Privacy Analysis in Response to Notice and Request for Comments, Docket No. NHTSA-2021-0085

Contents

Introduction

I am writing this comment as a second-year law student at the University of South Carolina School of Law in connection to a course, Technology Law: The Law of the Newly Possible, taught by Professor Bryant Walker Smith. This course was focused on the implications of vehicle automation for enforcement. While this comment does not regard automated vehicles, the proposed advanced drunk and impaired driving prevention (AD&IDP) technology would be a form of automated enforcement, which was heavily researched and discussed throughout the course. As a part of this course, I was lucky enough to ask Dr. Jefferey Michael, who has been published through the National Highway Traffic Safety Administration, about AD&IDP technology logistics.[1]

[1] Jeffrey P. Michael, EdD, https://publichealth.jhu.edu/faculty/3943/jeffrey-p-michael (last visited Apr. 13, 2022).

This comment will seek to provide support for an extension of the information collection by analyzing the privacy implications of such technology for the general public in the context of its potential benefits and its potential to cause harm. While there are many theoretical tools to analyze privacy implications, this comment will analyze potential issues using a typology of privacy to categorize harms related to "the feasibility, the potential benefits of, and the public policy challenges associated with a more widespread use of non-invasive technology to prevent alcohol-impaired driving."[2] Ideally, this categorization of harms will assist the NHTSA in extending its information collection by providing valid reasons why "the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information will have practical utility."[3]

Legislative Findings and Public Policy

The Infrastructure Investment and Jobs Act (II&J Act) found, "[A]dvanced drunk and impaired driving prevention technology can prevent more than 9,400 alcohol-impaired driving fatalities annually."[4] Where, "[I]n 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[.]"[5] Thus, if AD&IDP technology would have been integrated into passenger motor vehicles prior to 2019, at least ninety-two percent of those deaths would have been prevented. Furthermore, each day that passes without the integration of said technology will be accompanied by an average of twenty-five alcohol-impaired driving fatalities.

Public policy has been defined as "anything which tends to undermine that sense of security for individual rights, whether of personal liberty or private property, which any citizen ought to feel has a

[2] Notice and Request for Comments on an Extension of a Currently Approved Information Collection, 87 Fed. Reg. 14613 (proposed Mar. 15, 2022) [hereinafter *Notice*].
[3] *Id.*
[4] *See* Infrastructure Investment and Jobs Act, Pub. L. No. 117-58, § 24220, 135 Stat. 429 (2021) [hereinafter *Infrastructure Act*].
[5] *Id.*

tendency to be injurious to the public or the public good."[6] In the context of the II&J Act, AD&IDP technology would undermine the sense of security one would have when operating a vehicle while intoxicated or impaired. Although this sense of security is undermined, any citizen ought to feel intoxicated or impaired driving has a tendency to be injurious to the public in consideration of the shocking legislative findings of the II&J Act.

Traditionally, public policy goals regarding DUI enforcement have been "deterrence, punishment, public protection, rehabilitation, and promotion of respect for the law."[7] The public policy goal, public protection, falls within the scope of the NHTSA's regulatory authority, evidenced by "the passage of the National Traffic and Motor Vehicle Safety Act of 1966, which sought 'to reduce traffic accidents' by regulating the safety of motor vehicles."[8] To avoid regulating beyond its defined scope, the NHTSA should seek to only promote public protection by reducing traffic accidents and should not seek to promote deterrence, punishment, rehabilitation, or promotion and respect for the law. While AD&IDP technology would patently promote public protection by reducing traffic accidents, this technology could be used to serve other purposes beyond the NHTSA's scope. Therefore, to properly perform its functions, the NHTSA should collect as much information as necessary before prescribing a rule requiring AD&IDP technology.

Privacy Tools

When conducting a privacy analysis, Koops' conceptualization of the typology of privacy can be an extremely helpful resource.[9] Additionally, the typology of privacy harms by Citron and Solove allows

---

[6] *Mary R. v. B. & R. Corp.*, 149 Cal. App. 3d 308, 317, 196 Cal. Rptr. 871, 876 (1983) (quoting *Craemer* v. *Superior Court* (1968) 265 Cal.App.2d 216, 222 [71 Cal.Rptr. 193]).

[7] *United States v. Chalmers*, 81 F. App'x 464, 466 (4th Cir. 2003) (holding that public policy goals were reasonably related to the imposition of six months at a community facility when the defendant was arrested twice for driving under the influence).

