MARCH 2024

VEHICLE SAFETY SYSTEMS

Privacy Risks and Recommendations

FUTURE OF PRIVACY FORUM

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

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 and 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

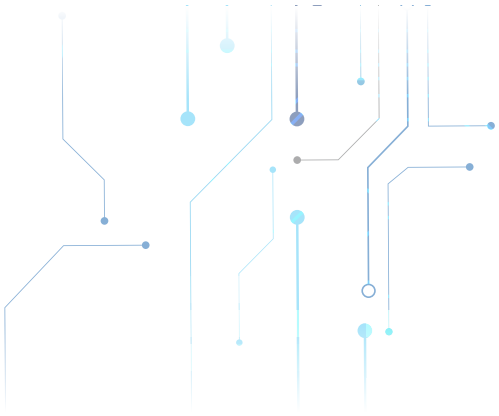
One frequent goal of ADAS, DMS, and ADS can be to identify driver impairment whether by alcohol, drugs, inattention, or drowsiness. Impairment refers to the deterioration of a driver's ability to safely perform the driving task, either through a driver's physiological and cognitive impairment or their 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 (CO_2) 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.

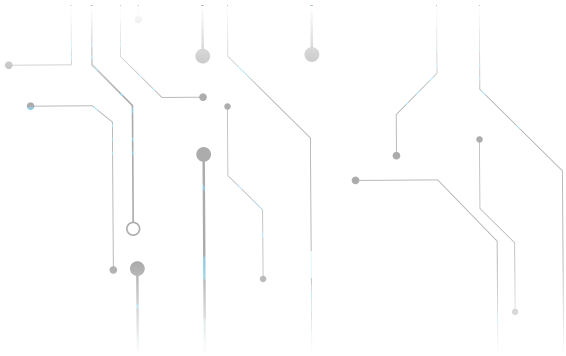
2. *Touch (Palmprint, Fingerprint, or other body-based touch)*

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 Luján (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

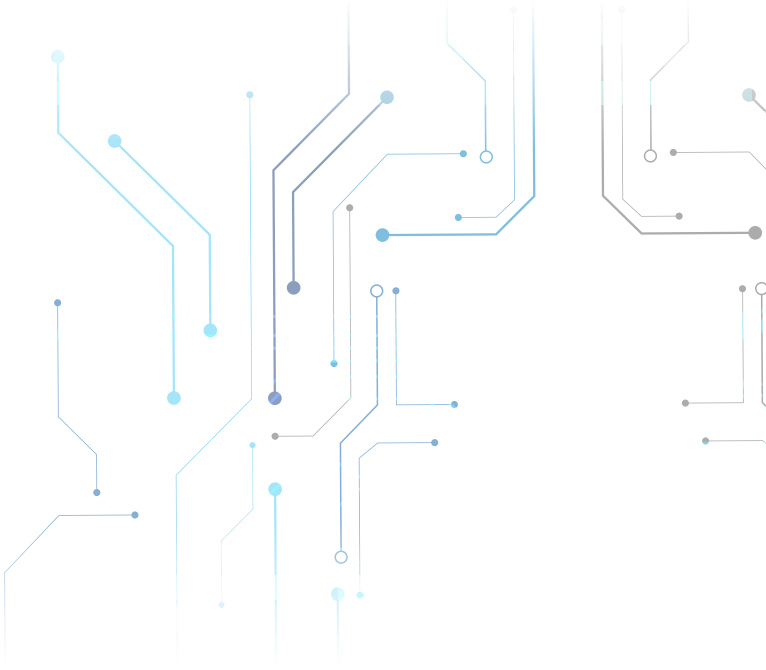
Each Vehicle Safety System has implications for privacy depending on functionality, as discussed above. They all collect or rely on different data types to operate. When data is collected, it can be used to inform insurance rates, how vehicle manufacturers can improve vehicle functions, or how to ensure 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

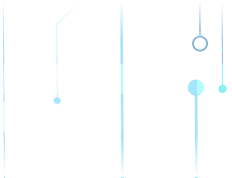
Regulators, technology developers, and technology deployers should identify and mitigate, to the extent possible, potential future harms to drivers, especially to people from underrepresented, marginalized, and multimarginalized communities.

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 saftey technology have you heard of?

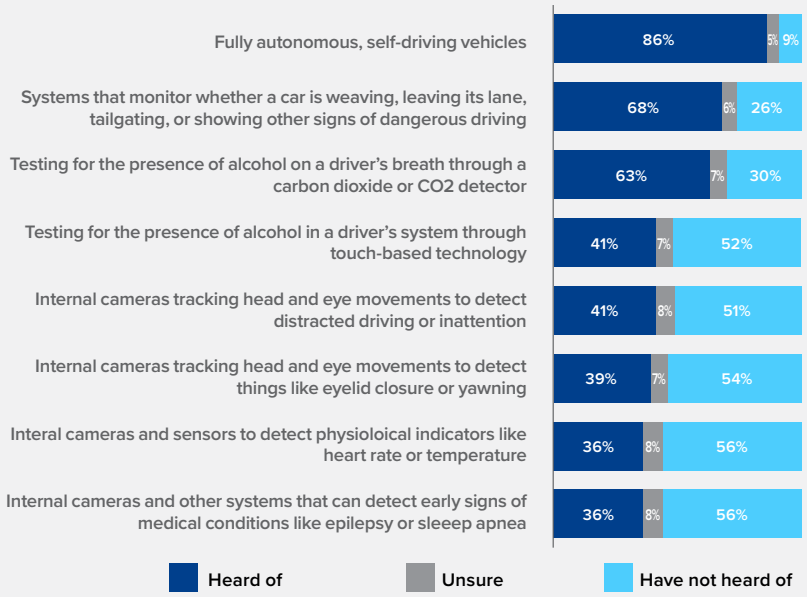


Fig 2: Which words do you think best describe these kinds of driver safety technologies, assuming that these technologies would not impact the price of a vehicle?

