70 Am. J. Comp. L. i39

American Journal of Comparative Law
October, 2022

U.S. National Reports to the 2022 General Congress of the International Academy of Comparative Law in Asunción, Paraguay
María Lubomira Kubica[a1]

Copyright © 2022 by American Society of Comparative Law, Inc.; María Lubomira Kubica

*i39 AUTONOMOUS VEHICLES AND LIABILITY LAW[d1]

Introduction

Mobility provided by autonomous vehicles (AVs) has become a trending topic in modern society, an object of debate all over the world.[1] Experts estimate that the introduction of "self-driving" or autonomous vehicles onto public roadways will result in as much as an 80% to 90% decrease in accidents.[2] These estimates reflect the fact that over 40% of fatal crashes presently are due to alcohol or drug consumption, distraction, or fatigue. The remaining accidents happen because of speeding, aggressive driving, overcompensation, inexperience, slow reaction times, inattention, and various other driver shortcomings. Consequently, human driver error accounts for over 90% of all accidents. AVs, on the other hand, neither drink nor write text messages when driving. They employ a program precluding them from breaking traffic laws. They have faster reaction times and can be optimized to ease the flow of traffic.[3]

It will be some time before fully autonomous vehicles are available in the market.[4] Even then, conventional vehicles (CVs) will not ***i40** suddenly disappear from sales and public roads. We will have to deal with a long transition period during which vehicles of all types will coexist until fully automated cars replace CVs entirely. To this panorama should be added cyclists, motorcyclists, and pedestrians, all of whom can also become the cause or victim of an accident. The result will be an evolution of the traffic mix and the occurrence of mixed accidents taking place throughout the transition period until the total dominance of fully automated cars.[5]

The current approach in the United States to liability for a car accident is to place the burden of paying damages on the human driver, since it is the driver's conduct that led to the accident. More specifically, U.S. states generally follow a system that merges compensation through first-party (the injured party's own) insurance together with the ability to bring a traditional fault action in torts, although this can vary from state to state. No-fault legislation in a minority of states (twelve) largely limits victims' claims to their own insurance. Only in exceptional cases, when the monetary or serious-injury "threshold" is met, can the victim in these states take advantage of the general negligence action to recover non-compensated losses. Most states, however, allow injured parties to bring a tort claim against the negligent driver without such limitations. While claims against the car manufacturer based upon the sale of a defective product are possible, in practice they are rare since driver error constitutes the main cause of almost all accidents (90%). Indeed, car defects account for as little as 2% of the total number of accidents.[6] (While defects that impact the extent of injuries in an accident, so-called crashworthiness, might produce products liability claims, this is not particularly relevant to the concerns raised by liability and CVs.)

The main problem of this approach in most countries, including the United States, is that it only considers conventional traffic in which the vehicle is under the total control of the human being.[7] This will no longer be the case in accidents caused by fully autonomous vehicles. Yet different issues arise when control of the vehicle is divided between a partially autonomous car and

a human being. Numerous experts in the United States have suggested that the introduction of AVs should be preceded by the adoption of a completely new regime or a revision of existing laws concerning liability for accidents caused by AVs.

***i41** The most obvious issue in such proposals is who will be liable. There are several possibilities: the automotive company (car manufacturer), the supplier, the software provider, the software operator, the AV owner, the driver, the car's occupants, the insurance company, among others.[8] Since part, or all, of the responsibility for causing the accident could be placed on the AV, the potential to invoke claims based upon product defect would increase. The situation will be even more complex in the case of partially autonomous vehicles, where one could ask if it is appropriate, for instance, to make the human driver liable for failing to use the manual override function available in the car.[9] If liability is attached to more than one subject, the additional issue of its apportionment arises.[10]

Privacy and data protection is another key topic related to the use of AVs that has already been addressed by U.S. laws.[11] It has been defined as "the most slippery territory for autonomous vehicles."[12] The problem is that artificial intelligence--in the form of the vehicle's autonomous systems, which totally or partially replace the driver--requires the submission of data from a significant number of sources to enable the proper functioning of an AV. For the management of traffic at intersections to be efficient, for the distribution of traffic to be intelligent and aimed at minimizing congestion, and for autonomous vehicles to travel safely in close-packed platoons, AV manufacturers are required to establish communication both between individual AVs and other AVs in their proximity, and between the autonomous vehicles and an external network.[13] Being necessary to assess the driving environment and control the operation of the vehicle, these data are also likely to affect three types of privacy interest: autonomy privacy interests, personal information privacy interests, and surveillance privacy interests.[14]

Finally, the different approaches to new technologies allow the classification of scholars and policymakers into two opposing ***i42** categories: generalists[15] and exceptionalists.[16] However, the greatest problem has been identified elsewhere. The real issue here is not whether to adapt existing laws or create technology-specific laws, but rather how to ensure that judges and legislators do not misunderstand the emerging digital world. A poorly conceived perception of IT tools on the part of the courts and legislative bodies might enable their improper use and undermine fundamental rights. With this in mind, it is essential to differentiate in practical terms between old and new technologies in order to avoid the incorrect use of precedent leading to the erosion of the very principles that the old rules deriving from it originally aimed to protect.[17]

I. Different Levels of Automated Driving Systems

In 2013, the National Highway Traffic Safety Administration (NHTSA) released its first policy on AVs in its *Preliminary Statement of Policy Concerning Automated Vehicles*.[18] This defined five different levels of autonomy (levels 0 to 4).

In September 2016, the NHTSA decided to update this approach in another policy statement which established some guidelines for the imminent transition of a roadway towards the presence of highly automated vehicles (HAVs) and adopted the Society of Automotive Engineers (SAE) classification of automation levels.[19] Consequently, AV capabilities are now defined in the United States in SAE International Standard J3016, jointly developed by European, American, and Australian authorities in search of a common language in the field.[20] The SEA distinguishes between six levels of automation. The scale comprises vehicles from level 0 to level 5, with the former indicating no automation at all and the latter full automation. Placement in one category or the other depends on the way in which steering and braking are controlled, if and to which extent the AV can operate without human control, and if this is possible in all situations.[21]

***i43** II. Specific Legal Rules Aimed at Including Self-Driving Cars in Road Traffic or In-Town Circulation

 © 2024 Thomson Reuters. No claim to original U.S. Government Works.

The speed and the extent to which the autonomous driving technologies are implemented can be partially determined by the corresponding government actions. In the United States, the competent federal government authority in this field is the NHTSA. An example of the agency's influence is the NHTSA's New Car Assessment Program (NCAP),[22] in which the NHTSA recommends to consumers what the agency views as the most reliable advanced crash avoidance technologies and the vehicles using them. The NHTSA's main objective is to ensure the safety of motor vehicles and, as such, it was long expected that the NHTSA would become an important agent not only in monitoring, fostering, and conducting research on AVs, but also in establishing new laws regarding autonomous driving technologies.[23]

U.S. state-based regulation in this field previously barely existed because of arguable federal preemption,[24] as a result of which the NHTSA carried out research on AVs for a number of years with the aim of introducing adequate regulation.[25] The initial expectation regarding the NHTSA's leading role in AV rulemaking was replaced by pessimism in the years that followed.[26] The agency has been criticized by long-term observers--as voiced in recent congressional hearings--for its constant lack of legislative initiative or for not being able to avoid delays in adopting safety standards.[27]

In the United States, both the registration of motor vehicles and the licensing of drivers fall within the scope of state law.[28] The NHTSA currently recommends that states not give permission for the public use of AVs until further conclusive research is done.[29] Perhaps inconsistently, the agency has stated that public use of AVs "is encouraged ***i44** by innovation in automated driving and their potential to transform our roadways."[30]

Some scholars argue that no specific legislation is needed for AVs to be legal on American roads.[31] Even so, in 2011, Nevada became the first state to implement rules governing autonomous cars, followed by Florida (2012)[32] and California (2012).[33] Currently, most states have similar legislation, and several others have issued executive orders related to autonomous vehicles.

