A representative copy of each materially different notice sent by each Covered Business to consumers or to any U.S. federal, state, or local government entity regarding the Covered Incident.

Unless otherwise directed by a Commission representative in writing, all Covered Incident reports to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin, “*In re* Drizly, LLC and James Cory Rellas, FTC File No. 2023185.”

X. Acknowledgments of the Order

IT IS FURTHER ORDERED that Respondents obtain acknowledgments of receipt of this Order:

- A. Each Respondent, within 10 days after the effective date of this Order, must submit to the Commission an acknowledgment of receipt of this Order sworn under penalty of perjury.

- B. For 10 years after the issuance date of this Order, Individual Respondent for any business that such Respondent, individually or collectively with any other Respondent is the majority owner or controls, directly or indirectly, and Corporate Respondent must deliver a copy of this Order to: (1) all principals, officers, directors, and LLC managers and members; (2) all employees, agents, and representatives with managerial responsibilities for a Covered Business' data security, collection of consumer information, and decision-making about the use of consumer information; (3) the employee(s) having primary responsibility for a Relevant Business' data security, collection of consumer information, and decision-making about the use of consumer information; and (4) any business entity resulting from any change in structure as set forth in the Provision titled Compliance Report and Notices. Delivery must occur within 10 days after the effective date of this Order for current personnel. For all others, delivery must occur before they assume their responsibilities.
- C. From each individual or entity to which Respondents delivered a copy of this Order, Respondents must obtain, within 30 days, a signed and dated acknowledgment of receipt of this Order.

XI. Compliance Report and Notices

IT IS FURTHER ORDERED that Respondents make timely submissions to the Commission:

- A. One year after the issuance date of this Order, each Respondent must submit a compliance report, sworn under penalty of perjury, in which:
1. Each Respondent must: (a) identify the primary physical, postal, and email address and telephone number, as designated points of contact, which representatives of the Commission, may use to communicate with Respondent; (b) identify all of that Respondent's businesses by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; (c) describe the activities of each business, including the goods and services offered, the means of advertising, marketing, and sales, and the involvement of any other Respondent (which Individual Respondent must describe if they know or should know due to their own involvement); (d) describe in detail whether and how that Respondent is in compliance with each Provision of this Order, including a discussion of all of the changes the Respondent made to comply with the Order; and (e) provide a copy of each Acknowledgment of the Order obtained pursuant to this Order, unless previously submitted to the Commission.
 2. Additionally, Individual Respondent must: (a) identify all their telephone numbers and all their physical, postal, email and Internet addresses, including all residences; (b) identify all their business activities, including any business for which such Respondent performs services whether as an employee or otherwise and any entity in which such Respondent has any ownership interest; (c) describe in detail such Respondent's involvement in each such business activity, including

title, role, responsibilities, participation, authority, control, and any ownership; and (d) explain whether or not any business identified in sub-part (b) is a Relevant Business.

- B. Each Respondent must submit a compliance notice, sworn under penalty of perjury, within 14 days of any change in the following:
1. Each Respondent must submit notice of any change in: (a) any designated point of contact; or (b) the structure of Corporate Respondent or any entity that Respondent has any ownership interest in or controls directly or indirectly that may affect compliance obligations arising under this Order, including: creation, merger, sale, or dissolution of the entity or any subsidiary, parent, or affiliate that engages in any acts or practices subject to this Order.
 2. Additionally, Individual Respondent must submit notice of any change in: (a) name, including alias or fictitious name, or residence address; or (b) title or role in any business activity, including (i) any business for which Respondent performs services whether as an employee or otherwise and (ii) any entity in which Respondent has any ownership interest and over which Respondent has direct or indirect control. For each such business, also identify its name, physical address, any Internet address, and whether or not it is a Relevant Business.
- C. Each Respondent must submit notice of the filing of any bankruptcy petition, insolvency proceeding, or similar proceeding by or against such Respondent within 14 days of its filing.
- D. Any submission to the Commission required by this Order to be sworn under penalty of perjury must be true and accurate and comply with 28 U.S.C. § 1746, such as by concluding: “I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on: _____” and supplying the date, signatory’s full name, title (if applicable), and signature.
- E. Unless otherwise directed by a Commission representative in writing, all submissions to the Commission pursuant to this Order must be emailed to DEbrief@ftc.gov or sent by overnight courier (not the U.S. Postal Service) to: Associate Director for Enforcement, Bureau of Consumer Protection, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580. The subject line must begin: *In re* Drizly, LLC and James Cory Rellas, FTC File No. 2023185.

XII. Recordkeeping

IT IS FURTHER ORDERED that Respondents must create certain records for 20 years after the issuance date of the Order, and retain each such record for 5 years, unless otherwise specified below. Specifically, Corporate Respondent and Individual Respondent for any business that such Respondent, individually or collectively with any other Respondents, is a

majority owner or controls directly or indirectly must create and retain the following records:

- A. Accounting records showing the revenues from all goods or services sold, the costs incurred in generating those revenues, and resulting net profit or loss;
- B. Personnel records showing, for each person providing services in relation to any aspect of the Order, whether as an employee or otherwise, that person's: name, addresses, telephone numbers, job title or position, dates of service, and (if applicable) the reason for termination;
- C. Copies or records of all consumer complaints related to information security, privacy, or identity theft whether received directly or indirectly by Corporate Respondent, such as through a third party, and any response;
- D. A copy of each unique advertisement or other marketing material of Corporate Respondent containing a representation subject to this Order;
- E. A copy of each widely disseminated and materially different representation by Corporate Respondent that describes the extent to which Corporate Respondent maintains or protects the privacy, security, availability, confidentiality, or integrity of any Covered Information, including any representation concerning a change in any website or other service controlled by Corporate Respondent that relates to privacy, security, availability, confidentiality, or integrity of Covered Information;
- F. For 5 years after the date of preparation of each Assessment required by this Order, all materials and evidence that the Assessor considered, reviewed, relied upon or examined to prepare the Assessment, whether prepared by or on behalf of Respondents, including all plans, reports, studies, reviews, audits, audit trails, policies, training materials, and assessments, and any other materials concerning Respondents' compliance with related Provisions of this Order, for the compliance period covered by such Assessment;
- G. For 5 years from the date received, copies of all subpoenas and other communications with law enforcement, if such communications relate to Respondents' compliance with this Order;
- H. For 5 years from the date created or received, all records, whether prepared by or on behalf of Respondents, that tend to show any lack of compliance by Respondents with this Order; and
- I. All records necessary to demonstrate full compliance with each Provision of this Order, including all submissions to the Commission.

XIII. Compliance Monitoring

IT IS FURTHER ORDERED that, for the purpose of monitoring Respondents'

compliance with this Order:

- A. Within 10 days of receipt of a written request from a representative of the Commission, Respondents must: submit additional compliance reports or other requested information, which must be sworn under penalty of perjury, and produce records for inspection and copying.
- B. For matters concerning this Order, representatives of the Commission are authorized to communicate directly with Respondents. Respondents must permit representatives of the Commission to interview anyone affiliated with Respondents who has agreed to such an interview. The interviewee may have counsel present.
- C. The Commission may use all other lawful means, including posing through its representatives as consumers, suppliers, or other individuals or entities, to Respondents or any individual or entity affiliated with Respondents, without the necessity of identification or prior notice. Nothing in this Order limits the Commission's lawful use of compulsory process, pursuant to Sections 9 and 20 of the FTC Act, 15 U.S.C. §§ 49, 57b-1.