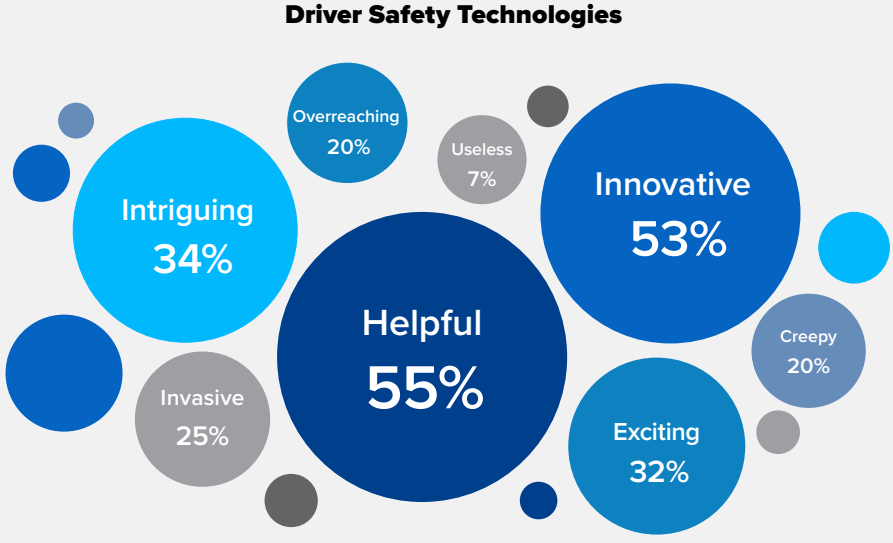


Fig 3: To what extent, if at all, are you concerned about the privacy of your personal data when interacting with the following types of companies and organizations?

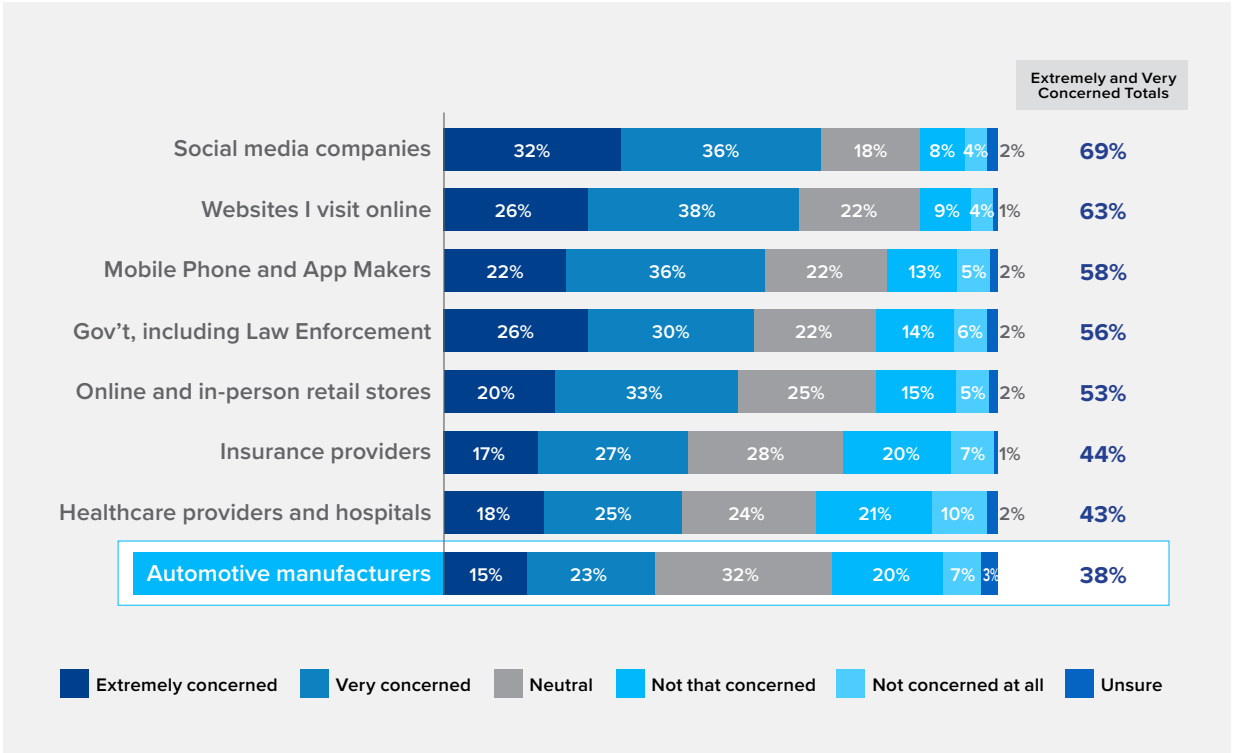


Fig 4: When it comes to data collection in passenger cars, just based on what you know, which of the following activities do you think collects user data that can be accessed by automotive manufacturers or third parties like insurance companies, advertisers or government agencies (inlcuding law enforcement)?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