[8] *Ctr. for Auto Safety & Pub. Citizen, Inc. v. Nat'l Highway Traffic Safety Admin.*, 371 U.S. App. D.C. 422, 424, 452 F.3d 798, 800 (2006) (quoting Pub. L. No. 89-563, 80 Stat. 718, 718 (originally codified at 15 U.S.C. §§ 1381 et seq. (1970))).

[9] *See generally* Bert-Jaap Koops et al., *A Typology of Privacy*, 38 U. PA. J. INT'L L. 483 (2017) [hereinafter *Typology*].

one to elucidate legally cognizable privacy harms, such as reputational harms.[10] Obviously, this will not be a simple analysis leading to black and white solutions as many of the proposed solutions to privacy issues will detract from public safety. Additionally, solutions tending to increase the general level of public safety may decrease the amount of privacy the public is afforded. Furthermore, affording one person privacy protections will almost always subject another person to privacy harms.

Bodily Privacy

Koops theorized that there were nine types of privacy.[11] Of these, bodily privacy, "typified by individuals' interest in the privacy of their physical body[,]" is most implicated by the II&J Act's requirement of AD&IDP technology.[12] Obviously, one's privacy of their physical body is invaded when a drunk driver's vehicle collides with their body and causes them to be injured or worse, die. However, in describing bodily privacy, Koops states, "The emphasis here is on negative freedom: being able to exclude people from touching one's body or restraining or restricting one's freedom of bodily movement."[13] Where the II&J Act seeks to prevent or limit the operation of a motor vehicle, one's freedom of bodily movement may be restricted.

Although the legislation requires the technology to accurately detect drunk or impaired drivers, inaccurate detection is likely inevitable. According to the NHTSA, issues surrounding the detection of drug-impaired driving include, "[T]he large number of substances with the potential to impair driving and increase crash risk, the variations in the ways different drugs can impair driving, the lack of basic information about many potentially impairing drugs, and the differences in the ways that drugs can affect the body and behavior."[14] Additionally, breath-based sensors to detect intoxicated drivers might be

---

[10] *Se generally* Solove, Daniel J. and Keats Citron, Danielle, "Privacy Harms" (2021). *GW Law Faculty Publications & Other Works*. 1534. https://scholarship.law.gwu.edu/faculty_publications/1534 (last visited Apr. 14, 2022) [hereinafter *Harms*].
[11] *Typology*, *supra* note 9, at 484.
[12] *Typology*, *supra* note 9, at 567.
[13] *Id.*
[14] NHTSA, *Drug-Impaired Driving: Understanding the Problem & Ways to Reduce It: A Report to Congress*, December 2009, https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/811268.pdf, (last visited Feb. 16, 2022).

triggered by an intoxicated passenger breathing too close to a sober driver. Without assurances that these issues are able to be overcome, many drivers will likely be the subject of inaccurate detections of intoxicated or impaired driving, restricting bodily privacy. Undoubtedly, people want to prevent the egregiously high number of fatalities that occur each year as a result of drunk and impaired driving accidents. However, legislators should seek to predict and prevent harms that may result from integrating this technology into vehicles before requiring the integration of this technology.

Proprietary Privacy

When a person is identified as drunk or impaired, causing their vehicle's operation to be limited or prevented, their proprietary privacy, "typified by a person's interest in using property as a means to shield activity, facts, things, or information from the view of others[,]" may too be harmed.[15] Whereas, today people are able to attempt to shield their state of intoxication or impairment from others while driving, advanced drunk and impaired driving technology may indirectly alert nearby people to the driver's state of intoxication or impairment. One can imagine a situation where a person attempting to shield the fact that they are on mind-altering anti-anxiety medication is prevented from operating their vehicle and passengers are able to infer the driver's impairment, causing increased consternation. Moreover, a person attempting to shield the fact that they are on mind-altering anti-psychotic medication may experience proprietary privacy harms if nearby people witness the driver being prevented from operating their vehicle.