XIV. Order Effective Dates

IT IS FURTHER ORDERED that this Order is final and effective upon the date of its publication on the Commission's website ([ftc.gov](https://www.ftc.gov)) as a final order. This Order will terminate 20 years from the date of its issuance, (which date may be stated at the end of this Order, near the Commission's seal), or 20 years from the most recent date that the United States or the Commission files a complaint (with or without an accompanying settlement) in federal court alleging any violation of this Order, whichever comes later; *provided, however*, that the filing of such a complaint will not affect the duration of:

- A. Any Provision in this Order that terminates in less than 20 years;
- B. This Order's application to any Respondent that is not named as a defendant in such complaint; and
- C. This Order if such complaint is filed after the Order has terminated pursuant to this Provision.

Provided, further, that if such complaint is dismissed or a federal court rules that the Respondents did not violate any provision of the Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Order will terminate according to this Provision as though the complaint had never been filed, except that the Order will not terminate between the date such complaint is filed and the later of the deadline for appealing such dismissal or ruling and the date such dismissal or ruling is upheld on appeal.

By the Commission.

April J. Tabor
Secretary

SEAL:
ISSUED: January 9, 2023

EV + AI Panel – CLE Resources

Page 17 of 17

The background of the slide features a stylized globe with a grid of latitude and longitude lines. The globe is composed of a dense pattern of small, glowing blue and red dots. A network of thin, white lines connects these dots, creating a web-like structure that suggests global connectivity and data flow. The overall color palette is dark blue and black, with highlights of red and white.

Global AI Law and Policy Tracker

By IAPP Research and Insights

Countries worldwide are designing and implementing AI governance legislation and policies commensurate to the velocity and variety of proliferating AI-powered technologies. Efforts include the development of comprehensive legislation, focused legislation for specific use cases, national AI strategies or policies, and voluntary guidelines and standards. There is no standard approach toward bringing AI under state regulation, however, common patterns toward reaching the goal of AI regulation can be observed. Given the transformative nature of AI technology, the challenge for jurisdictions is to find a balance between innovation and regulation of risks. Therefore, governance of AI often, if not always, begins with a jurisdiction rolling out a national strategy or ethics policy instead of legislating from the get-go.

This pattern is evident throughout this tracker. The tracker identifies legislative or policy developments or both in a subset of jurisdictions. Such initiatives are either already being deliberated at the country level or are in the process of commencing deliberations in countries across six continents, speaking to the global importance of AI. However, given the rapid and widespread policymaking in this space, the tracker does not include all AI initiatives within every jurisdiction across every continent. This tracker also offers brief commentary on the broader AI context and related developments and identifies laws or policies in parallel professions like privacy.

As individual jurisdictions press ahead with their own frameworks and approaches, they have also doubled down on multilateral efforts to coordinate and cohere different approaches. The Organisation for Economic Co-operation and Development's AI principles have been reaffirmed in many different contexts, including by digital and technology ministers of the G7 countries during the 2023 Hiroshima Summit. UNESCO, the International Organization for Standardization, the African Union and the Council of Europe are all working on multilateral AI governance frameworks. The U.K. government organized the first AI Safety Summit in 2023 for government and industry stakeholders to agree upon, evaluate and monitor the most significant risks from AI.

Tracking, unpacking and governing the complex field of global AI governance law and policy has quickly become a top-tier strategic issue for organizations. The [IAPP AI Governance Center](#) will continue to provide AI governance professionals with the content, resources, networking, training and certification needed to respond to the field's complex risks. The IAPP AI Global Law and Policy Tracker has been updated with valuable input from the global community of AI governance professionals, and we continue to welcome feedback and insights from this community.

Global AI Law and Policy Tracker





This map shows which jurisdictions are in focus and covered by this tracker. It does not represent the extent to which jurisdictions around the world are active on AI governance legislation.


Jurisdictions in focus


Argentina • Australia • Bangladesh • Brazil • Canada • Chile • China • Colombia • Egypt • EU • India • Indonesia • Israel
Japan • Mauritius • New Zealand • Peru • Saudi Arabia • Singapore • South Korea • Taiwan • United Arab Emirates • U.K. • U.S.


**Click on the country names above to navigate to its location in the tracker.*


	Specific AI governance law or policy	Relevant authorities	Other relevant laws and policies	Wider AI context
ARGENTINA	<p>Argentina has made policy initiatives on AI. It has developed a draft of a National AI Plan to help facilitate the use and development of AI in the country.</p> <p>Under Resolution 2/2023, Argentina released recommendations for trustworthy and reliable AI directed to the public sector.</p>	<ul style="list-style-type: none"> → National Big Data Observatory → Ministry of Science, Technology and Productive Innovation → National Committee for Ethics in Science and Technology → Undersecretariat of Information and Communication Technologies → Agency of Access to Public Information → National Securities Commission 	<ul style="list-style-type: none"> → National Cybersecurity Strategy [IN FORCE] → Personal Data Act [DRAFT] → Law 27,699 for the Protection of Individuals with respect to Automatic Processing of Personal Data [IN FORCE] → Central Bank Communication A 7724 [IN FORCE] → Provision 18/2015 Guide to Good Privacy Practices for Application Development [IN FORCE] 	<ul style="list-style-type: none"> • Argentina is a party to the Organisation for Economic Co-operation and Development's AI principles. See the OECD's Policy Observatory. • Argentina adopted UNESCO's Recommendation on the Ethics of AI. • See Argentina's Digital Agenda 2030. • See Argentina's Fintech Innovation Hub. • Argentina's data protection authority, the Agency of Access to Public Information, published Resolution No. 161/23, which created the Transparency and Protection of Personal Data Program in the use of AI. • The president's chief of staff also issued Administrative Decision No. 750/2023, creating the Interministerial Roundtable on AI. • Argentina is testing the IBM AI Platform, using an aquaculture project to evaluate AI technology and formally incorporate this platform into the Ministry of Science, Technology and Productive Innovation.


	Specific AI governance law or policy	Relevant authorities	Other relevant laws and policies	Wider AI context
AUSTRALIA	<p>The Australian government highlighted the application of existing regulatory frameworks for AI. In 2021, the government released an AI Action Plan, which set out a plan to build AI capability and accelerate the development and adoption of trusted, secure and responsible AI technologies in Australia.</p> <p>In June 2023, the government released a discussion paper on safe and responsible AI. This paper was a call for consultation on whether Australia has the right governance arrangements in place to support the safe and responsible use and development of AI. In January 2024, the government communicated its interim response on safe and responsible AI.</p>	<ul style="list-style-type: none"> → Department of Industry, Science and Resources → Commonwealth Scientific and Industrial Research Organisation → Office of the eSafety Commissioner → Office of the Australian Information Commissioner → Competition and Consumer Commission → National AI Centre's Responsible AI Network → National Science and Technology Council 	<ul style="list-style-type: none"> → Patents Act [IN FORCE] → Copyright Act [IN FORCE] → Privacy Act [IN FORCE] → Data Availability and Transparency Act [IN FORCE] → Consumer Data Right [IN FORCE] → Competition and Consumer Act [IN FORCE] → Compliance and Enforcement Policy for the Consumer Data Right <p>Australia was one of the first countries in the world to adopt AI ethics principles, which include a robust ethics framework:</p> <ul style="list-style-type: none"> • AI Ethics Framework • 8 AI Ethics Principles 	<ul style="list-style-type: none"> • Australia is a party to the OECD's AI principles. See the OECD's Policy Observatory. • Australia participated in the 2023 U.K. AI Summit, which led to the Bletchley Declaration. • Australia adopted UNESCO's Recommendation on the Ethics of AI. • See Australia's 2025 Digital Transformation Strategy. • The government announced it will set up an advisory body of industry and academic experts to help it devise a legislative framework around "high risk" AI applications. • The Human Technology Institute at the University of Technology Sydney recently released The State of AI Governance in Australia. • See the National Science and Technology Council's Rapid Response Information Report on generative AI. • In March 2020, the government released the AI Standards Roadmap: Making Australia's Voice Heard. This separate roadmap was developed by Standards Australia and commissioned by the Australian Department of Industry, Science, Energy and Resources. The roadmap's primary goal is to "ensure Australia can effectively influence AI standards development globally."