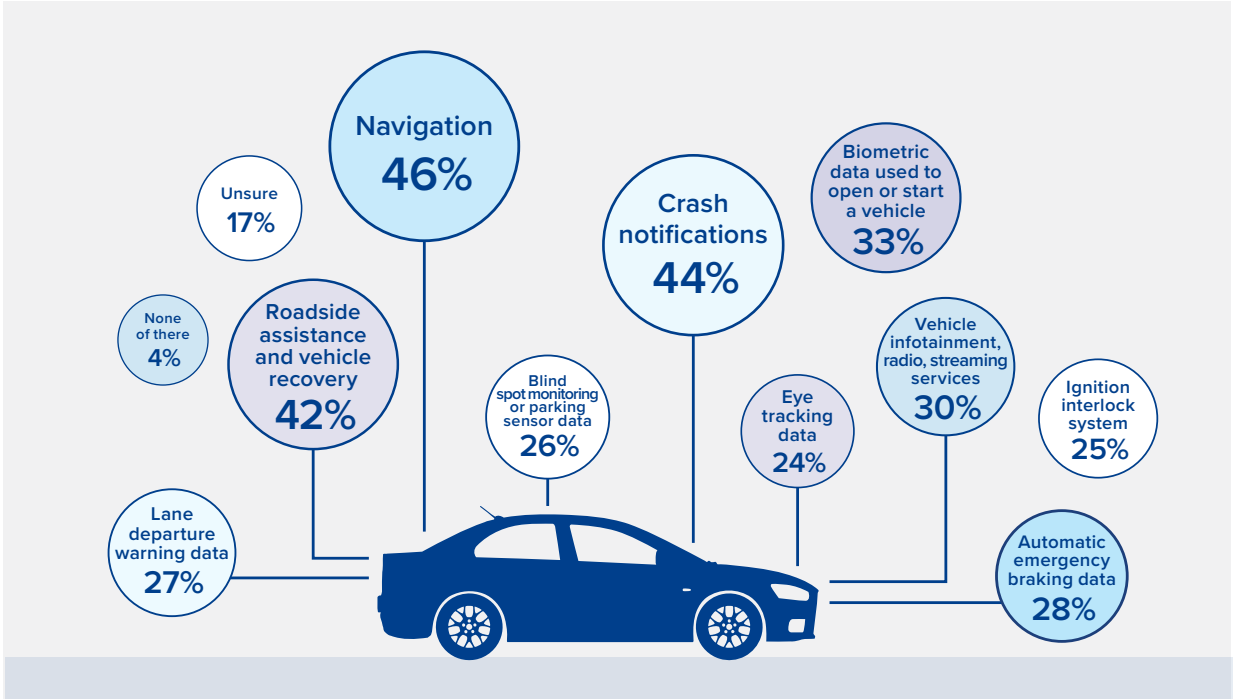


Fig 5: If you have concerns about technology to automatically detect a driver's alcohol levels, what best characterizes those concerns?

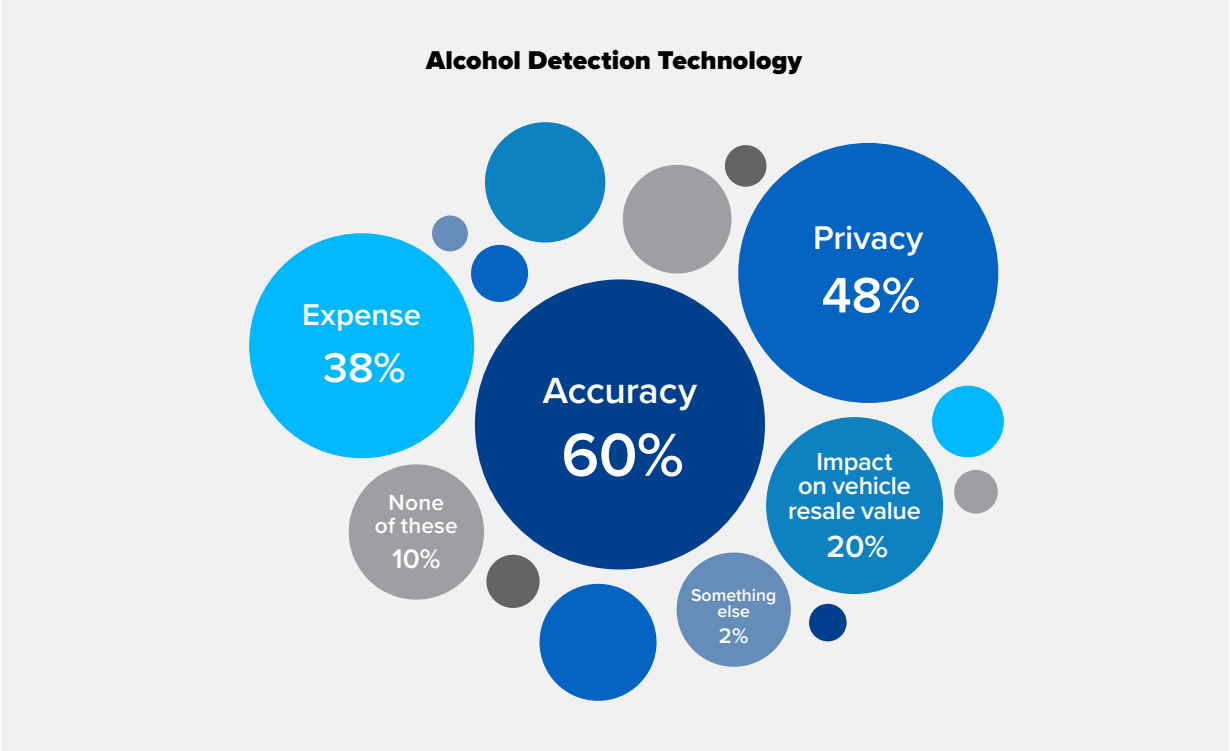


Fig 6: If you have concerns about technology to automatically detect impaired driving by monitoring driving behavior, what best characterizes those concerns?