There no room in this Report to analyze each and every state regulation on autonomous vehicles. In brief summary, all aim to foster the safe development, testing, and operation of AVs on public roads. Florida's Committee Substitute House Bill (CS/HB), for instance, announced that its legislature has a clear intent to promote autonomous technology,[34] "finds that the state does not prohibit or specifically regulate the testing or operation of autonomous technology in motor vehicles on public roads," and affirms that a "person who possesses a valid driver license may operate an autonomous vehicle in autonomous mode."[35] California's Senate Bill (SB) 1298 of 2012 similarly states the legislation's intent to both promote and ensure the safety of autonomous technologies.[36] Explaining that the state "presently does not prohibit or specifically regulate the operation of autonomous vehicles,[37] the legislation seeks to establish basic requirements for AV testing on roads[38] and for operating an autonomous vehicle,[39] including foreseeing the possibility of operating an AV without a driver inside. The legislation specifies the steps necessary to approve such an operation, and requires a remote driver who can engage or disengage the autonomous technology if the need arises. Finally, the State of Tennessee has forbidden local governments from barring the use of AVs on their roads.[40]

This proliferation of state legislation gave rise to considerable concern among autonomous vehicle industry representatives. When asked to assess the impact of state actions on their business at a hearing of the Energy and Commerce Subcommittee on Digital Commerce and ***i45** Consumer Protection in February 2017, many replied that they were worried about a possible significant negative effect that the patchwork of state laws might have on the future of the industry.[41] In parallel, some comments on state legislation from the public received by the NHTSA stressed that these regulations reflected several disparate approaches to adding to and amending state authority over AVs, and the agency was thus asked by both public commentators and state actors to deliver some guidance or even regulations that take into account a more national approach in the field of testing and rolling out AVs.[42]

 © 2024 Thomson Reuters. No claim to original U.S. Government Works.

Consequently, the preemption principle and the delimitation of federal and state roles in AV regulation became two of the most urgent and important issues that needed to be addressed by the NHTSA. The agency soon positioned itself on the issue in its policy statement of 2017, titled *Automated Driving Systems 2.0. A Vision for Safety* ("*AV 2.0*").[43] Generally speaking, it remains within the NHTSA's authority to regulate motor vehicle and motor vehicle equipment safety, while states are responsible for regulating the human driver and most other aspects of motor vehicle operations, included insurance and liability issues.

The main goal of the NHTSA, as explained in *AV 2.0*, is to guarantee a consistent and uniform national regulatory framework for AVs so as to avoid the creation of unnecessary barriers to their rollout and operation. To achieve this objective, in September 2014, the NHTSA entered into a two-year collaborative agreement with the American Association of Motor Vehicle Administrators (AAMVA) leading to the creation of the Autonomous Vehicle Best Practices Working Group. This group was entrusted with the task of organizing and disseminating information related to the development, design, testing, use, and regulation of AVs and other emerging vehicle technologies. The report prepared by the group is meant to provide uniformity between different state legislations and a "baseline safety approach to possible challenges" of the regulatory framework concerning AVs. In line with this report, the states are expected to revise their existing regulatory framework and ensure the implementation of policies that, although not identical, could guarantee the consistency necessary for innovation and the swift, widespread, and safe incorporation of AVs onto public roads at a national level.[44]

Among the best practices for legislatures identified by the NHTSA in *AV 2.0*, those that stand out include the requirements to provide a "technology-neutral" environment and to review traffic laws and regulations that may serve as barriers to the operation of AVs. With ***i46** reference to the former, *AV 2.0* strongly suggests that states, where it is not necessary, should not diminish competition and innovation by imposing the requirement that only motor vehicle manufacturers can test and roll out autonomous vehicles. In other words, every entity that complies with federal and state laws on the testing and rollout of AVs should be granted the possibility of operating in the state. As for traffic laws and regulations, these should neither limit nor prevent the testing or introduction of AVs on public roads by, for instance, demanding that a human operator always have one hand on the steering wheel. Such a requirement would impede the circulation on roads of AVs with levels 3 to 5 of automation.[45]

Further best practices have been developed in *AV 2.0* for state highway safety officials, although the NHTSA has explicitly underlined that it does not expect states to create any new processes and requirements aimed at fostering AV activity. Such guidelines are meant to support only those states that are thinking of introducing or are already in the process of establishing regulatory measures.[46]

In this way, the NHTSA's voluntary guidelines respond to what has been recognized by scholars as an essential need of the regulations on automated vehicles to find a balance between two competing objectives: protecting public safety, on the one hand, and enhancing innovation in automated technology, on the other. In other words, the undue risks posed by immature and inadequately engineered automated driving systems that may lead to crashes should be balanced against the possibility of better performing and safer vehicles in the long run. To find such a balance may not be easy due to the significant amounts of both judgement and science involved in this issue.[47]

While *AV 2.0* focuses on detailed safety recommendations for AVs, the NHTSA's subsequent policy statement, *Preparing for the Future of Transportation: Automated Vehicles 3.0*,[48] similarly addresses safety but without losing sight of the counter-objective of fostering the effective incorporation of automated driving systems test vehicles onto public roads and enabling their safe interaction with conventional cars, pedestrians and other public road users.[49]

Finally, the NHTSA has identified another factor that could render the incorporation of AVs onto U.S. public roads ineffective ***i47** if not addressed properly--public perception of the risk associated with automation.[50] Accordingly, the report from the National Science and Technology Council and the United States Department of Transportation, titled *Ensuring American Leadership in Automated Vehicle Technologies. Automated Vehicles 4.0*,[51] aims to build upon public confidence in these

 © 2024 Thomson Reuters. No claim to original U.S. Government Works.

emerging technologies. The report states that the U.S. Government will take all the steps necessary to guarantee that "entities do not make deceptive claims or mislead the public about the performance capabilities and limitations of AV technologies, including, for example, deceptive claims relating to vehicle safety or performance."[52]

III. Data Security is Needed for the Use of Self-Driving Cars: AVs and Privacy Issues

One of the earliest in-depth American analyses on how the use of AVs can affect the right to privacy was conducted by Dorothy Glancy in 2012. For the purposes of the research, Glancy distinguishes between self-contained autonomous vehicles and interconnected autonomous vehicles, as these two models present very different implications for privacy.[53] According to another study, conducted by a scientist from Berkeley, the term *autonomous vehicles*, when employed properly, can only refer to vehicles in which functions that go beyond the decision-making process--involving information acquisition in support of environment perception--are developed by the vehicle's self-contained systems without the need (and possibility) to communicate with the external network or infrastructure. This model would correspond to what Glancy understands by the term *self-contained autonomous vehicles* and what the scientist from Berkeley decided to simply name *autonomous vehicles*. *Interconnected autonomous vehicles* (or simply *connected vehicles*) "use communications with the infrastructure or other vehicles to acquire information or to negotiate maneuvers, they have 'cooperative' rather than 'autonomous' automation systems."[54]

Both models use privacy-sensitive data, but self-contained autonomous vehicles might be perceived as less vulnerable than interconnected autonomous vehicles in this regard for at least two reasons: First, they are not supplied with information or control messages ***i48** from outside the vehicle; second, the vehicle status information is retained within the vehicle and is not shared with an external network. Interconnected autonomous vehicles, described by Glancy as "puppet vehicles" under remote control, can present more risks to privacy as they are subject to a vehicular network that is external to the vehicle.[55]

A. Privacy Interests Involved

Glancy points to three potential privacy interests that in her opinion can, on the one hand, affect public reliance on AVs and, on the other, will influence the future law on AVs, with the possible outcome of some legal restrictions being placed on the design and operation of AVs. These interests are personal autonomy, personal information, and surveillance.[56]

1. Personal Autonomy Privacy Interests

Personal autonomy has been described as the interest related to control and self-determination, that empowers people with the right to decide their destiny independently. Within the analytical framework of this section, personal autonomy can be understood as perceiving the vehicle as a significant tool of personal choice, power, and control. As such, personal autonomy enables an individual to establish control over the following issues: "where she is now, where will she go next, when she will depart, how she will get there and with whom, as well as who can predict or decide where, when, and how she will travel in the future."[57]

From a functional perspective, there are two sides to autonomy privacy: positive and negative.[58] When applied to transportation choices, the positive side of autonomy privacy consists of one's right to decide where to go, how to get there, whether to travel or stay at home, and when to travel, for instance, as well as whether to drive a conventional car or choose an autonomous vehicle.[59] The negative side of autonomy privacy is perfectly expressed by Warren and Brandeis's now famous wording, "the right to be let alone,"[60] which means that an individual is granted a positive freedom that encompasses decisions taken independently, that is, "without observation, intrusion, or ***i49** interference."[61] The degree of intrusion in AVs, that is to say, whether an AV enables or precludes such interference, will largely depend on its design and how it was manufactured.[62]

 © 2024 Thomson Reuters. No claim to original U.S. Government Works.