However, bodily and proprietary privacy interests may be outweighed by the "public interest in the preservation of life" when such technology identifies a driver as lethally intoxicated.[16] The NHTSA has previously stated that, "Additional information about the driver's health or behavioral conditions could be interpreted from blood pressure, heart and respiration rate, blood glucose levels and other physiological parameters and could lead to vehicle intervention in driving and/or alert EMS or police of

[15] *Typology*, *supra* note 9, at 567.
[16] *Commonwealth v. Duncan*, 467 Mass. 746, 754, 7 N.E.3d 469, 475 (2014).

the impending health condition that may affect driving or cause a crash."[17] Before the technology would be able to identify a lethal dose of alcohol, a threshold may need to be determined where once a person's level of intoxication passes said threshold, they have a low chance of surviving. If the technology identifies a driver's level of intoxication has surpassed the threshold, proprietary privacy interests would be best served by allowing the driver to remain inside their vehicle to shield the fact that they are lethally intoxicated from nearby people. Further, bodily privacy interests would be best served by preventing anyone from touching the driver, as emergency medical services might. Conversely, public interests may be best served by notifying emergency medical services so they may attempt to preserve the intoxicated driver's life.

While establishing a threshold to determine when emergency medical services should be contacted may best serve public interest, determining the threshold could prove to be an onerous task when a driver is not only intoxicated but impaired as well. Certain prescription medicines, such as sleeping pills, can have a lethal effect when combined with alcohol.[18] Therefore, although a driver's level of intoxication may be relatively low, their chance of death may be significantly high. As a solution, people who use AD&IDP technology could be required to disclose any prescription medicines they take to the agency or organization responsible for determining the threshold. However, this would constitute communication of health information, implicating bodily privacy.[19] Perhaps, in an attempt to balance the public interest in preserving life with bodily privacy interests, when any level of intoxication is detected confluently with any level of impairment, operation of a motor vehicle should be limited or prevented.

Another issue inherent to the integration of advanced drunk and impaired driver prevention technology would arise when a driver is in the process of driving and becomes intoxicated or impaired.

---

[17] NHTSA, *The Potential For Adaptive Safety Through In-Vehicle Biomedical And Biometric Monitoring*, Paper Number 15-0377, https://www-esv.nhtsa.dot.gov/proceedings/24/isv7/main.htm (last visited Apr. 12, 2022).
[18] *See, e.g.*, *Commonwealth v. Pettie*, 363 Mass. 836, 838, 298 N.E.2d 836 (1973) (expert testimony that a combination of sleeping pills and alcohol would be expected to result in death).
[19] *See infra* note 23.

By preventing or limiting the operation of the motor vehicle, the technology would either force a vehicle to stop in the middle of the road, pull over safely, or become gradually slower until ultimately the vehicle will no longer move. If preventing drunk and impaired driving is prioritized, the best solution would likely be to stop the operation of the vehicle as quickly as possible. However, to ensure bodily privacy is not restricted, a vehicle would need to arrive at a safe destination before ceasing to operate. If a vehicle is unable to safely take over the controls to do this, that vehicle could stop in the middle of a busy interstate, causing another driver to collide with the car, and ultimately causing bodily harm to both drivers.

Behavioral Privacy

Furthermore, drivers passing by a vehicle, whether it stops in the middle of the road or safely pulls to the side, may be able to infer the stopped vehicle's driver's state of intoxication or impairment. This inference will likely harm not only a person's proprietary privacy but their behavioral privacy as well, which is "typified by the privacy interests a person has while conducting publicly visible activities."[20] The probability that such an inference will be made will be the highest when the technology is first integrated, as the technology will only be required in new motor vehicles. People will likely experience restricted proprietary and behavioral privacy due to the delayed and long-lasting effects of many legal mind-altering drugs. For example, a person who typically takes anti-anxiety medicine thirty minutes before they arrive at work could be delayed by traffic, their car could detect an impairment, and their vehicle could stop a short distance from their work along the same route that each of their co-workers takes. Whether the impaired employee walks to work or asks a co-worker to pick them up, they would most likely no longer be able to shield the fact that they suffer from an anxiety disorder without lying.

[20] *Typology*, *supra* note 9, at 568.

Communicational Privacy

Prior to integrating AD&IDP technology, communicational privacy should be considered, which is "typified by a person's interests in restricting access to communications or controlling the use of information communicated to third-parties."[21] When a driver has been identified as drunk or impaired, access to the communication of such information should be restricted so that malevolent actors are prevented from hurting the driver. For example, once a driver is identified as intoxicated or impaired, a vehicle could make a distinctive noise, communicating to nearby people the driver's state of intoxication or impairment. A malevolent actor could use this information to their advantage by waiting a short period of time and pretending to be a ride-share driver. Furthermore, if insecure communications to third parties of such information provide location data as well, a malevolent actor could intercept the information and attack the intoxicated or impaired person in their home.