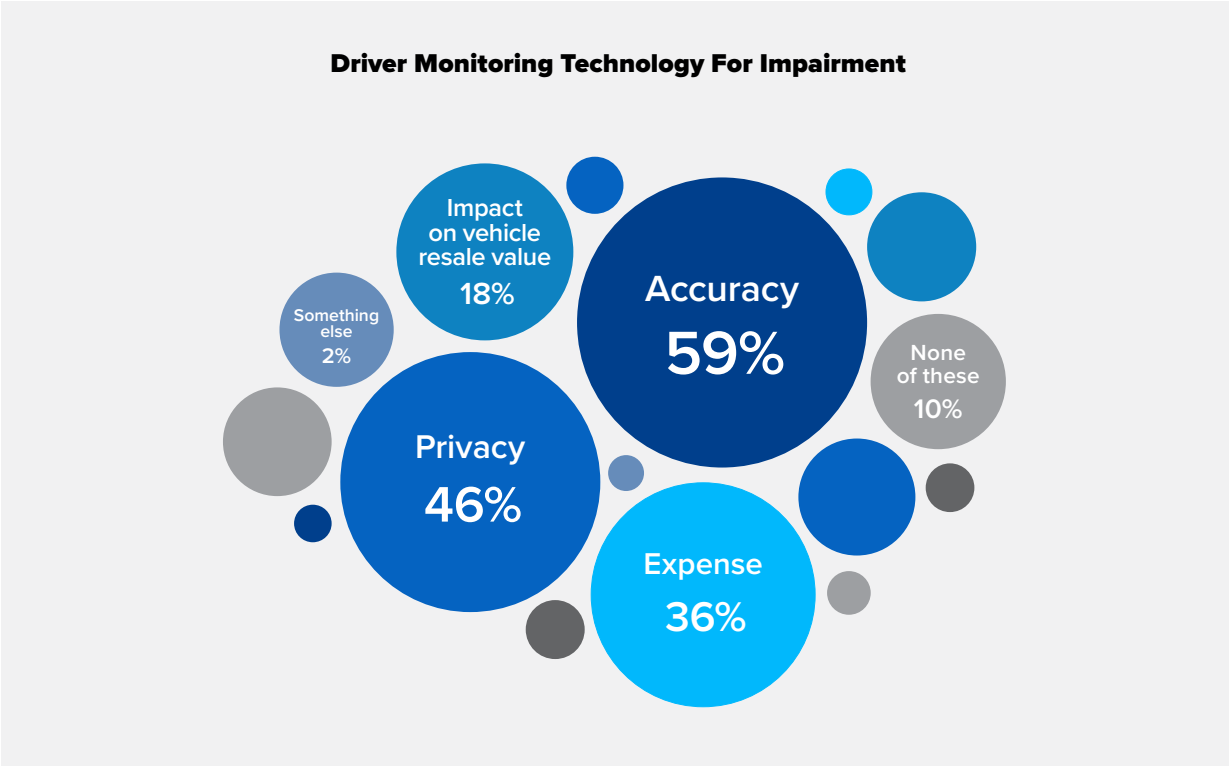


Fig 7: In general, how much would you say you trust that data collected about passenger cars is kept safe?

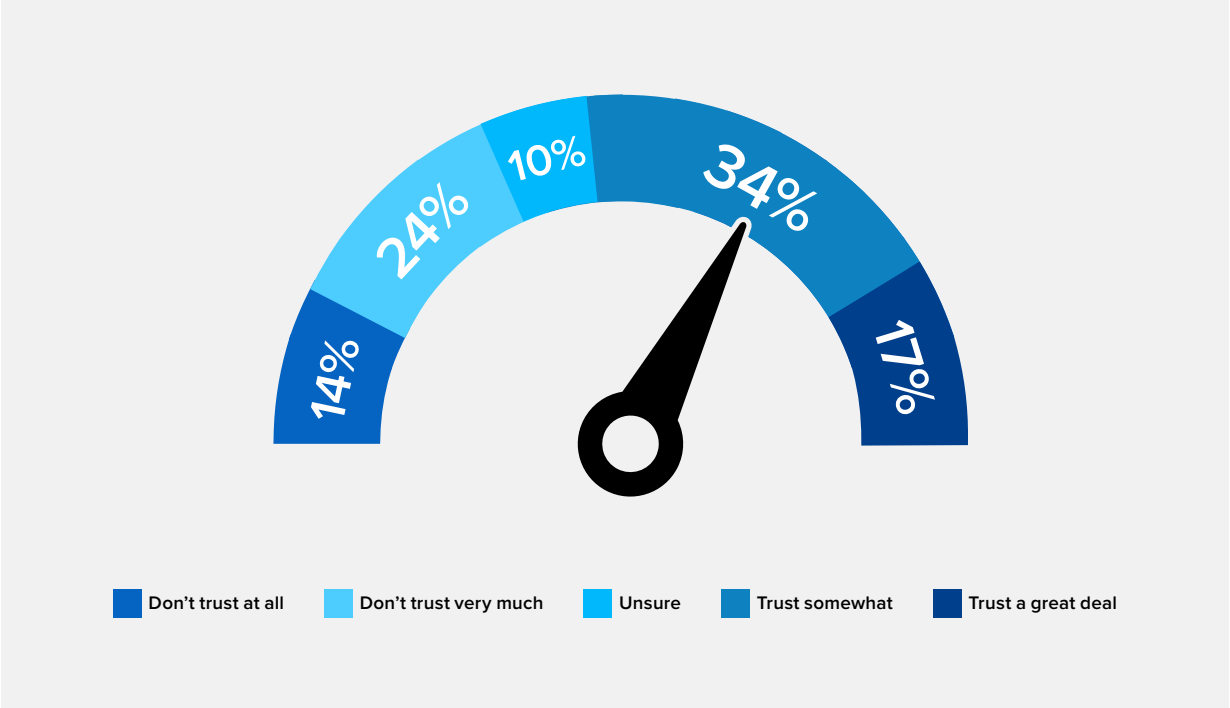


Fig 8: In general, how much would you say you trust data collected about you in automotive vehicles to be only used for the intended purpose?