Among the potential interferences with autonomy privacy, Glancy mentions the possibility of compiling personal information generated by an AV into a consumer profile that can later be employed as an unchosen "stand-in," or alter ego, for the AV's user. In the future, such a profile may be imposed within transactions, eliminating the actual individual and consequently interfering with the person's self-definition. This autonomy privacy right to self-definition is protected under U.S. law by privacy tort actions, privacy status, and regulations.[63] Another risk related to autonomy privacy is the capacity of AVs to locate users (and thus possibly interfere with their decision of which destination to choose), this being because a person's location is a factor that helps define that person's identity. Also, there might be physical and psychological intrusions from censors or snoopers that violate personal autonomy since every person has the right, in the United States granted by the Driver's Privacy Protection Act,[64] to drive anonymously. This act, passed at a federal level, bans state motor vehicle departments from any unpermitted disclosure of driver and vehicle licensing records that enables the identification of a person.[65] Another point is that AVs should be designed to allow the possibility of preventing, when moving from one location to another, the user being targeted with location-based advertising. Protection against governmental encroachment is provided for in the Bill of Rights to the U.S. Constitution.[6667]

The principal remedies that allow the safeguarding of autonomy privacy mentioned by Glancy include the individual user's affirmative choice, fully informed consent, and anonymity. All of these raise great challenges for autonomous vehicle developers. On the one hand, they would have to translate sophisticated technical information into easily understandable language so as to secure informed individual consent. On the other, introducing anonymity in interconnected autonomous vehicles may imply a drop in security due to the fact that it will no longer be permitted to trace misbehaving technology, detect antisocial activity, or prosecute individuals who participate in unlawful network activities. However, none of these latter concerns was sufficiently important for the U.S. Supreme Court when, in *United States v. Jones*,[68] ***i50** it established that it is essential in a democratic society whose aim is to elude authoritarianism to recognize the individual's right to choose anonymous personal mobility.[69]

2. Personal Information Privacy Interests

AVs will become the source of a large amount of data, some of which, when linked to a specific person, might well be treated as personal information. Origin and destination data, real-time and historical location information, or, put differently, the identified autonomous vehicle user's movements in physical space, as well as detailed behavioral data, are just some examples of the many types of personal information that may be generated in the future by AVs. All of this information will enable identification of the machine user's personality, behavior, and personal preferences. To match the owner with the self-driving vehicle will be especially easy at the beginning of AV commercialization, when such vehicles will be rare and the very presence of an AV on the road may be enough to identify its user.[70]

a. Interferences with Personal Information Privacy Interests in the Context of AVs

The AV-generated personal information use that can interfere with personal information privacy interests can be of several different kinds, according to Glancy. We will probably find companies using it for targeted marketing and advertising.[71] Also, one can imagine AV users being followed, stopped, questioned, or even having their identity stolen, by someone with access to the system. This information is of particular interest and value to government, law enforcement, and intelligence agencies, as it can help to capture and further investigate suspicious individuals or prosecute suspects. Such information also allows an individual's future location to be predicted and established.[72] As was pointed out by the U.S. Government Accountability Office, "[i]f disclosed or posted, location data may be used by criminals to identify an individual's present or probable future location, particularly if the data also contain other personally identifiable information."[73]

A very complex intimate portrait of an individual--including very sensitive information, such as habits, sexual orientation, beliefs, ideology, and behavior patterns, and potentially uncovering information on a possible affair, frequenting church, buying

a gun, having ***i51** an abortion, attending Alcoholics Anonymous meetings, or being associated with a political organization, for example--can be created based on locational tracking data generated by AVs.[74] This has not go unnoticed by the U.S. Supreme Court, who in *United States v. Jones* declared:

> Disclosed in [GPS] data ... will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, the synagogue or church, the gay bar and on and on.[75]

This is without mentioning data that could be derived from the synchronization of a mobile device with the vehicle or the vehicle with a device located in the driver's home, such as the currently much-used Alexa from Amazon.[76] Moreover, personal information generated by AVs can be further coupled with other information, this leading to more complete and more detailed profiling. For instance, if the AV's user usually parks overnight in a high-income residential neighborhood, the user is likely to be identified as wealthy and willing to shop in high-end retail stores. Consequently, once this label is stuck firmly on, the user could easily be subject to choice manipulation, as the advertisements specifically offered will be limited to expensive products.[77]

b. The "Third-Party Doctrine"

The personal information generated by AVs will pose even greater threats to privacy when transmitted or disclosed to others. The "third-party doctrine" grants easier access under court or administrative order to personal data (sometimes without prior notification to the privacy right holder in question) if the data is stored by someone other than the data subject. In such cases, neither a warrant nor probable cause is required, even when they would be if the data was held by the subject of the data. This is because "a person cannot have a reasonable expectation of privacy in information disclosed to a third party" and without such an expectation there is no search or seizure triggering the requirement for a warrant or probable cause.[78]

***i52** Scholars warn of that this sort of unthinking application of traditional legal rules to new technological facts could lead to a weakening of the privacy protection.[79] Currently, American courts have developed a two-tier method of dealing with new technology cases under existing precedents: they either fit the case into old standards or create new tests to establish the reasonable expectation standard of *Katz*.[80]

United States v. Maynard,[81] a landmark precedent subsequent to *Karo*[82] and *Knotts*,[83] however, creates a unique basis for the deauthorization of intensive monitoring without recourse to the automation rationale. The novel technique applied in *Maynard* consists of applying to the Fourth Amendment an adapted mosaic theory, developed in cases based on the Freedom of Information Act.[84] Mosaic theory distinguishes between a separate and personally sensitive piece of information, such as where in a public space a car is parked at a particular time, and a GPS tracker that collects information on a car's location in public spaces over a period of time. Revelation of such separate and personally sensitive piece of information will not be considered a search under the Fourth Amendment, while patterns and personal information that could be derived from the information collected by GPS will allow the establishment of personal data that in the opinion of the court should be protected by a warrant.[85]

In fact, the AV context is not the only one in which the "third-party doctrine" has aroused severe criticism. The rapid development of self-driven vehicles has only strengthened the discourse, the doctrine having long been called obsolete and ill-suited to the digital age in which almost all communications are by default entrusted to third parties.[86] This concern is expressed by the concurring opinion of Justice Sotomayor in *United States v. Jones* when she states that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information ***i53** voluntarily disclosed to third parties,"[87] especially in the digital age.[88]

 © 2024 Thomson Reuters. No claim to original U.S. Government Works.

Other critics opposed to the traditional third-party doctrine, which considers a combination of reasonable expectation and physical trespass, underline that the third party doctrine does not suit a modern society in which physical trespass is no longer needed for information to be obtained and the expectation of privacy is ever-changing due to new technologies and current events.[89] All of these arguments have led some scholars to take the view that the "third-party doctrine" should be completely abandoned and that law enforcement officers should always be required to obtain a warrant to gain access to requested information.[90] Some scholars have pointed to other channels for attacking the doctrine, including the fact that the doctrine has been rejected at the state level. Specifically, eleven states implicitly reject the doctrine in their constitutions, while ten others leave room to believe that they might do so in the future.[91]

There are, however, some voices among American scholars which argue that a complete elimination of the "third-party doctrine" is not desirable as it could constitute a real threat to law enforcement investigations. Certain aspects of the doctrine should therefore be maintained, for instance, when allowing access to bank records[92] or pen registers.[93] The third party doctrine should only be suppressed in those cases where the information was not shared with other actors willingly. In other words:

> Voluntary disclosure to third parties using new technologies should be afforded no protection. On the other hand, information that is not affirmatively or voluntarily shared, yet is accessible by third parties as a result of new technology, should be protected by the strongest form of Fourth Amendment protection--a warrant requirement.[94]

Under this approach, whether information was voluntarily revealed to a third party should depend upon the reasonable expectation test established in *Katz*; the purpose of the disclosure; the frequency of transmission; and public access to the information.[95]

***i54** Another idea on how to extend protection of the right to privacy into the digital age without completely doing away with the "third-party doctrine" comes from Matthew Tokson.[96] Tokson's theory is based on an in-depth analysis of available data about the behavior and the privacy expectations of Internet users, and according to his findings and conclusions, Internet users tend to make a sharp distinction between two very different situations: first, the information is disclosed to an automated system that is unable to actually understand the content of the information; second, the information is shared with a human being. In the former scenario, privacy is not threatened as long as the information is relayed to the machine voluntarily. This fact, in Tokson's opinion, has not been taken into account by the courts, who automatically started dealing with automated Internet systems as if they were equivalent to human beings.[97]