	Specific AI governance law or policy	Relevant authorities	Other relevant laws and policies	Wider AI context
BANGLADESH	<p>Bangladesh is looking to advance its AI policies and has published a National AI Strategy for 2019-2024. The strategy includes:</p> <ul style="list-style-type: none"> • Creating strategy and development roadmaps. • Overcoming challenges with the use of AI. • Leveraging AI for social and economic growth, and more. 	<p>→ Information and Communication Technology Division</p>	<p>→ Digital Security Act [IN FORCE]</p> <p>→ Data Protection Act [DRAFT]</p> <p>→ Telecommunication Regulatory Commission Regulation for Digital, Social Media and OTT Platforms [DRAFT]</p> <p>→ Constitution of the People's Republic of Bangladesh [IN FORCE]</p> <p>→ Right to Information Act [IN FORCE]</p> <p>→ Copyright Act [IN FORCE]</p> <p>→ Telecommunications Act [IN FORCE]</p>	<ul style="list-style-type: none"> • Bangladesh adopted UNESCO's Recommendation on the Ethics of AI. • See Digital Bangladesh.


	Specific AI governance law or policy	Relevant authorities	Other relevant laws and policies	Wider AI context
BRAZIL	<p>Brazil published an AI Strategy, as well as a summary. The strategy proposes to finance research projects that apply ethical solutions, establish technical requirements that advance ethical applications, develop techniques to mitigate algorithmic bias, create parameters around human intervention where automated decisions may create high-risk situations, and implement codes of conduct to encourage traceability and safeguard legal rights. Brazil also strives to encourage data sharing per its data protection law, the LGPD, create an AI observatory for measuring impact and disseminate open-source codes for identifying discriminatory trends.</p> <p>Brazil has a proposed comprehensive AI Bill, which emphasizes human rights and creates a civil liability regime for AI developers. The proposed AI Bill would:</p> <ul style="list-style-type: none"> • Prohibit certain "excessive risk" systems. • Establish a regulatory body to enforce the law. • Create civil liability for AI providers. • Require reporting obligations for significant security incidents. • Guarantee various individual rights, such as explanation, nondiscrimination, rectification of identified biases and due process mechanisms. <p>In July 2023, the country's DPA, the Autoridade Nacional de Proteção de Dados, published a Preliminary Analysis of Bill No. 2338/2023, which provides for the use of AI in Brazil. Further, the ANPD has now published its final opinion on Bill 2338/2023.</p>	<p>→ Ministry of Science, Technology and Innovation</p> <p>→ ANPD</p>	<p>→ General Data Protection Act [IN FORCE]</p> <p>→ Civil Rights Framework for the Internet [IN FORCE]</p> <p>→ Consumer Protection Code [IN FORCE]</p>	<ul style="list-style-type: none"> • Brazil is a party to the OECD's AI principles. See the OECD's Policy Observatory and article on Brazil's path to responsible AI. • Brazil participated in the 2023 U.K. AI Summit, which led to the Bletchley Declaration. • Brazil adopted UNESCO's Recommendation on the Ethics of AI. • See Brazil's Digital Transformation Strategy. • The ANPD entered into a technical cooperation agreement with the Development Bank of Latin America "to develop an experimental regulatory tool" for AI-related innovation.


	Specific AI governance law or policy	Relevant authorities	Other relevant laws and policies	Wider AI context
CANADA	<p>Canada's anticipated AI and Data Act, part of Bill C-27, is intended to protect Canadians from high-risk systems, ensure the development of responsible AI, and position Canadian firms and values for adoption in global AI development. The AIDA would:</p> <ul style="list-style-type: none"> • Ensure high-impact AI systems meet existing safety and human rights expectations. • Prohibit reckless and malicious uses of AI. • Empower the Minister of Innovation, Science and Industry to enforce the act. <p>Canada published a code of practice for generative AI development and use in anticipation of, and to assure compliance with, the AI and Data Act.</p> <p>The country also issued a Directive on Automated Decision-Making, which imposes several requirements on the federal government's use of automated decision-making systems.</p>	<ul style="list-style-type: none"> → Ministry of Innovation, Science and Economic Development → Canadian Institute for Advanced Research → Office of the Privacy Commissioner of Canada → House of Commons' Standing Committee on Industry, Science and Technology → Advisory Council on AI 	<ul style="list-style-type: none"> → Personal Information Protection and Electronic Documents Act [IN FORCE] → Privacy Act [IN FORCE] → Consumer Product Safety Act [IN FORCE] → Food and Drugs Act [IN FORCE] → Motor Vehicle Safety Act [IN FORCE] → Bank Act [IN FORCE] → Human Rights Act [IN FORCE] → Criminal Code [IN FORCE] → Quebec's Law 25: An Act to modernize legislative provisions as regards the protection of personal information [IN FORCE] 	<ul style="list-style-type: none"> • Canada is a party to the OECD's AI principles. See the OECD's Policy Observatory. • Canada also participated in the 2023 U.K. AI Summit, which led to the Bletchley Declaration. • As part of the G7, Canada endorsed the 11 Hiroshima Process International Guiding Principles for Advanced AI systems. • Canada also adopted UNESCO's Recommendation on the Ethics of AI. • According to its AI Strategy, by 2030 Canada plans to achieve an AI ecosystem founded on scientific excellence, exceptional training and talent pools, public-private collaboration, and commitment to AI technologies which produce positive social, economic and environmental change for people and the planet. In achieving these goals, Canada has established three AI institutes: Amii in Edmonton, Mila in Montreal, and the Vector Institute in Toronto. • The House of Commons' Standing Committee on Industry, Science and Technology issued a report for various AI recommendations in 2019. • There is currently a proposed amendment to the Ontario Working for Workers Act for AI in hiring. This would be the country's first legislation requiring businesses to disclose whether they use AI in their hiring processes.


	Specific AI governance law or policy	Relevant authorities	Other relevant laws and policies	Wider AI context
CHILE	<p>In October 2021, Chile published its first National Policy and Action Plan on AI on AI. The country's previous Minister of Science, Technology, Knowledge and Innovation Andrés Couve explained the policy is built on the following:</p> <ul style="list-style-type: none"> • Development of enabling factors. • Use and development of AI technology. • Aspects of ethics and safety. <p>Chilean Parliament is discussing a bill on incorporating legal and ethical issues for the creation, distribution, commercialization and use of AI.</p>	<ul style="list-style-type: none"> → Ministry of Science, Technology, Knowledge and Innovation → Future Challenges, Science, Technology and Innovation Committee → National Research and Development Agency → National Center for AI Research → Chilean Transparency Council → National Consumers Agency 	<ul style="list-style-type: none"> → Digital Economy Partnership Agreement [IN FORCE] → Political Constitution of the Republic of Chile [IN FORCE] → Law No. 19,628 on the Protection of Private Life [IN FORCE] → Law No. 20,285 on the Transparency of Public Functions and Access to Information on Public Administration [IN FORCE] → Law 21,180 on Digital Transformation of the State [IN FORCE] → Industrial Property Law No. 19,039 [IN FORCE] → Law No. 17,336 on Intellectual Property [IN FORCE] → Fintech Law [IN FORCE] → Personal Data Protection Bill No. 11,144-07 [DRAFT] 	<ul style="list-style-type: none"> • Chile is a party to the OECD's AI principles. See the OECD's Policy Observatory. • Chile participated in the 2023 U.K. AI Summit, which led to the Bletchley Declaration. • Chile also adopted UNESCO's Recommendation on the Ethics of AI. • See Chile's 2035 Digital Transformation Strategy. • In 2023, Chile hosted the first Latin American and Caribbean Ministerial and High Level Summit on the Ethics of AI, with support from UNESCO and CAF. • The Inter-American Development Bank supported the Chilean government's project to develop new transport technology applications, specifically focusing on big data and autonomous vehicles.