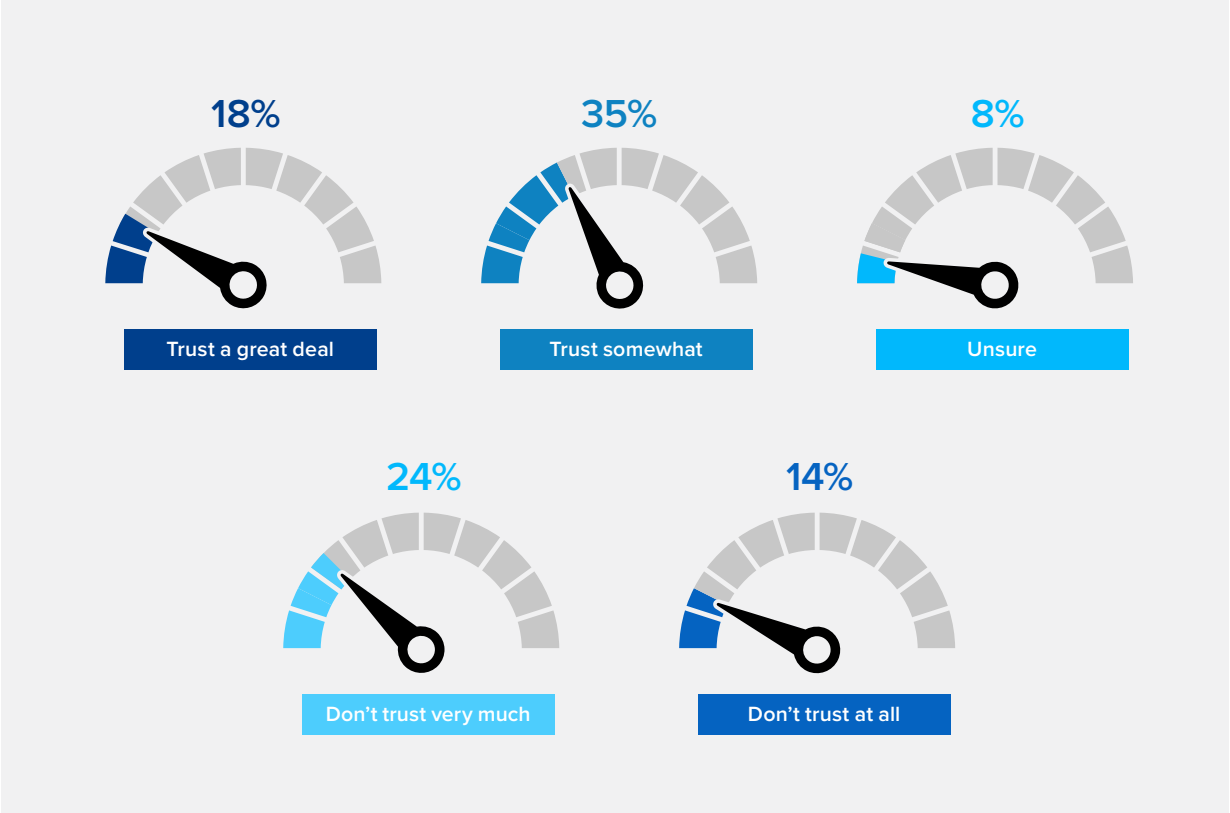


Fig 9: How much trust do you have in each of the following types of technology to report accurate data?

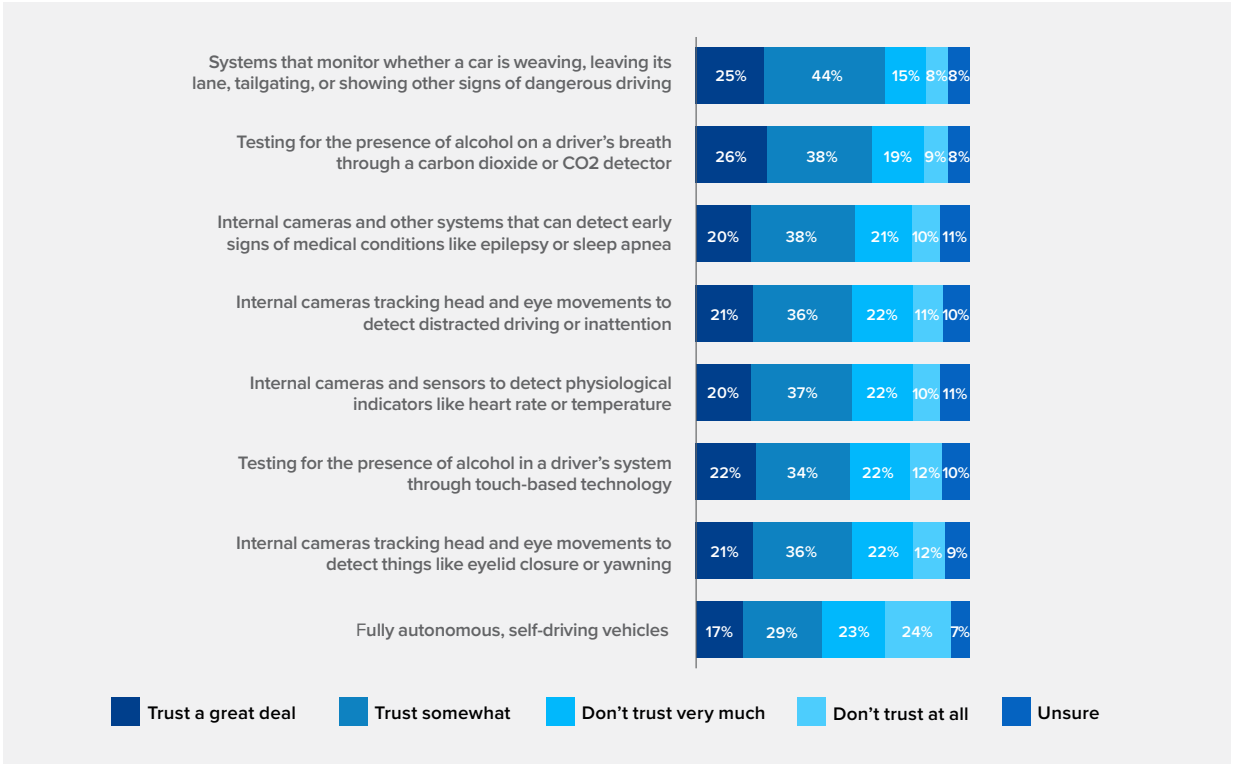


Fig 10: How concerned are you about driver safety technologies sharing your data in the following ways?