3. Surveillance Privacy Interests

Glancy distinguishes surveillance privacy interests as a separate category as they go much further than just the autonomy and personal information interests of individuals, having the potential to compromise the whole political and social well-being of American society.[98] The situation was perfectly described by Supreme Court Justice Sonia Sotomayor in her concurring opinion in *United States v. Jones* when she declared that "[a]wareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible of abuse."[99] "[M]aking available at a relatively low cost such a substantial quantum of intimate [GPS location] information about any person whom the Government, in its unfettered discretion, chooses to track" may "alter the relationship between citizen and government in a way that is inimical to democratic society."[100]

Within surveillance, scholars frequently identify two different categories: covert and overt surveillance. The latter term is used to describe an activity whose aim is, through openly watching, to influence the behavior of the person being observed. In the

 © 2024 Thomson Reuters. No claim to original U.S. Government Works.

context of AVs, overt surveillance could lead to a modification of users' conduct related to speed limits, smoking, or drinking alcohol, to mention just a few examples. This could happen because, for instance, every single breach of the speed limit would be instantly reported to the enforcement ***i55** agencies, which would force the AV user to comply with traffic regulations in the future. Thus, in the words of Glancy, "[o]ne purpose of overt surveillance is to interfere with individual autonomy through the power of scrutiny."[101]

On the other hand, covert surveillance involves the secret monitoring, collecting, and reporting of personal information and includes targeted surveillance and mass surveillance. It could result in a major threat to self-driving car users as sophisticated AV technology could frequently preclude ordinary people from understanding the risk posed by covert surveillance.[102] The main difference between targeted and mass surveillance is the subject at whom it is aimed: in the former, it is a specific identified person, while in the latter, it is everyone who falls within an area or sector. One can also imagine large-scale surveillance of a whole population that could be used as an instrument of control over every individual's behavior within this population.

Targeted surveillance in the form of vehicle tracking without a warrant was held to be unconstitutional by the U.S. Supreme Court in *United States v. Jones*.[103] This type of surveillance will operate differently depending on whether the autonomous vehicle is self-contained or interconnected. The latter type, due to its main characteristics, namely its continuous access and connectivity to an external network and other vehicles and devices, if not secured by data encryption and anonymity, could provide immediate remote access to the real-time location of the autonomous vehicle and its user, as well as to the records of the user's past locations. Targeted surveillance in the case of self-contained autonomous vehicles would be more difficult, as the lack of connection to an external network would preclude remote real-time tracking, unless the vehicle was attached to a tracking device. Nevertheless, the records of past itineraries available on the computer system within the vehicle could be misused by those with access to them, even though this would probably be forbidden by burglary and other laws. Targeted surveillance requiring access to information stored in a self-contained autonomous vehicle would likely need both probable cause and a warrant. Finally, this type of surveillance has been described by Glancy as that which places at risk a very important aspect of individual autonomy--"the ability to resist being categorized, manipulated psychologically, intimidated or mechanistically predicted by society or the government."[104]

Meanwhile, mass surveillance allows for the creation of behavior patterns in, and detailed profiles of, AV users, which could serve the following purposes: (i) the generation of an algorithmic profile of an ordinary/typical AV user; (ii) the prediction of each individual user's ***i56** behavior; and (iii) the identification of the user who will or will not comply with the created pattern. The argument according to which the unencrypted information captured by mass surveillance is necessary for most transportation management and planning was not convincing to Glancy as, in her opinion, the anonymous data of both the vehicle and the driver are quite sufficient for these purposes. Patterns and profiles generate by AV data can have multiple uses, serving as valid input not only for enforcement agencies, but also in the private sector for marketers and advertisers who are willing to predict and manipulate future consumer behavior.[105]

B. Proposals for the Future

Some of the regulatory proposals are aimed at creating a flexible legal framework, a *soft law* regime that could be achieved through a third-party certification system. Within this approach, the Privacy by Design system, in force in Canada, is currently touted as the most appropriate.[106] In the United States, this concept has been long promoted by general privacy specialists such as Helen Nissenbaum,[107] has been proposed as an effective strategy for optimizing privacy in the case of online technologies by the Federal Trade Commission (FTC),[108] and has also been positively received by the White House.[109] Specifically with respect to the transportation sector, Privacy by Design was touted in 2008 as a desirable solution for intelligent transportation systems.[110]

 © 2024 Thomson Reuters. No claim to original U.S. Government Works.

Privacy by Design (PbD), whose origins can be traced back to the mid-1990s, has been described as a holistic concept. Dr. Anne Cavoukian, Ontario's Information and Privacy Commissioner, did much to popularize PbD in Canada. The main goal of PbD is to embed privacy into IT systems, accountable business practices, and physical design and network infrastructures. The idea is to create a soft law that would establish and implement the fundamental principles of Fair Information Practices into the design, operation, and management of information processing technologies and systems.[111]

***i57** Comparative law literature deems such *soft law* to be a more efficient and desirable solution than setting forth detailed regulation centered on AI for at least three different reasons: (i) no matter how adequate the regulations created for the protection of personal data may be, the rapid advance of AI will easily go beyond the limits of legal coverage; (ii) as AI gets exponentially smarter, humans may not be able to keep up with its progress, further limiting their understanding of what privacy protection should encompass; and (iii) the judicial mechanism of granting compensation or another remedy to a victim, after the passage of an often considerable period of time, is not adequate to solve the current problems related to AI and privacy.[112] Illustrating the second reason, the unpredictability of AI robots is the main factor rendering the "reasonable expectation of privacy" test an ineffective approach to privacy protection in an AI-driven world.[113]

Those who favor a traditional regulatory regime for AVs advocate a new and coherent legal framework that could guide and foster the driverless car revolution. Because these vehicles will operate across the borders of different states--and consequently laws regulating communication, cybersecurity, and privacy issues in AVs will be of an interstate nature--in their opinion, such a regulation should be enacted at the federal level. This task should be entrusted to a dedicated consortium of federal government agencies, created either through executive order or by Congress, charged with sharing up-to-date industry information between the entities that would form part of the consortium, such as, at a minimum, the NHTSA, the FTC, the Federal Communications Commission (FCC), the National Institute of Standards and Technology (NIST), and Intelligent Transportation Society of America (ITS America). Jurisdiction over cybersecurity and data privacy, as well as the enforcement of other consumer protection measures, should be left in the hands of the FTC. States and private industry would also play a role in this framework, although this would be rather limited, as it is deemed ideal to defer most aspects of the regulation to the federal consortium. As for the content, this new and AV-specific piece of legislation should take into account the findings of the U.S. Government Accountability Office's (GAO) In-Car Location-Based Service report.[114]

Most scholars also seem to agree on imposing the warrant requirement in the case of a search of the digital data generated by autonomous vehicles.[115]

***i58 IV. Intersection of Freedom, Privacy and Civil Liability**

As mentioned above, privacy and liability are considered to be crucial and the most controversial issues related to the use of autonomous vehicles. Almost all scholars tend to treat them separately, although some refer to both issues in the same paper.[116] By contrast, a paper by Jack Boeglin presents an integrated approach that takes into account freedom, privacy, and liability.[117] He views the three issues to constitute interlocking parts of the puzzle. Specifically, Boeglin argues that the person to be held liable in AV accidents should be the vehicle's user, and the extent of the user's liability should vary depending on the degree of the user's freedom and privacy that the user's AV protects.[118]

To understand this argument, one must understand the difference between discretionary and non-discretionary vehicles, as well as between communicative and uncommunicative vehicles. Discretionary vehicles are those that permit "the freedom and personal autonomy of their users to the greatest extent possible."[119] Specifically, the user can take over control of the vehicle whenever the user wants, maintain influence on the driving profile, and override the choice of route selected by the vehicle. Essentially, this seems to equal so-called automated vehicles or cars with an advanced form of driving assistance or simply vehicles with SAE automation levels 1-3. Boeglin uses the term *discretionary* to define this type of AV as vehicles which

 © 2024 Thomson Reuters. No claim to original U.S. Government Works.

help to limit the stress and danger of driving without completely eliminating the user's autonomy that is ceded to the car on a discretionary basis.[120]

Conversely, non-discretionary vehicles impede their users' selection of route, determination of driving style, or ability to switch the self-driving function off and take control of the vehicle. A nondiscretionary vehicle, for example, can obstruct the user's travel plans by deciding that the roads are too unsafe or the weather conditions too severe to drive in.[121]

The distinction between communicative and uncommunicative vehicles overlaps with Dorothy Glancy's division between interconnected (communicative) and self-contained (uncommunicative) AVs described earlier.