	Specific AI governance law or policy	Relevant authorities	Other relevant laws and policies	Wider AI context
CHINA	<p>China was one of the first countries to implement AI regulations. Chinese lawmakers are in the process of drafting comprehensive AI regulation. Various regulations and policies apply to specific AI uses. These include:</p> <ul style="list-style-type: none"> • Algorithmic Recommendation Management Provisions [IN FORCE] • Interim Measures for the Management of Generative AI Services [IN FORCE] • Deep Synthesis Management Provisions [IN FORCE] • AI guidelines and summary of regulations [IN FORCE] • Scientific and Technological Ethics Regulation [IN FORCE] • Next Generation AI Development Plan [IN FORCE] 	<ul style="list-style-type: none"> → Cyberspace Administration of China → Ministry of Industry and Information Technology → Ministry of Public Security → State Administration for Market Regulation → National Development and Reform Commission 	<ul style="list-style-type: none"> → Cybersecurity Law [IN FORCE] → Data Security Law [IN FORCE] → Personal Information Protection Law [IN FORCE] → Shenzhen Special Economic Zone AI Industry Promotion Regulation [IN FORCE] 	<ul style="list-style-type: none"> • China is a party to the OECD's AI principles. See the OECD's Policy Observatory. • China participated in the 2023 U.K. AI Summit, which led to the Bletchley Declaration. • China also adopted UNESCO's Recommendation on the Ethics of AI. • See China's AI development plan. • See the Ministry of Science and Technology's 2021 AI governance document on ethical norms for AI use.


	Specific AI governance law or policy	Relevant authorities	Other relevant laws and policies	Wider AI context
COLOMBIA	<p>Colombia has various policies addressing AI governance, including the following:</p> <ul style="list-style-type: none"> • AI Expert Mission. • AI National Strategy Policy. • AI in the Public Sector. 	<ul style="list-style-type: none"> → Administrative Department of the Presidency of the Republic → CAF → Ministry of Information and Communication Technologies → Ministry of National Education → Administrative Department of Science, Technology and Innovation → National Planning Department → Superintendence of Industry and Commerce → AI Task Force 	<ul style="list-style-type: none"> → Personal Data Protection Law [IN FORCE] → Habeas Data Law, Law 1266 amended by Law 2157 of 2021 [IN FORCE] → Decree 338 [IN FORCE] 	<ul style="list-style-type: none"> • Colombia is a party to the OECD's AI principles. See the OECD's Policy Observatory. • Colombia also adopted UNESCO's Recommendation on the Ethics of AI. • Colombia published an Ethical Framework that reiterates best practices, suggestions and recommendations on how best to integrate ethical principles with the use of AI in projects primarily for the benefit of the public sector entities. • An AI Task Force was created in partnership with the CAF to bolster AI progress.
EGYPT	<p>Egypt's National AI Strategy focuses on four pillars:</p> <ul style="list-style-type: none"> • AI for government. • AI for development. • Capacity building. • International activities. <p>The country's other initiatives include an AI roadmap and Charter for Responsible AI.</p>	<ul style="list-style-type: none"> → National Council for AI → Ministry of Communications and Information Technology 	<ul style="list-style-type: none"> → Law No. 151 of 2020 on the Protection of Personal Data [IN FORCE] → Law No. 175 of 2018 Regarding Anti-Cyber and Information Technology Crimes [IN FORCE] → Telecommunication Regulation Law, Law No. 10 of 2003 [IN FORCE] → Law No. 82 of 2002 on the Protection of Intellectual Property Rights [IN FORCE] 	<ul style="list-style-type: none"> • Egypt is a party to the OECD's AI principles. See the OECD's Policy Observatory. • Egypt also adopted UNESCO's Recommendation on the Ethics of AI. • Egypt chaired several meetings for the Arab AI Working Group, which allows representatives from Arab countries to discuss AI strategies. See the group's chair election, second meeting and third meeting. • See the Applied Innovation Center. • The Senate Education Committee stressed the urgency of issuing a document to evaluate the ethics and control of AI in Egypt.


	Specific AI governance law or policy	Relevant authorities	Other relevant laws and policies	Wider AI context
<div data-bbox="136 264 172 300">EU</div> <div data-bbox="136 1294 172 1329">↓</div>	<p>In December 2023, the EU AI Act completed the political trilogue stage, with agreement reached on the respective positions of the European Commission, Council and Parliament. In brief, the act:</p> <ul style="list-style-type: none"> • Creates harmonized rules for placing AI on the EU market. • Applies to the EU and any third-country providers and deployers that place AI systems on the EU market. • Centers around a risk-based approach. • Prohibits use of certain AI systems and provides specific requirements for high-risk systems. • Creates harmonized transparency rules for certain AI systems. <p>Further, in 2018, the Commission published communication from the European Parliament, Council, Economic and Social Committee, and the Committee of the Regions on the approach of AI in Europe.</p>	<ul style="list-style-type: none"> → Proposed future EU AI Board → European Data Protection Board → Special Committee on AI in a Digital Age → EDPB's ChatGPT Task Force → Member state AI authorities, for example: <ul style="list-style-type: none"> - Spain's AI supervision agency, the Agencia Española de Supervisión de la Inteligencia Artificial → Member state DPAs, for example: <ul style="list-style-type: none"> - France's Commission nationale de l'informatique et des libertés - Germany's Federal Commissioner for Data Protection and Freedom of Information - Italy's Garante - Spain's Agencia Española de Protección de Datos - Belgium's DPA 	<ul style="list-style-type: none"> → General Data Protection Regulation [IN FORCE] → Digital Services Act [IN FORCE] → Digital Markets Act [IN FORCE] → AI Liability Directive [DRAFT] → EU Cyber Resilience Act [DRAFT] → Ethics guidelines for trustworthy AI [IN FORCE] → New Product Liability Directive [DRAFT] 	<ul style="list-style-type: none"> • The EU is a party to the OECD's AI principles. See the OECD's Policy Observatory. • The EU participated in the 2023 U.K. AI Summit, which led to the Bletchley Declaration. • As a nonenumerated member of the G7, the EU endorsed the 11 Hiroshima Process International Guiding Principles for Advanced AI systems. • The EU also adopted UNESCO's Recommendation on the Ethics of AI. • See the EU's approach and timeline for AI development. • Member states and the European Commission worked to create a Coordinated Plan on AI in 2018. This plan includes a table showcasing how 23 of 27 EU countries, as well as Norway and Switzerland, have progressed with their national strategies. The coordinated plan, updated in 2021, builds on the original 2018 plan. • In January 2024, the European Commission decided to establish an EU AI Office, to "ensure the development and coordination of AI policy at European level, as well as supervise the implementation and enforcement of the forthcoming AI Act."