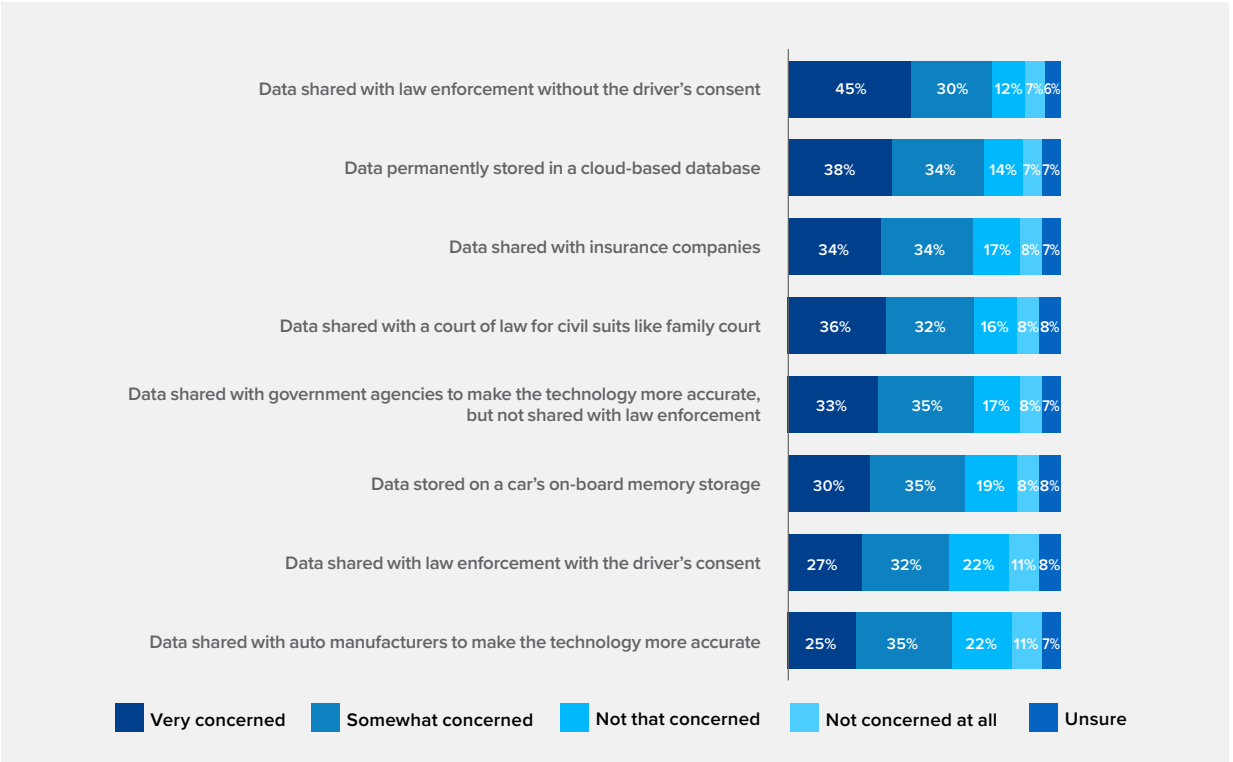


Fig 11: How comfortable would you be with technology that passively detects alcohol levels to identify whether a driver may be impaired and prevents them from starting their car, if...