***i59** In the case of the discretionary-uncommunicative model of AV, where both the freedom and the privacy of the user are protected to the greatest degree possible, Boeglin compares the vehicle to a chauffeur.[122] This allows Boeglin to apply the doctrine of *respondeat superior* under which liability damages for accidents caused by a chauffeur falls upon the chauffeur's principal.[123] Hence, the AV user becomes liable for the damage caused by the faulty activity of this type of vehicle and will then channel the risks of such accidents to the private insurance market. Assigning liability to AVs' users would be "the price" for the maximum degree of control, discretion, and autonomy over the AV's operation.[124]

By contrast, Boeglin argues that the discretionary-communicative model of AV, which maintains the user's freedom but at the same time limits privacy by sharing information generated by the vehicle with the external network, makes it appealing to apply a product liability regime to some accidents caused by this model of AV. For example, a manufacturer's possibility to monitor the behavior of a discretionary-communicative AV could inform her/his duty to warn the user of bad weather, traffic jams, and similar circumstances. The manufacturer would follow principles of foreseeability and reasonableness. Otherwise, it remains the user who is liable for the accident caused by the AV as with the discretionary-uncommunicative model.[125]

For non-discretionary-uncommunicative vehicles, Boeglin proposes a proportional share liability regime for manufacturers, which he argues is feasible on the condition that each self-driving vehicle from the same manufacturer is sufficiently uniform. The liability here would be strict and split according to the per-mile accident costs assigned to each AV product.

Finally, the last model of AV--non-discretionary-communicative--where neither freedom nor privacy is protected, would trigger, according to Boeglin, the market-share liability of manufacturers that, after also considering the option of compensation by government, he perceives as the simplest and cheapest.

***i60 V. Proposals on How Civil Liability in the Context of AVs Should Evolve in the Future**

A. Applying Old Rules to the New Reality: Generalism

Much ink has been spent by the scholars on the issue whether the existing rules will be capable of dealing with the complexities posed by AVs liability. A considerable group of American scholars is of the opinion that this is possible.[126] In the words of Villasenor, "[p]roducts liability law offers a time-tested framework that has proven to be adaptive to technology-driven liability issues in ... other contexts," and it "will be equally capable of doing so when applied to autonomous vehicles."[127] According to Garza, "product liability law is capable of handling the advent of autonomous vehicles, just as it handled seatbelts, airbags and cruise control and the use of camaras and record keeping devices in the vehicles will lead to cheaper and speedier trials."[128]

Others argue that "[e]arly claims likely will resemble the contemporary lawsuits that allege negligent vehicle use." Those early trials will encompass failure-to-warn theory rather than the design defect, as the latter is difficult to prove because of lack of transparency provoked by the complex and sophisticated cars' programming.[129]

 © 2024 Thomson Reuters. No claim to original U.S. Government Works.

Under U.S. law, manufacturer can be held liable mainly by virtue of product liability. The regulation allows the victim to claim damages in three different cases: for manufacturing defects, design defects, and failures to warn. The court will acknowledge the manufacturing defect when a product does not comply with its specification or in case an unexplainable accident happens (the so-called malfunction doctrine). Design defects can be described as those in which "the foreseeable risks of harm could have been reduced or avoided by use of a reasonable alternative design." To determine the existence of this defect the courts employ two different tests: the consumer expectations test and the risk-utility test. A failure-to-warn claim will be successful when the manufacturer fails to comply with his duty to inform users how to safely use the product and/or will omit to warn the consumer about the hidden use-related risks.[130]

Those who criticize approaching liability for accidents caused by AVs on bases of traditional product liability point out that failure to warn will no longer apply in SAE level 3 vehicles because no affirmative ***i61** act to trigger the autonomous driver is necessary.[131] Furthermore, in most cases, the sophisticated and complex programming of autonomous vehicles will make it difficult to spot the exact cause of the accident and, consequently, the person liable (for example, whether it was a software or hardware malfunction).[132] In other instances, one or several entities could be held liable, raising the hardly solvable in this case question of apportionment of liability.[133] LeValley published a singular study in which he argues that AV manufacturers should be treated like "common carriers" who owe "the public the highest duty of care [and should be] liable for even the slightest negligence."[134]

Voices also exist that advocate for a shift from manufacturers' product liability to liability of AVs owners/users, which could be done either through application of strict liability[135] or through traditional negligence tort law coupled with a first-party insurance.[136] Vicarious liability under the doctrine of *respondiate superior* also might be used to impose liability upon the owner/user of an AV.[137] This solution is familiar to experts on tort liability for the behavior of robots.[138] Courts in the United States, however, are reluctant to endow robots with the personhood and treat them as employees creating vicarious liability.[139]

Mixed approaches also exist in this regard. According to Gurney, for instance, the liability caused by a vehicle in autonomous mode should stay normally with the manufacturer, but it could shift back to the driver if he is attentive. Who to make liable by virtue of this theory would depend on the nature of driver and his ability to prevent the accident. Thus, manufacturer would be responsible in the rest of the scenarios, namely in case of Disable, Diminished Capabilities and Distracted Driver.[140]

Other scholars plead for protection of manufacturers against costly lawsuits, consequently suggesting three ways of how to avoid product liability: assumption of risk, new legislation, or federal preemption ***i62** of state tort actions.[141] A Federal Motor Vehicle Safety Standard (FMVSS) adopted by NHTSA could serve this latter purpose.[142]

Assumption of risk "provides that a product user who knowingly accepts the risks of a potentially hazardous product assumes some or all of the responsibility for any harm that may befall them from use of the product."[143] In order for the defense to work, two elements must be present: knowledge (the plaintiff must know and understand the risks) and plaintiff must assume the risk free and voluntary.[144]

When it comes to legislative protection, it should be enacted either at federal or at state level, and it should protect the manufacturer against, or limit his liability.[145]

Finally, some scholars have suggested an analogy to the liability imposed on the owners of dogs causing injury to deal with accidents caused by AVs. Specifically, AVs resemble dogs in that they "think and act independently from their human owners, and these independent acts have similar consequences of inflicting personal injury or property damage."[146]

 © 2024 Thomson Reuters. No claim to original U.S. Government Works.

B. Reconciling the Old with the New: Between Exceptionalism and Generalism (a Mixed Approach)

One of the most interesting in-depth proposals in the field of liability for accidents caused by AVs comes from Mark Geistfeld. His approach can be described as mixed, as it combines the old and well-established tort doctrines in force in most of the states with two new federal safety regulations. The author's starting point is the conviction that many of those scholars who criticize the generalist approach to liability for accidents caused by AVs have not fully understood the following: "[t]he technology itself largely solves the most vexing tort problems."[147] This idea is so because with the massive deployment of AVs, the whole way of driving will change; in particular, driving based on the individualized behavior of human beings will become collective and systemized. Consequently, according to Geistfeld, it is very likely ***i63** that in the future we will witness the advent of the following driving pattern: a whole fleet of AVs will be controlled and administered by a single driver--the operating system. In this scenario, in which a fully functioning operating system orders each car of the fleet how to behave, it will be the system itself that causes the crash.[148] This would mean that the particular circumstances of the crash would be meaningless since the vehicle--a component of systemized driving--"should be evaluated through performance data for the fleet. Aggregate driving data can resolve otherwise difficult tort questions."[149]

The two requirements imposed by tort law and applied to damage caused by AVs, namely, the reasonably safe programming or design of the operating system, would be satisfied if aggregate data from premarket testing were able to demonstrate in a convincing manner that the fleet of AVs, when in use, is at least twice as safe as traditional (conventional) cars. Aggregate driving data also make it possible to deal with the third tort law requirement leading to avoidance of the manufacturer's liability--the obligation to adequately warn consumers of the risk inherent in AV use. This obligation would be satisfied, according to Geistfeld, when the insurance calculus referring to a risk-adjusted annual premium for insuring the vehicle--carried out based on aggregate driving data--is disclosed to the final consumer.[150]