Informational Privacy

Synonymous with communicational privacy, informational privacy is "typified by the interest in preventing information about one-self to be collected and in controlling information about one-self that others have legitimate access to."[22] In the context of bodily privacy, efforts to preserve informational privacy would be those aimed at "restricting and controlling information about the body (e.g., health or genetic information)."[23] Specifically, when a driver has been identified as drunk or impaired, the legitimate access to such information by law enforcement and private organizations should be restricted. If the technology works as required by the II&J Act, drunk and impaired drivers should not be able to operate their vehicles without the operation being limited or prevented, negating the need to communicate health information with law enforcement.

---

[21] *Id.*
[22] *Id.*
[23] *Typology*, *supra* note 9, at 569.

Reputational Privacy Harms

Similarly, legitimate access to information that can be used to identify a person and their state of intoxication or impairment by private companies should be severely restricted. Information identifying a driver as intoxicated or impaired has the potential to cause reputational harms, which are harms that impair a person's ability to maintain personal esteem in the eyes of others; can taint a person's image; and can result in lost business, loss of employment, or social rejection.[24] Furthermore, private companies should be prevented from selling the data, as it has the potential to damage a person's reputation. The United States Supreme Court has affirmed the notion that intangible harms, such as reputational harms, can be sufficiently concrete to ensure a plaintiff has Article III standing to sue in federal court.[25] One acceptable use of the information by vehicle manufacturers and dealers would be to provide calibration, diagnostic, and maintenance services. However, in this context, manufacturers and dealers should be required to anonymize the data and periodically delete it. In doing this, manufacturers and dealers will be dissuaded from selling the data to other companies for a profit.

Issues

While MADD may have urged the NHTSA to take action to meet the deadline of the II&J Act, there are many issues that may arise from the implementation of this technology that need to be addressed before requiring the technology to be integrated into all new motor vehicles. Not only should these issues be addressed, but also assurances should be made that seek to prevent the technology from causing more harm than good. In light of the shocking statistics provided by the II&J Act, it may be difficult to prioritize privacy concerns. However, the NHTSA should be in favor of addressing each issue and providing assurances so that legislative support for requiring the integration of this technology does not falter once the technology is actually integrated. Furthermore, many concerns raised by this privacy analysis may be overcome by arguing in support of pre-existing public policies.

---

[24] *See Harms*, *supra* note 10, at 39.
[25] *See TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2200 (2021).

The list of issues below is by no means exhaustive but should offer insight into the wide range of possible outcomes of requiring the integration of advanced drunk and impaired driver prevention technology.

Issues that may arise once a driver has been positively identified as intoxicated or impaired:

1) The technology could be ineffective in preventing or limiting the operation of the motor vehicle, enabling an intoxicated or impaired driver to continue operating their vehicle and endangering public safety.
    a. Bodily Privacy – Death
    b. Proprietary Privacy – Ability to use the technology to shield facts from others
2) After a car equipped with the technology identifies a driver as intoxicated or impaired, the intoxicated or impaired driver could decide to drive an older vehicle that is not equipped with this technology or other modern safety technologies. This would lead to the intoxicated or impaired driver operating a less-safe vehicle while impaired. Where, if the technology had not been integrated into the newer car in the first place, the intoxicated or impaired driver and their passengers' lives may have been saved by other modern safety technologies.
    a. Bodily privacy – Death, restriction of bodily movement
    b. Behavioral Privacy – Inability to maintain bodily privacy while conducting publicly visible activities
3) A technologically savvy person may figure out a way to alter the information previously collected by the technology so it provides evidence tending to show an intoxicated or impaired driver was actually sober. Where, if the intoxicated or impaired driver is arrested for driving under the influence, they may be able to offer the information provided by the modified technology as evidence to escape criminal liability. If this is possible, the intoxicated or impaired driver may continue to drive in a dangerous condition without legal repercussions.
    a. Bodily Privacy – Death, communication of health information

   b. Proprietary Privacy – Ability to use the technology to shield facts from others