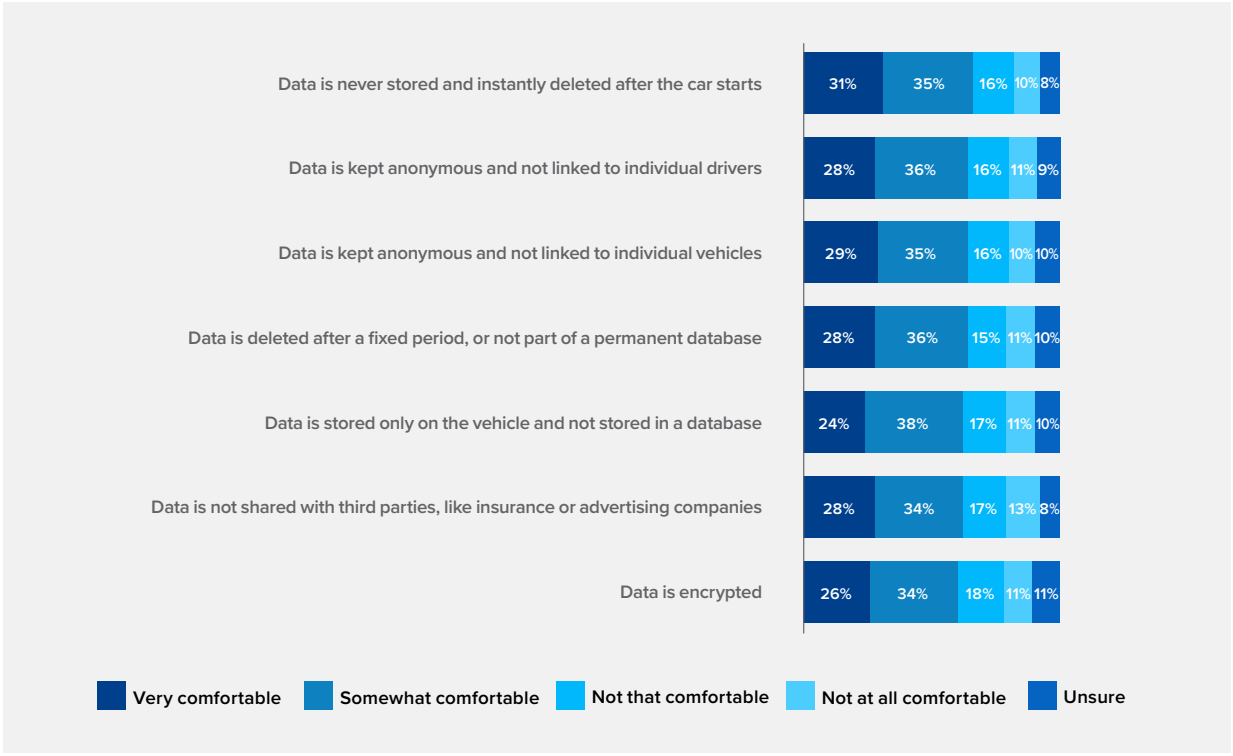


Fig 12: Which of these would you consider essential, or "must have," as part of any technology that passively detects alcohol levels to identify whether a driver may be impaired and prevents them from starting their car? Choose all that apply.

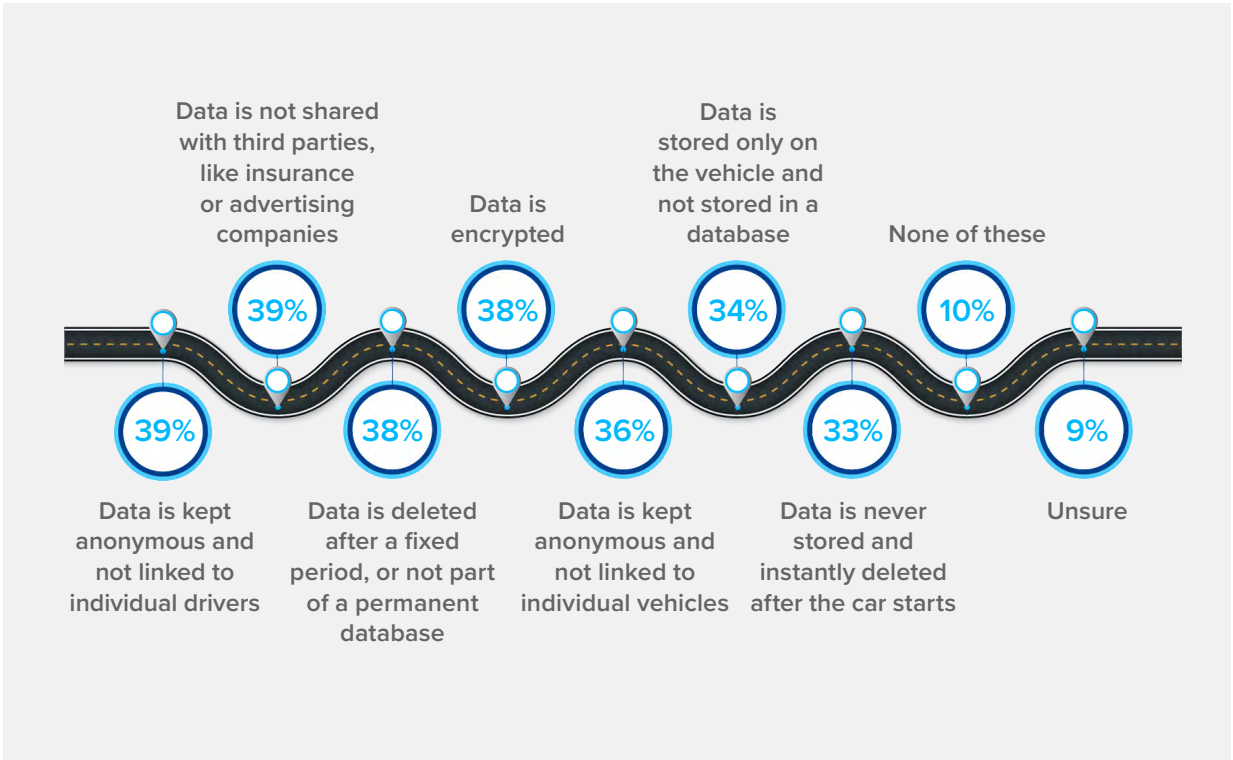


Fig 13: Which of these would you consider essential or "must-have" as part of any technology that monitors whether a driver is weaving, leaving their land, tailgating, or showing other signs of impaired driving by constantly monitoring driving behavior? Choose all that apply.