Geistfeld proposes two federal regulations to remedy the lack of legal uniformity with the minimum displacement of state tort law. The idea is to find a common core among state tort laws that could be transformed into federal regulations governing the reasonable safety of automated driving technologies. Such regulations should, in Geistfeld's opinion, be entrusted to the NHTSA and take into account the associated tort obligations concerning adequate pre-market testing and disclosure of the inherent risk of crash. These regulations would be in line with the tort law followed in a majority of the states, with the result that "regulatory compliance would also satisfy the associated tort obligations in most states."[151] Under this proposal, federal law would preempt filing of claims based on divergent state tort law followed only by the minority of states, thereby achieving uniformity across the country without the federal government dictating the appropriate rule.[152]

All told, under this proposal state tort law helps to create a comprehensive regulatory framework that, in broad strokes, could be shaped in the following way:

> [A] regulatory-compliant autonomous vehicle would subject the manufacturer to tort liability only for crashes caused ***i64** by malfunctioning physical hardware (strict products liability); malfunctions of the operating system due to either programming error (same) or third-party hacking (strict liability again, with an important caveat); the manufacturer's failure to adopt a reasonably safe design or to provide adequate warnings for ensuring safe deployment of the vehicle (an ordinary products liability claim); or the manufacturer's failure to treat consumers and bystanders equally when designing the vehicle and its operating system (an ordinary negligence claim). A manufacturer would also be subject to tort liability for not complying with the federal regulations (negligence *per se*).[153]

 © 2024 Thomson Reuters. No claim to original U.S. Government Works.

C. Manufacturer Enterprise Responsibility: New, Uniform, and Vehicle-Focus Liability and Insurance at Federal Level

Another proposal to deal with liability from accidents involving AVs comes from Kenneth S. Abraham and Robert L. Rabin.[154] Their proposal addresses the likelihood that the rollout of SAE levels 4-5 AVs will be progressive, leading to an extended period of time in which they coexist on roads with conventional vehicles and partially automated CVs.

To address this, Abraham and Rabin advocate the implementation of the manufacturer enterprise responsibility (MER), similar to the system of workers' compensation. This would set aside the current liability and insurance regime only when the threshold of registered AVs at SAE autonomy levels 4 or 5 reach 25%.[155] Until then, the traditional tort law system, including potential product liability would remain in force for *all* types of accidents.

Once the 25% threshold is crossed, then the proposed no-fault MER system would govern accidents involving AVs, even if the accident also involved a CV and even if there was a negligent takeover of an AV by a human driver--leaving the conventional tort system only to govern accidents involving solely CVs. The proposal calls for federal enactment of MER pre-empting state legislation and common law rules.

1. Pure Accidents

When it comes to individuals and damage covered, the scope of application of MER would extend to the AV's occupants, as well as ***i65** to pedestrians, bicyclists, motorcyclists, and other third-party bystanders, for bodily injuries “arising out of the operation” of an AV. The latter is an essential limiting condition since an accident substantially caused by, for instance, a pedestrian or bicyclist will not qualify for the compensation under the scheme as it will not be considered to have “arisen out of the operation” of an AV. The causal nexus between AV's operation and injury would be not existent in this case.

MER would not cover *property damage*. Abraham and Rabin argue that the common practice of purchasing property insurance is the best coverage option in those cases, leading to no hardship or unfairness. Indeed, they advocate eliminating product liability of AV's manufacturers for property damage.

Bodily injuries would be compensated up to the specified benefit limits. This would not apply to cases in which the injuries were caused by AV owner's sole negligence, for instance by breaching the owner's obligation to update the software or to tweak it, or from negligent non-compliance with a duty of maintenance. This restrain would also apply to the “negligent driver” in those situations in which he was made responsible for some limited tasks he could perform (for example, if he is rarely permitted to drive manually when parking an SAE level 4 vehicle).[156]

Abraham and Rabin argue for manufacturer's liability rather than auto-owner financial responsibility for several reasons. The manufacturer has operational control over an AV, whereas the owner is only the occupant; the manufacturer is in the best position to decide what to invest in the operational system so as to avoid additional accidents and liability for accidents will incentivize the manufacturer to research the ways of improving the system and minimalize the rates of currently unavoidable accidents; finally, the manufacturer can internalize the cost of the accident into the AV's price.

MER would be an exclusive remedy, eliminating manufacturers' and operators' liability in tort for bodily injuries “arising out of the operation” of an AV, “even if injuries resulting from ... malfunctions had been actionable under current products liability doctrine because they resulted from manufacturing or design defects.”[157] This rule would be subject to three exceptions: (i) claimants would be permitted to seek punitive damages from the manufacturer or component-part maker; (ii) conventional tort actions when a third party caused an AV related accident as, for example, through a cyberattack on AV software; or (iii) when the owner of the vehicle has modified it in a manner that causes an accident.[158]

 © 2024 Thomson Reuters. No claim to original U.S. Government Works.

When it comes to benefits level, Abraham and Rabin argue that:

> ***i66** [U]nlimited medical expenses and up to $1 million in compensation for wage losses, indexed for inflation, should be available to each eligible MER claimant. Benefits would be paid periodically. In addition, up to $500,000 should be available, according to a schedule of noneconomic losses, for specified permanent or long-term injuries .... Finally, up to $1 million for wrongful death should be payable to the heir or heirs-at-law of a person killed in an HAV accident. This also should be paid pursuant to a schedule that is a function of the heir, or heirs', age and relationship to the decedent.[159]

"[I]n all but the largest cases involving out-of-pocket losses in excess of $1 million, collateral sources should be entitled to full reimbursement out of an MER recovery, rather than a proportionate reimbursement."[160]

2. Mixed Accidents

In the case of mixed accidents, there are two scenarios: a CV driver or passenger is injured in an accident with an AV; or an AV occupant is injured in an accident with a CV or third party. Abraham and Rabin conclude that in the first scenario efficiency reasons favor granting the CV plaintiffs the access to AV's owner MER. As with pure AV accidents, charging the manufacturer with the responsibility for accidents occurred in the first scenario would create safety incentives for the manufacturer. The same reasons informed Abraham and Rabin's preference as to the second scenario. Consequently, they argue for a complete abolition of the right of AV occupants to claim damages from CV drivers under negligence liability and recommend a full shift to an exclusively MER system as long as such solution would be advisable and politically feasible. Otherwise, they think that "CV defendants could still be liable in negligence to HAV occupants for sums not compensated by HAV plaintiffs' MER."[161]

3. Funding

Lack of statistically adequate data in the initial phase of MER would make it necessary to assess manufacturers' responsibility based on annual market share. Later, "assessment should be based on the frequency and severity of payouts for each manufacturer's AVs."[162]

***i67 4. Administration and Claim-Processing**

The continuing need for auto-liability insurance in such cases as negligent failure to maintain the vehicle, injuries caused by a manually operated AV, or property damage, converts the insurer in a perfect MER administrator. Therefore, claims would be filed with the insurance company that would receive a commission from the Fund for processing the complaint. All disputes arising out of such a claim (claim denied or partially paid) would be resolved by an administrative law judge in each state and could be appealed to a federal district court.[163]

D. Common Enterprise Liability

Problems related with identifying who is liable in accidents caused by AVs--the auto manufacturer or the maker of a component part--have induced another American scholar, David Vladeck, to think of the product liability regime as undesirable in this context, and led him to propose what he refers to as "common enterprise liability"--strict joint and several liability of both the auto maker and the part maker.[164]

 © 2024 Thomson Reuters. No claim to original U.S. Government Works.