	Specific AI governance law or policy	Relevant authorities	Other relevant laws and policies	Wider AI context
EU, continued		<ul style="list-style-type: none"> - Poland's Urząd Ochrony Danych Osobowych - Austria's DPA - Hungary's National Authority for Data Protection and Freedom of Information 		<ul style="list-style-type: none"> • Some EU member states have national AI strategies, many of which emphasize research, training and labor preparedness, as well as multistakeholder and international collaboration. For example, France's national AI strategy lays out three main objectives: <ul style="list-style-type: none"> - Improve the AI education and training ecosystem. - Establish an open data policy for implementing AI applications and pooling assets. - Develop an ethical framework for fair and transparent use of AI.
INDIA	<p>A proposed Digital India Act would replace the IT Act of 2000 and regulate high-risk AI systems. The Indian government has advocated for a robust, citizen-centric and inclusive "AI for all" environment. A task force has been established to make recommendations on ethical, legal and societal issues related to AI, and to establish an AI regulatory authority.</p> <p>According to its National Strategy for AI, India hopes to become what it calls an "AI garage" for emerging and developing economies, where scalable solutions can be easily implemented and designed for global deployment.</p>	<ul style="list-style-type: none"> → NITI Aayog → Ministry of Electronics and Information Technology → Ministry of Commerce and Industry → AI Task Force 	<ul style="list-style-type: none"> → Information Technology Act [IN FORCE] → The Information Technology Rules [IN FORCE] → Competition Act [IN FORCE] → Motor Vehicles Act [IN FORCE] → Digital Personal Data Protection Act [IN FORCE] → Copyright Act [IN FORCE] → National e-Governance Plan [IN FORCE] 	<ul style="list-style-type: none"> • India is a party to the OECD's AI principles. See the OECD's Policy Observatory. • India participated in the 2023 U.K. AI Summit, which led to the Bletchley Declaration. • India also adopted UNESCO's Recommendation on the Ethics of AI. • NITI Aayog, the government's public policy think tank, launched the AI Research, Analytics and knowledge Assimilation platform to elaborate on AI requirements in India. • See India AI, an umbrella program of the Ministry of Electronics and Information Technology.


	Specific AI governance law or policy	Relevant authorities	Other relevant laws and policies	Wider AI context
INDONESIA	<p>In 2020, Indonesia released the National Strategy on AI as part of the AI Towards Indonesia's Vision 2045. The following five national priorities were outlines as where AI is anticipated to have the biggest impact:</p> <ul style="list-style-type: none"> • Health services. • Bureaucratic reform. • Education and research. • Food security. • Mobility and smart cities. <p>Further, Indonesia released a Circular on AI Ethics. While not binding, it provides a reference point for formulating and establishing internal company policies for Indonesia's AI industry. Since issuing the circular, the Ministry of Communication and Informatics committed to preparing specific regulations regarding AI use and development.</p>	<ul style="list-style-type: none"> → Ministry of Communication and Informatics → Agency for the Assessment and Application of Technology → Ministry of Research, Technology and Higher Education → National Cyber and Crypto Agency 	<ul style="list-style-type: none"> → Law No. 27 of 2022 on Personal Data Protection [IN FORCE] → Electronic Information Law [IN FORCE, AMENDMENT TO LAW IN DRAFT] → Article 40 of Law No. 36 of 1999 regarding Telecommunications [IN FORCE] → Law No. 14 of 2008 on Public Information Transparency [IN FORCE] → Copyright Act [IN FORCE] 	<ul style="list-style-type: none"> • Indonesia is a party to the OECD's AI principles. See the OECD's Policy Observatory. • Indonesia participated in the 2023 U.K. AI Summit, which led to the Bletchley Declaration. • Indonesia also adopted UNESCO's Recommendation on the Ethics of AI. • See Indonesia's roadmap for industry, Making Indonesia 4.0.


	Specific AI governance law or policy	Relevant authorities	Other relevant laws and policies	Wider AI context
ISRAEL	<p>Based on a draft policy for regulation and ethics in AI, Israel wants to form a uniform risk-management tool, establish a governmental knowledge and coordination center, and maintain involvement in international regulation and standardization. In general, voluntary standardization, sector-based self-regulation and modular experimentation tools, e.g., sandboxes, will be favored over a lateral framework. The following resources are available for policy guidance:</p> <ul style="list-style-type: none"> • Israeli AI Regulation and Policy White Paper: A First Glance. • Harnessing Innovation: Israeli Perspectives on AI Ethics and Governance. • Policy on AI Regulation and Ethics. 	<ul style="list-style-type: none"> → Ministry of Innovation, Science and Technology → Ministry of Justice → Privacy Protection Authority → Israel National Cyber Directorate 	<ul style="list-style-type: none"> → Basic Law: Human Dignity and Liberty [IN FORCE] → Privacy Protection Law [IN FORCE] → Data Security Regulation [IN FORCE] → Credit Data Law [IN FORCE] → Copyright Act [IN FORCE] 	<ul style="list-style-type: none"> • Israel is a party to the OECD's AI principles. See the OECD's Policy Observatory. • Israel participated in the 2023 U.K. AI Summit, which led to the Bletchley Declaration. • Israel's Ministry of Justice issued an opinion that machine learning will fall under the fair-use provision in the country's Copyright Act.


	Specific AI governance law or policy	Relevant authorities	Other relevant laws and policies	Wider AI context
JAPAN	<p>In 2022, Japan released a National AI Strategy. Japan promotes the notion of "agile governance," whereby the government provides nonbinding guidance and defers to the private sector's voluntary efforts to self-regulate.</p> <p>The following white papers have been issued for policy guidance:</p> <ul style="list-style-type: none"> • AI Governance in Japan Ver. 1.1. • Governance Guidelines for Implementation of AI Principles. • AI Utilization Guidelines, an initiative for implementing the OECD AI Principles. <p>In 2023, the AI Strategy Council released draft AI Operator Guidelines, which clarify how operators should develop, provide and use AI.</p>	<ul style="list-style-type: none"> → Ministry of Economy, Trade and Industry → Council for Science, Technology and Innovation → Personal Information Protection Commission → Fair Trade Commission 	<ul style="list-style-type: none"> → Improving Transparency and Fairness of Digital Platforms Act [IN FORCE] → Financial Instruments and Exchange Act [IN FORCE] → Protection of Personal Information Act [IN FORCE] → Antimonopoly Act [IN FORCE] → Product Liability Act [IN FORCE] → Copyright Law [IN FORCE] 	<ul style="list-style-type: none"> • Japan is a party to the OECD's AI principles. See the OECD's Policy Observatory. • Japan participated in the 2023 U.K. AI Summit, which led to the Bletchley Declaration. • As part of the G7, Japan endorsed the 11 Hiroshima Process International Guiding Principles for Advanced AI systems. • Japan also adopted UNESCO's Recommendation on the Ethics of AI. • The Social Principles of Human-Centric AI, drafted by the Council for Social Principles of Human-Centric AI, describe AI's role in Japan's "Society 5.0" and advocates that AI should be human-centric; promote education/literacy; protect privacy; ensure security; maintain fair competition; ensure fairness, accountability and transparency; and promote collaborative innovation. • Minister of Education, Culture, Sports, Science and Technology Keiko Nagaoka declared the country's copyright laws cannot be enforced on materials used in AI training datasets. • Japan's Ministry of Economy, Trade and Industry introduced the Contract Guidelines for AI and Data Use to assist parties involved in AI business transactions. • See the Draft AI Research and Development Guidelines for International Discussions.