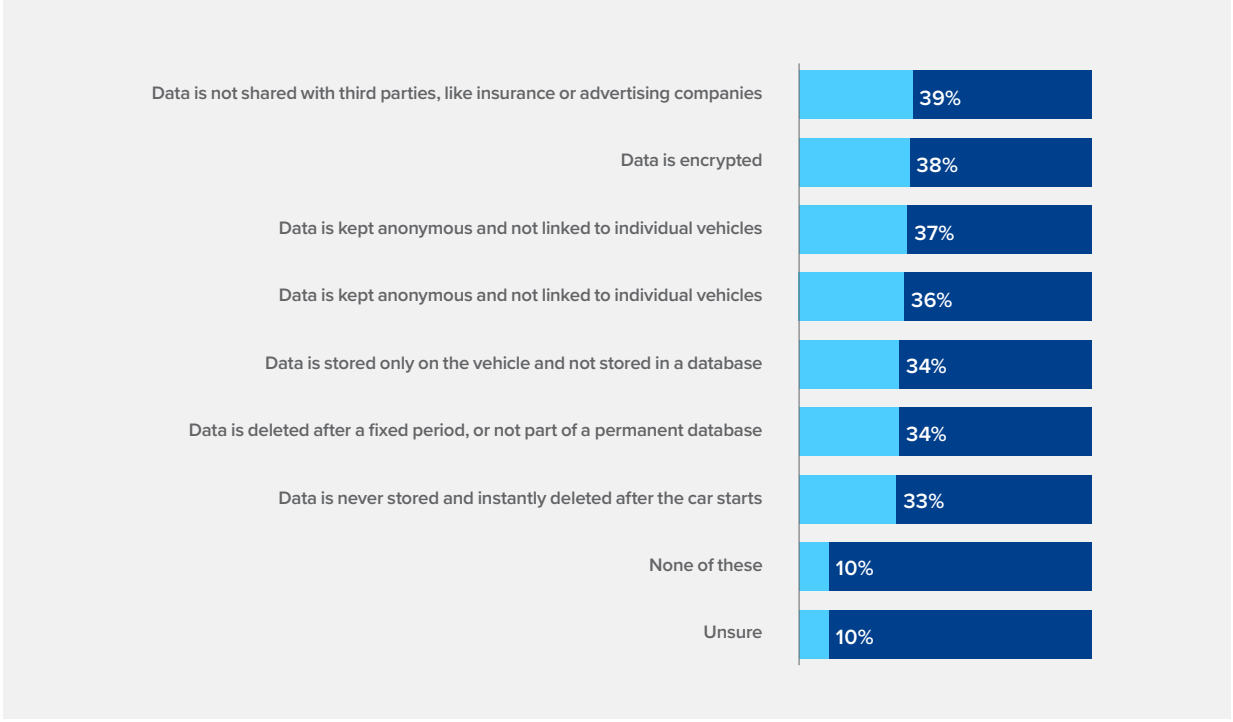
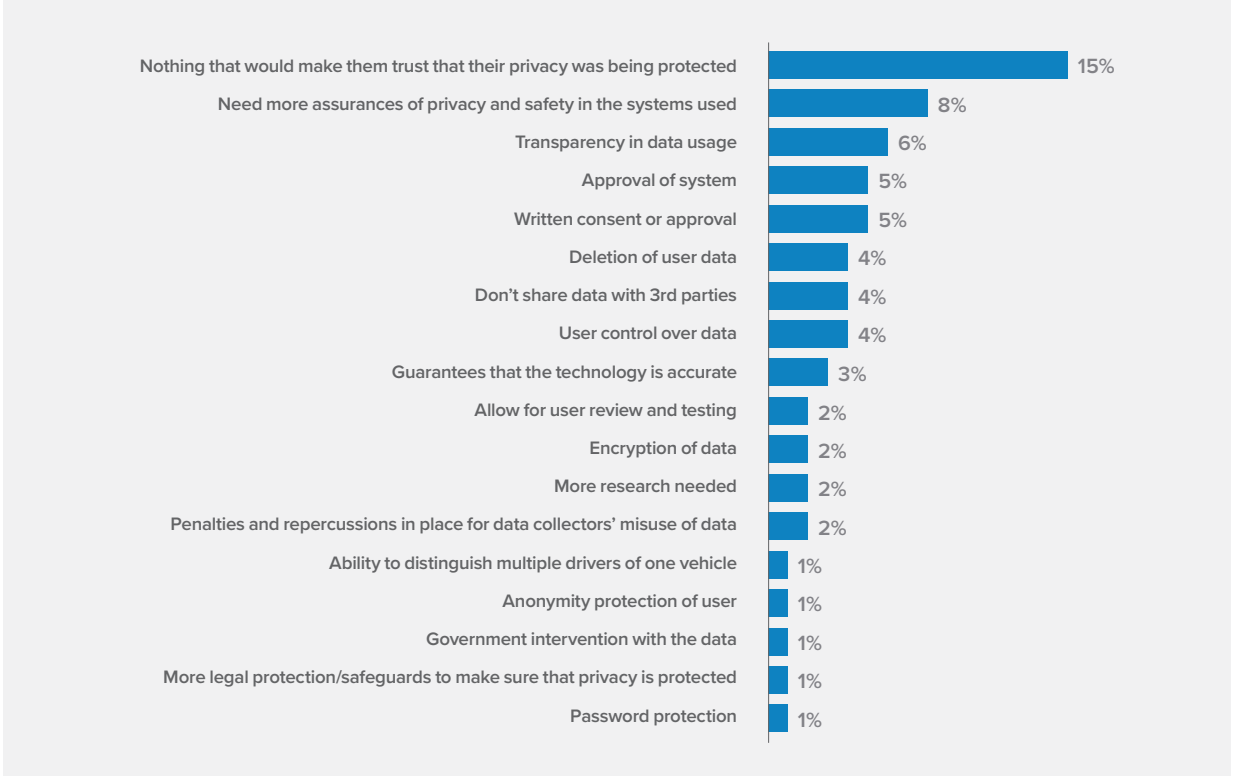


Fig 14: In general, what do you think you would need in order to trust that these driver safety systems were protecting your privacy?



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&scisig=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.lifesafer.com/blog/how-does-an-ignition-interlock-device-work/#:~:text=Camera%20ignition%20interlocks%20will%20also,a%20printed%20or%20electronic%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 Approache*s, 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 Bertoncello 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 Luján, *Luján, 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.whi*tehouse.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, 831 32 (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. C*alifornia 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.

1350 EYE STREET NW | SUITE 350 | WASHINGTON, DC 20005 FPF.ORG | info@fpf.org