E. Two-Tier Insurance Program Introduced at Federal Level

Among the scholars concerned with excessive liability on AV manufacturers, one can find exceptionalists such as Kyle Colona. She proposes a two-tier insurance program with a ceiling on damages, resembling the Price-Anderson Act that, in her opinion, should be enacted by the Congress at federal level. The first trier would have fully individual insurance coverage paid by each manufacturer, while for the second trier each manufacturer would contribute a certain amount to the secondary insurance pool. The second pool could be used only if the first was exhausted. In that way, the risk would be spread and shared between many manufacturers and insurance companies, avoiding bankruptcy of manufacturers for costly lawsuits. The author finds grounds for such a regulation in the high risk posed by the AVs, comparable to that of the nuclear energy.[165]

VI. Should Regulations for Self-Driving Cars Be National, Continental or International Through the Vienna Convention?

As mentioned earlier, there is also the question of whether the regulation of self-driving cars should be enacted at the federal ***i68** or state level, or both. According to the National Transportation Research Board, the complexity of the safety features present in the manufacturing process of AVs and the magnitude of the problem make it almost impossible for the NHTSA to comprehensively regulate the issue.[166]

Consequently, in a September 2016 policy statement presenting the NHTSA's strategy for regulating highly automated vehicle (HAV) technologies, the NHTSA touched upon the question of the division of competences between the agency and the states in the context of AVs.[167] Specifically, the statement recognizes that "[r]ules and laws allocating tort liability could have a significant effect on both consumer acceptance of HAVs and their rate of deployment."[168] In particular, "a patchwork of inconsistent laws and regulations among the 50 States and other U.S. jurisdiction ... could delay the widespread deployment of these potentially lifesaving technologies."[169] Because "a manufacturer should be able to focus on developing a single HAV fleet rather than 50 different versions to meet individual state requirements,"[170] the NHTSA "strongly encourages States to allow DOT alone to regulate the performance of HAV technology and vehicles."[171] The NHTSA, however, also "confirms that States retain their traditional responsibilities for vehicle licensing and registration, traffic laws and enforcement, and motor vehicle insurance and liability regimes."[172] Nevertheless, at the same time, the agency states that "[i]t may be desirable to create a commission to study liability and insurance issues and make recommendations to the States."[173]

This last suggestion has not been welcomed by some American scholars, who believe that such a process would be time-consuming and as a result lead not only to gaps in a law that is slowly catching up, but also to confusion on the part of the manufacturers, who would be devoid of essential guidance for the future. This would be a "cumbersome process" that could only be considered in a long run, because such a proposal would have to be approved by the legislative powers of each state.[174]

More broadly, many American scholars have criticized the division of competences between the NHTSA and the states. These scholars are ***i69** concerned about the lack of uniformity and the legal uncertainty that leaving the regulation of almost all aspects of AVs to state legislatures could bring, and thus advocate federal control.[175] Diverging state regulations also raise great concern within the automotive industry. As automobile insiders and a supporting scholar testified before a Senate Committee in 2016: "A patchwork of state laws governing the operation of self-driving cars threatens to stall their development."[176]

It is evident that the states will have to react somehow to adjust the existing rules to the new reality and to emerging problems and complexities the courts may face in litigations concerning AVs. This might lead to motley scenarios in which "[s]ome states would adopt MER; others would retain common law negligence liability; others would retain their hybrid negligence/auto no-fault approaches; still other states might adopt a revised version of common law tort, along lines now being proposed

by commentators."[177] This patchwork of regulation is incompatible with the national, or indeed international character of the AVs business.[178]

When it comes to international law, United States is a party to the 1949 Geneva Convention on Road Traffic, but it is not a party or signatory to the 1968 Vienna Convention on Road Traffic, and hence has no obligations under this treaty.[179] There appears in the United States to be little thought to or advocacy of looking to treaties for guidance on regulation of AVs.

Footnotes

d1 https://doi.org/10.1093/ajcl/avac015

a1 Assistant Professor of Private and Comparative Law at Universidad Loyola Andalucía, Seville, Spain. The author is enormously grateful to Professor Frank Gevurtz for his immense patience, outstanding editing, and excellent assistance. It has also been a privilege to be able to count on the suggestions and indications of Professor Michael D. Green--my great American friend. Finally, many thanks to Mark Willis for proofreading of this Report.

1 Rodrigo Marçal Gandia et al., *The Quintuple Helix Model and the Future of Mobility: The Case of Autonomous Vehicles*, *in* 25th International Colloquium of Gerpisa-R/Evolutions: New Technologies and Services in the Automotive Industry 1, 2 (2017).

2 Jeff McMahon, *Driverless Cars Could Drive Car Insurance Companies Out of Business*, Forbes (Feb. 19, 2016), www.forbes.com/sites/jeffmcmahon/2016/02/19/autonomous-vehicles-could-drive-car-insurance-companies-out-of-business/?sh=2f8fac2d2231. U.S. Chamber Inst. for Legal Reform, Torts of the Future: Autonomous Vehicles, Addressing the Liability and Regulatory Implications of Emerging Technologies 1 (2018).

3 Daniel J. Fagnant & Kara Kockelman, *Preparing a Nation for Autonomous Vehicles: Opportunities, Barriers and Policy Recommendations for Capitalizing on Self-Driven Vehicles*, 77 Transp. Res. Part A: Pol'y & Prac. 167, 169 (2015).

4 For the early predictions, see U.S. Chamber Inst. for Leg. Reform, Torts of the Future 2 (2017). *See also* Francesco Biondi, *Why We Still Don't Have Self-Driving Cars on the Roads in 2021*, Conversation (June 16, 2021), https://theconversation.com/why-we-still-dont-have-self-driving-cars-on-the-roads-in-2021-162646.

5 Kenneth S. Abraham & Robert L. Rabin, *Automated Vehicles and Manufacturer Responsibility for Accidents: A New Legal Regime for a New Era*, 105 Va. L. Rev. 127, 131-32 (2019).

6 U.S. Dep't of Transp., Nat'l Highway Traffic Safety Admin., DOT HS 812 115, *Traffic Safety Facts: Crash Stats, Critical Reasons for Crashes Investigated in the National Motor Vehicle Causation Survey* 1 (Feb. 2015), https://crashstats.nhtsa.dot.gov>Api>Publication.

7 Cesare Bartolini et al., *Critical Features of Autonomous Road Transport from The Perspective of Technological Regulation and Law*, 27 Transp. Res. Proc. 791 (2017).

8 Lisa Collingwood, *Privacy Implications and Liability Issues of Autonomous Vehicles*, 26 Info. & Com. Tech. L. 32 (2017).

9 Abraham & Rabin, *supra* note 5, at 140.

 © 2024 Thomson Reuters. No claim to original U.S. Government Works.

10 Gary E. Marchant & Rachel A. Lindor, *The Coming Collision Between Autonomous Vehicles and the Liability System*, 52 Santa Clara L. Rev. 1321, 1326-27 (2012).

11 Araz Taeihagh & Hazel Si Min Lim, *Governing Autonomous Vehicles: Emerging Responses for Safety, Liability, Privacy, Cybersecurity, and Industry Risks*, 39 Transp. Rev. 103, 113 (2018).

12 Tom Vanderbilt, *Let the Robot Drive: The Autonomous Car of the Future Is Here*, Wired (Feb. 23, 2012), https://www.wired.com/2012/01/ff-autonomouscars/.

13 William J. Kohler & Alex Colbert-Taylor, *Current Law and Potential Legal Issues Pertaining to Automated, Autonomous and Connected Vehicles*, 31 Santa Clara High Tech. L.J. 99, 120 (2015).

14 Dorothy J. Glancy, *Privacy in Autonomous Vehicles*, 52 Santa Clara L. Rev. 1171, 1173-74 (2012).

15 John Villasenor, *Products Liability and Driverless Cars: Issues and Guiding Principles for Legislation* 1, 2 (2014), www.brookings.edu/research/products-liability-and-driverless-cars-issues-and-guiding-principles-for-legislation; Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. Chi. Legal F. 207, 208-10 (1996)

16 Ryan Calo, *The Case for a Federal Robotics Commission* 1, 1-4 (Sept. 2014), www.brookings.edu/wp-content/uploads/2014/09/RoboticsCommissionR2_ Calo.pdf; Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 Harv. L. Rev. 501, 534-49 (1999).

17 Lindsey Barret, *Herbie Fully Downloaded: Data-Driven Vehicles and the Automobile Exception*, 106 Geo. L.J. 181, 183 (2017).

18 U.S. Dep't Transp. Nat'l Highway Traffic Safety Admin., *Preliminary Statement of Policy Concerning Automated Vehicles* 4-5 (2013), www.nhtsa.gov/staticfiles/rulemaking/pdf/Automated_Vehicles_Policy.pdf.

19 Abraham & Rabin, *supra* note 5, at 130.

20 Soc'y Auto. Eng'rs On-Road Automated Vehicle Standards Comm., Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles (2018).

21 Mohamed Alawadhi et al., *Review and Analysis of the Importance of Autonomous Vehicles Liability: A Systematic Literature Review*, 11 Int'l J. Sys. Assur. Eng. Mgmt. 1227 (2020).