 MAURITIUS	Specific AI governance law or policy	Relevant authorities	Other relevant laws and policies	Wider AI context
	<p>Mauritius published an AI Strategy. The strategy goes in depth on the benefits and challenges of AI, specifically how AI impacts the country's various industries, and sets out a clear vision for development of AI.</p> <p>Other initiatives from the Mauritius government include:</p> <ul style="list-style-type: none"> • AI Society. • AI for Agriculture project. 	<ul style="list-style-type: none"> → Ministry of Technology, Communication and Innovation → Ministry of Finance and Economic Development → AI Council → Research and Innovation Council → Data Protection Office 	<ul style="list-style-type: none"> → Financial Services (Robotic and AI Enabled Advisory Services) Rules [IN FORCE] → Data Protection Act [IN FORCE] → National Cyber Security Strategy [IN FORCE] → Cybersecurity and Cybercrime Act [IN FORCE] → Industrial Property Act [IN FORCE] → Copyright Act [IN FORCE] → Protection against Unfair Practices (Industrial Property Rights) Act [IN FORCE] 	<ul style="list-style-type: none"> • Mauritius is a party to the OECD's AI principles. See the OECD's Policy Observatory. • Mauritius also adopted UNESCO's Recommendation on the Ethics of AI. • See the Digital Mauritius 2030 strategic plan. • In 2019, the Minister of Technology, Communication and Innovation officially opened the workshop, Leading Innovation in Business and Government Services through AI, which is organized by the Mauritius Research and Innovation Council.


	Specific AI governance law or policy	Relevant authorities	Other relevant laws and policies	Wider AI context
NEW ZEALAND	<p>Many New Zealand government agencies are signatories to the Algorithm Charter, which sets out a series of ethical commitments around the development and use of algorithms. The charter provides a risk matrix to assess the likelihood and impact of algorithmic applications. The New Zealand government generally prioritizes trustworthy and human-centric AI development.</p> <p>Although there is no comprehensive AI regulation in New Zealand, the current Privacy Act 2020 applies to the use of AI systems in the country. The Office of the Privacy Commissioner issued guidance on compliance with privacy law when using generative AI tools, as well as a summary. Further, the Office of the Privacy Commissioner published the Privacy Commissioner's expectations around generative AI in June 2023.</p> <p>The Law, Society and Ethics Working Group published a set of guiding Trustworthy AI in Aotearoa principles designed to provide direction for AI stakeholders.</p>	<ul style="list-style-type: none"> → Ministry of Business, Innovation and Employment → Statistics New Zealand → Office of the Privacy Commissioner → Department of Internal Affairs 	<ul style="list-style-type: none"> → Privacy Act [IN FORCE] → Bill of Rights Act [IN FORCE] → Treaty of Waitangi [IN FORCE] → Human Rights Act [IN FORCE] → Māori Data Sovereignty Principles → Māori Data Governance Model 	<ul style="list-style-type: none"> • New Zealand is a party to the OECD's AI principles. See the OECD's Policy Observatory. • New Zealand also adopted UNESCO's Recommendation on the Ethics of AI. • The New Zealand government released AI cornerstones, which will inform an eventual national AI strategy. • See the AI Forum of New Zealand. • "An example of governance for AI in health services from Aotearoa New Zealand" published on nature.com has been recognised for its approach in the health sector, particularly in terms of prioritising the voice of Māori. • The Office of the Privacy Commissioner is currently conducting consultation on a Biometrics Privacy Code of Practice under the Privacy Act to regulate the use of biometric technologies. If enacted, that code of practice will have the force of law under the Privacy Act. • The Department of Internal Affairs published initial advice on Generative AI in the public service.


	Specific AI governance law or policy	Relevant authorities	Other relevant laws and policies	Wider AI context
PERU	<p>Peru enacted several AI initiatives, including Law 31814 to promote the use of AI "in favor of the economic and social development of the country." The law includes the following principles:</p> <ul style="list-style-type: none"> • Risk-based security standards. • Multi-stakeholder approach. • Internet governance. • Digital society. • AI privacy. <p>Peru also developed a National AI Strategy that aids in the promotion, development and adoption of AI in the country. The first draft includes a roadmap, goals, definitions and external context examples to further develop the strategy.</p>	<ul style="list-style-type: none"> → Secretariat of Government and Digital Transformation → Presidency of the Council of Ministers → National Directorate of Intelligence → Superintendence of Banking, Insurance and Pension Fund Administration → Ministry of Justice and Human Rights → National Authority for the Protection of Personal Data → National Authority for Transparency, Access to Public Information and Protection of Personal Data 	<ul style="list-style-type: none"> → Supreme Decree No. 157-2021-PCM [IN FORCE] → Supreme Decree No. 003-2013-JUS [IN FORCE] → Personal Data Protection Law No. 29733 [IN FORCE] → Law of Transparency and Access to Public Information [IN FORCE] → Finance Regulation for Information Security and Cybersecurity [IN FORCE] → Cyber Defense Law No. 30999 [IN FORCE] → Law 30096 on Computer Crime [IN FORCE] → Financial sector Cybersecurity Framework [IN FORCE] → Copyright Law, Legislative Decree 822 [IN FORCE] 	<ul style="list-style-type: none"> • Peru is a party to the OECD's AI principles. See the OECD's Policy Observatory. • Peru also adopted UNESCO's Recommendation on the Ethics of AI. • See the National Digital Transformation Policy for 2030.


	Specific AI governance law or policy	Relevant authorities	Other relevant laws and policies	Wider AI context
SAUDI ARABIA	<p>Saudi Arabia has a National Strategy on Data and AI, which provides a welcoming, flexible and stable regulatory framework, including incentive schemes, to attract AI companies, investors and talents. According to the strategy, Saudi Arabia aspires to be one of the leading economies utilizing and exporting data and AI after 2030. It is ready to leverage its "young and vibrant population" and "unique centralized ecosystem." The country hopes to attract outside investment by hosting global AI events and applying its influence as a tech hub within the Middle East.</p>	<ul style="list-style-type: none"> → Saudi Data and AI Authority → National Data Management Office → Ministry of Communications and Information Technology 	<ul style="list-style-type: none"> → Personal Data Protection Law [IN FORCE] → Data Management and Personal Data Protection Standards [IN FORCE] → Children and Incompetents' Data Protection Policy [IN FORCE] → Data Classification Policy [IN FORCE] → General Rules for the Transfer of Personal Data outside the Geographical Borders of the Kingdom [IN FORCE] → Data Sharing Policy [IN FORCE] → Freedom of Information Policy [IN FORCE] → Open Data Policy [IN FORCE] 	<ul style="list-style-type: none"> • Saudi Arabia is a party to the OECD's AI principles. See the OECD's Policy Observatory. • Saudi Arabia also adopted UNESCO's Recommendation on the Ethics of AI. • The government of Saudi Arabia in collaboration with the Saudi Data and AI Authority signed a memorandum of understanding to create an AI center dedicated to the energy segment.

	Specific AI governance law or policy	Relevant authorities	Other relevant laws and policies	Wider AI context
SINGAPORE	<p>Singapore developed voluntary governance frameworks and initiatives for ethical AI deployment, data management and sectoral implementation, including:</p> <ul style="list-style-type: none"> • Model AI Governance Framework. • National AI Programmes in Government and Finance. • Veritas Initiative, an implementation framework for AI governance in the financial sector. • AI Verify Foundation, a governance testing toolkit. • IPOS International, part of the Intellectual Property Office of Singapore that realizes customized IP solutions. • Proposed Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems. • Principles to Promote Fairness, Ethics, Accountability and Transparency in the Use of AI and Data Analytics in Singapore's Financial Sector. • Implementation and Self-Assessment Guide for Organizations, a companion to the Model AI Governance Framework. <p>Singapore is also seeking international feedback on a new governance framework for generative AI.</p>	<ul style="list-style-type: none"> → Smart Nation Digital Government Group → AI Ethics and Governance Steering Committee → Personal Data Protection Commission → Monetary Authority of Singapore → Infocomm Media Development Authority → Advisory Council on the Ethical Use of AI and Data 	<ul style="list-style-type: none"> → Personal Data Protection Act [IN FORCE] → Computer Misuse Act [IN FORCE] → Copyright Act [IN FORCE] → Patents Act [IN FORCE] → Competition Act [IN FORCE] → Cybersecurity Act [IN FORCE] → Protection from Online Falsehoods and Manipulation Act [IN FORCE] → Road Traffic Act [IN FORCE] → The Digital Economy Partnership Agreement [IN FORCE] 	<ul style="list-style-type: none"> • Singapore is a party to the OECD's AI principles. See the OECD's Policy Observatory. • Singapore participated in the 2023 U.K. AI Summit, which led to the Bletchley Declaration. • Singapore also adopted UNESCO's Recommendation on the Ethics of AI. • Based on Singapore's National AI Strategy, the city-state aims to be a global hub for AI, thereby generating economic gains and improving lives. A key tenet in Singapore's AI policy is that its citizens understand AI tech and its workforce attains the necessary competencies to participate in an AI economy. • The Singapore VerifyAI initiative, known as the "crosswalk" was unveiled at the inaugural US-Singapore Dialogue on Critical and Emerging Technologies. The crosswalk links IMDA's AI Verify with the U.S. National Institute of Standards and Technology's AI Risk Management Framework. • See the Primer to the Model AI Governance Framework. • See the Trusted Data Sharing Framework. • See the Guide to Job Redesign in the Age of AI. • Complementing the Model Framework and ISAGO are two volumes of a Compendium of Use Cases that show "how local and international organisations across different sectors and sizes implemented or aligned their AI governance practices with all sections of the Model Framework." <ul style="list-style-type: none"> - Volume 1. - Volume 2.