4) The technology could have inaccurately identified the person as intoxicated or impaired, causing a sober person to be unjustly prevented from operating their vehicle or causing a sober person to be unjustly limited in the operation of their vehicle. Furthermore, if a driver is operating a work vehicle that communicates the information collected by this technology to the employer, the driver could lose their job. Additionally, a person who is prevented from operating their motor vehicle as a result of an inaccurate identification could lose their job by failing to make timely delivery of the goods that they are transporting for their job.
   a. Bodily Privacy – Restriction of bodily movement, communication of health information
   b. Behavioral Privacy – Inability to maintain privacy while conducting publicly visible activities
   c. Informational Privacy – Health information communicated to the employer
   d. Reputational Privacy Harms – Impaired ability to maintain personal esteem in the eyes of others, loss of employment
5) The technology could have inaccurately identified the person as fatally intoxicated or impaired, preventing or limiting operation of the motor vehicle and alerting emergency medical services, potentially causing the sober driver to incur extensive medical bills.
   a. Bodily Privacy – Restriction of bodily movement, communication of health information
   b. Proprietary Privacy – Inability to shield chronic conditions from passengers
   c. Informational Privacy – EMS has legitimate access to the information
6) The technology could have accurately identified the person as fatally intoxicated or impaired while they were attempting to drive to a hospital, preventing or limiting the operation of the motor vehicle and ultimately causing the driver to die. Where, if the technology had not prevented or limited the operation of the vehicle, the person may have been able to arrive at a hospital, obtain medical assistance, and survive.
   a. Bodily Privacy – Death, restriction of movement, communication of health information

   b. Informational Privacy – EMS has legitimate access to the information

7) The technology could inadvertently communicate the driver's state of intoxication or impairment to others by preventing or limiting the operation of a motor vehicle in a distinctive manner. Also, as most people would expect a new car to operate without any issues, when first integrated, the technology could inadvertently communicate the driver's state of intoxication or impairment to others by preventing or limiting the operation of a motor vehicle.
   a. Bodily Privacy – Communication of health information
   b. Proprietary Privacy – Inability to shield state of intoxication or impairment from others
   c. Behavioral Privacy – Inability to maintain privacy while conducting publicly visible activities
   d. Communicational Privacy – Inability to restrict third-party access to health information
   e. Reputational Privacy Harms – Impaired ability to maintain personal esteem in the eyes of others
8) The technology could have accurately identified the person as impaired, even though they were only under the influence of a legally prescribed medicine, while they were attempting to drive to work, preventing or limiting the operation of the motor vehicle near a driver's place of employment, and ultimately causing the driver to be terminated as an employee.
   a. Bodily Privacy – Bodily movement restricted
   b. Proprietary Privacy – Impaired ability to shield medical condition from an employer
   c. Communicational Privacy – Inability to restrict access to health information
   d. Reputational Privacy Harms – Impaired ability to maintain personal esteem in the eyes of others, loss of employment
9) The technology could effectively limit or prevent the operation of the motor vehicle, causing the driver to be forced to stop in an unsafe location, such as in the middle of a busy highway or directly in front of a large truck. Even if no collision occurs, the technology could inadvertently cause traffic congestion. If an increase in traffic congestion is persistent immediately after this

technology is integrated, a person causing the congestion could be portrayed on the news as intoxicated or impaired.

a. Bodily Privacy – Death, restriction of bodily movement
b. Proprietary Privacy – Inability to use a vehicle to shield health information from others
c. Behavioral Privacy – Inability to maintain privacy while conducting publicly visible activities
d. Informational Privacy – Inability to restrict legitimate third-party access to health information

Issues that may arise when communicating the information collected by this technology:

10) The information used to determine the driver's state of intoxication or impairment could be communicated to law enforcement, causing a person who was prevented from driving a vehicle to be arrested, charged with driving under the influence, and ultimately subjected to a blood test.
    a. Bodily Privacy – Inability to exclude people from touching one's body, restriction of bodily movement
    b. Informational Privacy – Inability to restrict legitimate access to health information
    c. Reputational Privacy Harms – Impaired ability to maintain personal esteem in the eyes of others, loss of employment
11) The information used to determine the driver's state of intoxication or impairment could be communicated to companies tasked with maintaining the efficacy of the technology, other companies, or law enforcement. The people receiving these communications could fail to provide adequate data security measures or could sell the data, enabling malevolent actors to access it. Additionally, extraneous information could be communicated and therefore intercepted, such as location information or what prescription medicines a driver takes, increasing the risk of this technology resulting in harm.
    a. Bodily privacy – Death, communication of health information

b. Proprietary Privacy – Inability to use a vehicle to shield potentially dangerous information from others
c. Communicational Privacy – Inability to restrict third-party access to health information
d. Informational Privacy – Inability to restrict legitimate access to health information
e. Reputational Privacy Harms – Impaired ability to maintain personal esteem in the eyes of others