	Specific AI governance law or policy	Relevant authorities	Other relevant laws and policies	Wider AI context
SOUTH KOREA	<p>South Korea has a comprehensive AI Act in the works to ensure accessibility to AI technology for all developers without government approval, but this requires reliability measures. South Korea is also setting new standards on copyrights of AI-generated content.</p> <p>South Korea has numerous policy initiatives regarding AI and technology under its National Strategy for AI, including the AI Research and Development Strategy, the Data Industry Activation Strategy, and the System Semiconductor Strategy. The nation intends to leverage its high education level, widespread acceptance of new technology and preeminent IT infrastructure to implement these initiatives.</p> <p>Additionally, in August 2023, the Personal Information Protection Commission published guidance for the safe use of personal information in the age of AI.</p>	<p>→ Ministry of Science and ICT</p> <p>→ Personal Information Protection Commission</p> <p>→ Communications Commission</p> <p>→ Internet and Security Agency</p> <p>→ Financial Services Commission</p> <p>→ Fair Trade Commission</p> <p>→ National Information Society Agency</p> <p>→ Korea AI Association</p>	<p>→ Personal Information Protection Act [IN FORCE]</p> <p>→ Monopoly Regulation and Fair Trade Act [IN FORCE]</p> <p>→ Copyright Act [IN FORCE]</p> <p>→ Protection and Use of Location Information Act [IN FORCE]</p> <p>→ Consumer Protection in Electronic Commerce Act [IN FORCE]</p> <p>→ Promotion and Communications Network Utilization and Information Protection Act [IN FORCE]</p> <p>→ Credit Information Use and Protection Act [IN FORCE]</p> <p>→ Product Liability Act [IN FORCE]</p>	<ul style="list-style-type: none"> • South Korea adopted UNESCO's Recommendation on the Ethics of AI. • The Digital New Deal was created by the South Korean government to promote both educational and industrial efforts on AI opportunities. • See the AI Open Innovation Hub.

	Specific AI governance law or policy	Relevant authorities	Other relevant laws and policies	Wider AI context
TAIWAN	<p>Taiwan has embraced a holistic approach to developing an AI environment. The government is currently drafting an act that would govern AI, specifically "the legal definition of AI, privacy protections, data governance, risk controls and ethical principles related to AI." The following resources have been issued for policy guidance:</p> <ul style="list-style-type: none"> • National Science and Technology Council's policy discussing AI Innovation. • AI Taiwan Action Plan. • AI Taiwan Action Plan 2.0. • 2022 AI-Readiness Assessment Report. 	<ul style="list-style-type: none"> → Fair Trade Commission → NSTC, previously the Ministry of Science and Technology → Ministry of Health and Welfare → Executive Yuan of Taiwan → Ministry of Digital Affairs → Industrial Technology Research Institute → Taiwan AI Center of Excellence 	<ul style="list-style-type: none"> → Personal Data Protection Act [IN FORCE] → Fair Trade Act [IN FORCE] → Cybersecurity Management Act [IN FORCE] → Company Act [IN FORCE] → Child and Youth Sexual Exploitation Prevention Act [IN FORCE] → Copyright Act [IN FORCE] → Patent Act [IN FORCE] → Freedom of Government Information Law [IN FORCE] → Financial Technology Development and Innovative Experimentation Act [IN FORCE] → FinTech Regulatory Sandbox Guidance → MoST AI Technology Research and Development Guidelines → Guidelines on the use of Generative AI [DRAFT] 	<ul style="list-style-type: none"> • See the Digital Nation and Innovative Economic Development Program. • See the 5+2 Industrial Innovation Plan. • See Smart Taiwan 2030. • See Taiwan AI Labs. • See the country's Forward-looking Infrastructure Development Program. • See the Unmanned Vehicle Technology Innovation Sandbox.

	Specific AI governance law or policy	Relevant authorities	Other relevant laws and policies	Wider AI context
UNITED ARAB EMIRATES	<p>In 2017, the UAE became the first country to establish an AI ministry. The nation's Council for AI and Blockchain will oversee policies that promote an AI-friendly ecosystem, advance AI research and accelerate collaboration between public and private sectors. The UAE is poised to become a hub for AI research, collaboration, innovation and education per its National Strategy for AI. The following resources have been issued for policy guidance:</p> <ul style="list-style-type: none"> • National Program for AI. • AI Ethics Principles and Guidelines. • Generative AI guide. • AI coding license. • AI System Ethics Self-Assessment Tool. • AI Adoption Guideline in Government Services. • The Dubai International Financial Centre's Regulation 10 on Processing Personal Data Through Autonomous and Semi-Autonomous Systems [IN FORCE]. 	<ul style="list-style-type: none"> → Minister of AI, Digital Economy and Remote Work Applications Office → AI and Blockchain Council → Data Office → Council for Digital Wellbeing → Regulations Lab → Abu Dhabi Global Market's Office of Data Protection → DIFC 	<ul style="list-style-type: none"> → Personal Data Protection Law [IN FORCE] → Central Bank Rulebook [IN FORCE] → Federal Decree Law on Combating Rumours and Cybercrimes [IN FORCE] → Penal Code [IN FORCE] → Federal Law concerning the Regulation of Competition [IN FORCE] → Federal Law on Consumer Protection [IN FORCE] → Federal Decree Law on Copyrights and Neighbouring Rights [IN FORCE] → Health Data Law [IN FORCE] → Federal Law on the Regulation and Protection of Industrial Property Rights [IN FORCE] → ADGM's Data Protection Regulations 2021 [IN FORCE] → Federal Law on the Civil Transactions Law of the United Arab Emirates State [IN FORCE] → Minister of AI, Digital Economy and Remote Work Applications Office's AI Ethics Principles and Guidelines 	<ul style="list-style-type: none"> • The UAE is a party to the OECD's AI principles. See the OECD's Policy Observatory. • The UAE participated in the 2023 U.K. AI Summit, which led to the Bletchley Declaration. • The UAE also adopted UNESCO's Recommendation on the Ethics of AI. • Abu Dhabi hosts a growing startup community, advanced machine-learning facilities and educational institutions, like Mohamed bin Zayed University which teamed up with IBM to open the AI Center of Excellence, in addition to a new supercomputing resource for complex algorithms and large datasets. With this infrastructure in place, the UAE hopes to deploy AI in priority sectors such as energy and transportation. • The National Program for AI published a Deepfake Guide in 2021. • The UAE AI and Robotics Award for Good aims to "encourage research and applications of innovative solutions in (AI) and robotics to meet existing challenges in the categories of health, education and social services." • See the country's Guidelines for Financial Institutions adopting Enabling Technologies. • See the AI Hardware Infrastructure Report.

	Specific AI governance law or policy	Relevant authorities	Other relevant laws and policies	Wider AI context
U.K.	<p>The U.K. government proposed a context-based, proportionate approach to regulation and will rely on existing sectoral laws to impose guardrails on AI systems. The following resources are available for policy guidance:</p> <ul style="list-style-type: none"> • A pro-innovation approach to AI regulation. • Algorithmic Transparency Recording Standard Hub. • AI Standards Hub, a new U.K. initiative dedicated to the evolving and international field of standardization for AI technologies. • Guide to using AI in the public sector by the U.K. government. • The Government Digital Service and the Office for AI's guide on understanding AI ethics and safety. • The Centre for Data Ethics and Innovation's AI Governance research report. • Guidance on the AI auditing framework from the Information Commissioner's Office. • ICO and Alan Turing Institute's Explaining decisions made with AI. 	<ul style="list-style-type: none"> → Office for AI → Information Commissioner's Office → Digital Regulation Cooperation Forum → Financial Conduct Authority → AI Council → Department for Science, Innovation and Technology 	<ul style="list-style-type: none"> → Equality Act [IN FORCE] → U.K. General Data Protection Regulations and Data Protection Act [IN FORCE] → Consumer Protection Act [IN FORCE] → Financial Services and Markets Act [IN FORCE] → Consumer Rights Act [IN FORCE] → National Security and Investment Act [IN FORCE] → Copyright, Designs and Patents Act [IN FORCE] → Advanced Research and Invention Agency Act [IN FORCE] → National Cyber Security Centre's Assessing intelligent tools for cyber security [IN FORCE] → AI (Regulation) Bill [DRAFT] 	<ul style="list-style-type: none"> • The U.K. is a party to the OECD's AI principles. See the OECD's Policy Observatory. • In 2023, the country hosted the AI Summit, which led to the Bletchley Declaration. • The U.K. also adopted UNESCO's Recommendation on the Ethics of AI. • As part of the G7, the U.K. endorsed the 11 Hiroshima Process International Guiding Principles for Advanced AI systems. • Specific action items include launching a national AI research and insights program, developing a diverse AI workforce, enabling better data availability, creating a national strategy for AI in health and social care, applying AI systems to climate change mitigation, piloting an AI standards hub to coordinate with global AI standardization, and developing a cross-government standard for algorithmic transparency. • The Centre for Data Ethics and Innovation published a Roadmap to an Effective AI Assurance Ecosystem, which is also part of the National AI Strategy. Further, the CDEI created an AI Assurance Guide as a companion to the roadmap. • See the U.K. AI Safety Institute.

	Specific AI governance law or policy	Relevant authorities	Other relevant laws and policies	Wider AI context
<p>U.S. (FEDERAL)</p> <p>The U.S. has released numerous frameworks and guidelines. Congress has passed legislation to preserve U.S. leadership in AI research and development, as well as control government use of AI. In May 2023, the Biden-Harris administration updated the National AI Research and Development Strategic Plan, emphasizing a principled and coordinated approach to international collaboration in AI research. The Office of Science and Technology Policy issued a request for information to obtain public input on AI's impact. The National Telecommunications and Information Administration sought feedback on what policies can create trust in AI systems through an AI Accountability Policy Request for Comment. Specific AI governance law and policy includes:</p> <ul style="list-style-type: none"> Executive orders: <ul style="list-style-type: none"> Maintaining American Leadership in AI Promoting the Use of Trustworthy AI in the Federal Government The Safe, Secure, and Trustworthy Development and Use of AI Acts and bills: <ul style="list-style-type: none"> AI Training Act [IN FORCE] National AI Initiative Act (Division E, Sec. 5001) [IN FORCE] AI in Government Act (Division U, Sec. 101) [IN FORCE] Algorithmic Accountability Act [DRAFT] National AI Commission Act [DRAFT] <p>↓</p>		<ul style="list-style-type: none"> → Office of Science and Technology Policy → National AI Initiative Office → Federal Trade Commission → Consumer Financial Protection Bureau → Department of Justice → Equal Employment Opportunity Commission 	<ul style="list-style-type: none"> → FTC Act, Section 5 [IN FORCE] → Fair Credit Reporting Act [IN FORCE] → Equal Credit Opportunity Act [IN FORCE] → Title VII of the Civil Rights Act [IN FORCE] → Americans with Disabilities Act [IN FORCE] → Age Discrimination in Employment Act [IN FORCE] → Fair Housing Act [IN FORCE] → Genetic Information and Nondiscrimination Act [IN FORCE] → American Data Privacy and Protection Act [DRAFT] → Health Equity and Accountability Act [DRAFT] 	<ul style="list-style-type: none"> • The US is a party to the OECD's AI principles. See the OECD's Policy Observatory. • The U.S. participated in the 2023 U.K. AI Summit, which led to the Bletchley Declaration. • The U.S. also adopted UNESCO's Recommendation on the Ethics of AI. • As part of the G7, the U.S. endorsed the 11 Hiroshima Process International Guiding Principles for Advanced AI systems. • In general, the U.S. approach to AI governance has been slow and incremental, seeking to preserve civil and human rights for Americans throughout AI deployment, as well as mobilize international collaboration which upholds democratic values and mutual advancement. • See the U.S. AI Safety Institute. • U.S. Senate Committee on the Judiciary's Subcommittee on Privacy, Technology and the Law held a hearing on the legislation of AI. • U.S. senators met for the first time with top technology industry executives in a closed-door session about AI regulation called the AI Insight Forum. Majority Leader Schumer made Floor Remarks on the first forum. • The Singapore VerifyAI initiative known as "crosswalk" was unveiled at the inaugural U.S.-Singapore Dialogue on Critical and Emerging Technologies. The crosswalk links IMDA's AI Verify with the U.S. NIST's AI Risk Management Framework.

	Specific AI governance law or policy	Relevant authorities	Other relevant laws and policies	Wider AI context
U.S. (FEDERAL), continued	<ul style="list-style-type: none"> - Digital Platform Commission Act [DRAFT] - Global Technology Leadership Act [DRAFT] - Transparent Automated Governance Act [DRAFT] • Nonbinding frameworks: <ul style="list-style-type: none"> - Blueprint for an AI Bill of Rights - National Institute of Standards and Technology AI Risk Management Framework - Guidance for Regulation of AI Applications • Government initiatives: <ul style="list-style-type: none"> - Voluntary Commitments from Leading AI Companies to Manage the Risks Posed by AI - TTC Joint Roadmap on Evaluation and Measurement Tools for Trustworthy AI and Risk Management - Congressional AI effort of Sen. Charles E. Schumer, D-N.Y. - National Security Commission on AI - Bipartisan legislative framework for AI announced by U.S. Senators Richard Blumenthal, D-Conn., and Josh Hawley, R-Mo. 			

Contact

Gabrielle Schwartz

AI Governance Research Lead, IAPP

gschwartz@iapp.org

Uzma Chaudry

AI Governance Center Fellow, IAPP

uchaudhry@iapp.org

Joe Jones

Research and Insights Director, IAPP

jjones@iapp.org

For further inquiries, please reach out to research@iapp.org.

Follow the IAPP on social media



Updated February 2024.

The IAPP disclaims all warranties, expressed or implied, with respect to the contents of this material, including any warranties of accuracy, merchantability or fitness for a particular purpose. Nothing herein should be construed as legal advice.

© 2024 IAPP. All rights reserved.