12) A technologically savvy person may figure out a way to cause the technology to identify an intoxicated or impaired driver as sober, enabling the intoxicated or impaired person to operate a vehicle, posing a danger to public safety. Where, if the intoxicated or impaired driver is arrested for driving under the influence, they may be able to offer the information provided by the modified technology as evidence to escape criminal liability.
    a. Bodily Privacy – Death, communication of health information
    b. Proprietary Privacy – Ability to shield facts from others
13) Establishing a general threshold of impairment that, when passed identifies a driver as intoxicated or impaired, without accounting for the various prescription medicines and how they could interact with each other and with alcohol, would likely lead to inaccurate identifications of impaired or intoxicated drivers. Drivers who take prescription medicines could be forced to disclose their medication regimen to avoid having the operation of their vehicle prevented or limited. This disclosure may need to be directed to an agency or company responsible for determining a threshold for when a driver is intoxicated or impaired or a threshold for when a driver is fatally intoxicated or impaired.
    a. Bodily Privacy – Communication of health information, restriction of bodily movement
    b. Proprietary Privacy – Inability to use a vehicle to shield health information
    c. Behavioral Privacy – Inability to maintain privacy while conducting publicly visible activities
    d. Informational Privacy – Limited ability to restrict legitimate access to health information

Solutions

To prevent unnecessary reputational harms from occurring, a positive identification of intoxication or impairment should be followed by a discrete notification to the driver. If the vehicle is already in motion, following the notification, the driver should be given a designated period of time to pull over at a safe location. Ideally, this notification would not alert the passengers to the positive identification unless the driver fails to pull over within the designated period of time. This would aim to prevent reputational harms in the event of a false positive. Additionally, bodily privacy may be promoted by allowing people to drive their car, temporarily, away from a dangerous situation.

Alternatively, drivers should be afforded the opportunity to temporarily override the technology and resume operation, at least when the technology is first integrated. The override may need to be approved by an agency responsible for maintaining the technology so that severely intoxicated or impaired people are not allowed to continue driving. This way, any issues regarding precision, sensitivity, and reliability may be overcome. Although indefinitely allowing an override would defeat the essential purpose of the technology, specific situations may necessitate the need for an override. For example, a driver who has been prevented from operating their vehicle while going over a bridge with no shoulder or sidewalk may need to drive to escape the danger of another vehicle colliding with their vehicle or their body. Also, when a driver has been identified as fatally intoxicated or impaired, that driver may be on their way to a hospital. In this situation, a temporary override may be necessary and could be revoked if the driver veers off course.

Furthermore, to ensure precision, sensitivity, and reliability, additional information collection is likely required. Part of this information collection should consist of the input of various prescription medicines and their dosages so that drivers who are legally prescribed certain medicines do not experience false positives. Once integrated, the NHTSA should implement a system similar to the

Transportation Security Administration's Redress Control Number system.[26] Under this system, affording a driver a wider scope of sensitivity as a result of being prescribed certain medicines should only be allowed when the prescribing doctor has confirmed the driver's medication regiment. By requiring a doctor's approval, the risk of abuse should be severely diminished.

Also, as part of the extended information collection, cybersecurity and information security specialists should be consulted to develop a framework conforming to the privacy policies framework VIIC identified for V2V technology.[27] Implementing such a framework will minimize the risk of intercepted communications and the reputational harms that may occur as a result. Additionally, by enhancing security, people should be precluded from altering the information created by AD&IDP technology and from causing the technology to produce a false negative.

To prevent the information collected by AD&IDP technology from being used to terminate an employee, employers should be precluded from accessing the information produced by this technology. The NHTSA should seek to only allow manufacturers or agencies tasked with carrying out calibration, diagnostic, and maintenance services to access such information. This should prevent reputational harms while also promoting behavioral, bodily, and informational privacy. Although an employer may wish to prevent their employees from driving in an intoxicated or impaired condition, other technologies can be purchased and implemented.

To prevent the NHTSA from regulating beyond its defined purpose, the information collected by AD&IDP technology should not be communicated with law enforcement or used as evidence in a criminal trial. If possible, this will prevent the information produced by AD&IDP technology from being used by a drunk or impaired driver as exculpatory evidence. Additionally, restricting the communication

---

[26] DHS, Transportation Security Administration, *Redress Control Numbers*, https://www.dhs.gov/redress-control-numbers#:~:text=The%20Redress%20Control%20Number%20(redress,the%20watch%20list%20matching%20process. (last updated Jan. 01, 2022) (last visited Apr. 12, 2022).

[27] NHTSA, *Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application*, August 2014, 146, https://www.nhtsa.gov/staticfiles/rulemaking/pdf/V2V/Readiness-of-V2V-Technology-for-Application-812014.pdf (last visited Apr. 12, 2022).

of information produced by AD&IDP technology will lessen the potential for the information to be intercepted by third parties. In doing so, bodily privacy will be promoted by keeping health information private and preventing malevolent actors from using the information to cause bodily harm to a driver. Furthermore, preventing the information from being intercepted by third parties will reduce the risk of reputational harms resulting from the integration of this technology.

By requiring the technology to only be integrated into newer cars, many people suffering from alcohol and substance abuse disorders may simply drive older vehicles that aren't equipped with current life-saving technology. In a perfect world, every motor vehicle would be integrated with this technology. However, to realistically achieve traffic safety, the NHTSA should recommend to legislators that they create tax incentives that would be afforded to people who choose to have this technology installed. Additionally, the NHTSA should seek to have the integration of this technology into older vehicles subsidized so that the general public is more willing to embrace the technology.

Conclusion

While many people may find it egregious to advocate for privacy-based solutions prior to the integration of AD&IDP technology in light of drunk and impaired driving's continuously growing death toll, "[N]ot a single aspect of privacy takes absolute precedence over other rights and interests."[28] Therefore, the various harms to privacy each issue presents should not be outweighed by each other or by the public interest in preventing thousands of drunk and impaired driving deaths each year. Rather, each issue should be addressed in light of a totality of the circumstances to ensure the integration of advanced drunk and impaired prevention technology is more beneficial than it is harmful. While many of the issues and solutions presented may be outside the scope of the NHTSA, the NHTSA may be able to use its significant political power to address them.

[28] DE HERT P. & S. GUTWIRTH, *Privacy, data protection and law enforcement. Opacity of the individual and transparency of power* in E. CLAES, A. DUFF & S. GUTWIRTH (eds..), *Privacy and the criminal law*, Antwerp/Oxford, Intersentia, 2006, 72. (ISBN 90 5095 545 2).

As previously noted, bodily privacy interests are implicated when people are killed or injured, when bodily movement is restricted, when people are forced into dangerous situations, and when health information is communicated. Proprietary privacy interests are implicated when people are unable to use their vehicle to shield information, facts, or activities from others. Behavioral privacy interests are implicated when people conduct publicly visible activities, such as driving or sitting in a car that has been prevented from being operated. Communicational privacy interests are implicated when people are able to access or use the information being communicated by a vehicle equipped with AD&IDP technology. Informational privacy interests are implicated when information about drivers is collected and when legitimate access to such information is controlled. Reputational harms may occur when people lose employment, create traffic congestion, or are forced to disclose their medication regimen as a result of this technology.

To promote privacy, further public policy goals, and prevent reputational harms from occurring, employees should be assured that they will not be legally terminated as a result of this technology. Also, once a positive identification has occurred, a driver should be discreetly notified and either be given a grace period to pull over safely or afforded the opportunity to override the technology. Further, people who take certain prescription medicines should be afforded the opportunity to input their medication regimen into a system, with their doctor's approval, which would afford that person a wider scope of sensitivity. Moreover, further consultation with cybersecurity and information security experts to develop a privacy policy framework is likely necessary to prevent communications from being intercepted and to prevent the technology from being tampered with. Additionally, information produced by this technology should not be communicated to law enforcement or be used as evidence in a criminal trial. Lastly, the NHTSA should use its political power to promote granting subsidies and tax incentives to people who decide to integrate this technology into their vehicle.

Without adequate assurances that each type of privacy previously listed can be sufficiently balanced against conflicting ideals, the required integration of AD&IDP technology may be premature and beyond the NHTSA's scope of regulatory authority.