22 *See* Nat'l Highway Traffic Safety Admin., DOT HS 810 698, *The New Car Assessment Program Suggested Approaches for Future Program Enhancements* (2007), https://www.federalregister.gov/documents/2007/01/25/E7-1130/the-new-car-assessment-program-suggested-approaches-for-enhancements.

23 Stephen P. Wood et al., *The Potential Regulatory Challenges of Increasingly Autonomous Motor Vehicles*, 52 Santa Clara L. Rev. 1423, 1426-27 (2012).

24 Abraham & Rabin, *supra* note 5, at 137.

 © 2024 Thomson Reuters. No claim to original U.S. Government Works.

25 David Shepardson, *U.S. Working to Set Rules for Self-Driving Cars*, Detroit News, Oct. 24, 2012, at D3.

26 *See, e.g.*, Jerry. L. Mashaw & David. L Harfst, The Struggle for Auto Safety 173-201 (1990). See, more recently, Robert L. Rabin, *Pathways to Auto Safety: Assessing the Role of the National Highway Transportation Safety Administration*, *in* Administrative Law from the Inside Out: Essays on Themes in the Work of Jerry L. Mashaw 297, 309-11 (Nicholas R. Parrillo ed., 2017); Abraham & Rabin, *supra* note 5, at 137.

27 Abraham & Rabin, *supra* note 5, at 137.

28 F. Patrick Hubbard, *"Sophisticated Robots": Balancing Liability, Regulation, and Innovation,* 66 Fla. L. Rev. 1803, 1845 (2014).

29 Press Release, Nat'l Highway Traffic Safety Admin., Preliminary Statement of Policy Concerning Autonomous Vehicles 10 (May 30, 2013), www.nhtsa.gov/staticfiles/rulemaking/pdf/Automated_Vehicles_Policy.pdf.

30 *Id.* at 10.

31 Bryant Walker Smith, *Automated Vehicles Are Probably Legal in the United States*, 1 Tex. A&M L. Rev. 411 (2014).

32 *See* Comm. Substitute House Bill (CS/HB) 1207 of 2012, H.B. 1207 Fla., 2012 Leg. (Fla. 2012), Fla. Stat. chs. 316, 319 (2013).

33 *See* Senate Bill (SB) 1298 of 2012, S.B. 1298 (Cal. 2012), Cal. Veh. Code div. 16.6, § 38750 (West 2013).

34 Fla. H.B. 1207 § 1.

35 *Id.* § 3, Fla. Stat. § 316.85 (2013). Derived from Cf Walker Smith, *supra* note 31, at 506.

36 Cal. S.B. 1298 § 1.

37 *Id.*

38 Cal. S.B. 1298 § 2.

39 *Id.*

40 Ben Husch & Anne Teigen, *Regulating Autonomous Vehicles*, 25 Legis Brief (2017), www.ncsl.org/research/transportation/regulating-autonomous-vehicles.aspx.

41 *Id.*

42 U.S. Dep't Transp. Nat'l Highway Traffic Safety Admin., Automated Driving Systems 2.0: A Vision for Safety 19 (2017), www.nhtsa.gov/sites/nhtsa.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf.

43 *Id.* at 19-25.

 © 2024 Thomson Reuters. No claim to original U.S. Government Works.

44 *Id.* at 19-20.

45 *Id.* at 21.

46 *Id.* at 22-24.

47 Steven E. Shladover & Christopher Nowakowski, *Regulatory Challenges for Road Vehicle Automation: Lessons from the California Experience*, 122 Transp. Rsch. Part A: Pol'y & Prac. 125, 126 (2019).

48 U.S. Dep't Transp. Nat'l Highway Traffic Safety Admin., Preparing for the Future of Transportation: Automated Vehicles 3.0 (2018) www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/320711/preparing-future-transportation-automated-vehicle-30.pdf.

49 Dasom Lee & David J. Hess, *Regulations for on Road Testing of Connected and Automated Vehicles: Assessing the Potential for Global Safety Harmonization*, 136 Transp. Rsch. Part A: Pol'y & Prac. 85, 90 (2019).

50 Recognized as well by Steven E. Shladover & Christopher Nowakowski, *Regulatory Challenges for Road Vehicle Automation: Lessons from the California Experience*, 122 Transp. Res. Part A: Pol'y & Practice 125, 126 (2019).

51 Nat'l Sci. & Tech. Council & U.S. Dep't Transp., Ensuring American Leadership in Automated Vehicle Technologies. Automated Vehicles 4.0 (2020) www.transportation.gov/sites/dot.gov/files/docs/policy-initiatives/automated-vehicles/360956/ensuringamericanleadershipav4.pdf.

52 *Id.* at 4.

53 Glancy, *supra* note 14, at 1178.

54 Steven E. Shladover, *Connected and Automated Vehicle Systems: Introduction and Overview,* 22 J. Intell. Transp. Sys. 190, 190-91 (2018).

55 Glancy, *supra* note 14, at 1179.

56 *Id.* at 1187.

57 *Id.* at 1188.

58 For more on these two sides of autonomy privacy in general, see Isaiah Berlin, Two Concepts of Liberty (1958); E. Goffman, Behavior in Public Places 3-12 (1963), E. Goffman, The Presentation of Self in Everyday Life (1959); Charles Fried, *Privacy*, 77 Yale L.J. 475, 475-82 (1968); Samuel D. Warren & Luis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 207 (1890).

59 Glancy, *supra* note 14, at 1193.

60 Warren & Brandeis, *supra* note 60, at 195.

 © 2024 Thomson Reuters. No claim to original U.S. Government Works.

61 Hill v. Nat'l Collegiate Athletic Ass'n, 7 Cal. 4th 1, 35 (1994).

62 Glancy, *supra* note 14, at 1193-94.

63 *See, e.g.*, Sidis v. F-R Pub. Corp., 113 F.2d 806 (2d Cir. 1940); Melvin v. Reid, 112 Cal. App. 285 (1931).

64 *See* Drivers' Privacy Protection Act, 18 U.S.C. §§ 2721-2725 (2012).

65 Glancy, *supra* note 14, at 1191-92.

66 U.S. Const. amends. I-X.

67 Glancy, *supra* note 14, at 1191-94.

68 United States v. Jones, 565 U.S. 400 (2012).

69 Glancy, *supra* note 14, at 1195.

70 *Id.* at 1195-1200.

71 *See* Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. Pa. L. Rev. 327, 376 (2015).

72 Glancy, *supra* note 14, at 1196.

73 U.S. Gov't Accountability Off., GAO-14-649T, *Consumers' Location Data: Companies Take Steps to Protect Privacy, but Practices Are Inconsistent, and Risk May Not Be Clear to Consumers* 5-6 (2014), www.gao.gov/assets/670/663787.pdf.

74 Barret, *supra* note 17, at 196.

75 United States v. Jones, 565 U.S. 400 (2012), at 415 (Sotomayor, J., concurring).

76 On the possibility of synchronizing a car with home-based assistant devices, see Natt Garun, *Screendrive: 2017 Ford Fusion Energi Is the First Car with Alexa*, Verge (May 1, 2017), www.theverge.com/2017/5/1/15438554/2017-ford-fusion-energi-alexasync3-review.

77 Glancy, *supra* note 14, at 1196 (2012).

78 Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich. L. Rev. 561, 563 (2009). *See also* Allison S. Bohm, Edward J. George, Bennett Cyphers & Shirley Lu, *Privacy and Liberty in an Always-On, Always-Listening World*, 19 Colum. Sci. & Tech. L. Rev. 1, 16-19 (2017).

79 Barret, *supra* note 17, at 194.

 © 2024 Thomson Reuters. No claim to original U.S. Government Works.

80 Katz v. United States, 389 U.S. 347 (1967). *See also* Margaret E. Twomey, *Voluntary Disclosure of Information as a Proposed Standard for the Fourth Amendment's Third-Party Doctrine*, 21 Mich. Telecomm. & Tech. L. Rev. 401, 411 (2015).

81 United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010).

82 United States v. Karo, 468 U.S. 705 (1984).

83 United States v. Knotts, 460 U.S. 276 (1983).

84 *See* Erin Smith Dennis, *A Mosaic Shield:* Maynard*, the Fourth Amendment and Privacy Rights in the Digital Age*, 33 Cardozo L. Rev. 737, 754-759 (2011).

85 *Maynard*, 615 F.3d at 544, 562.

86 Barret, *supra* note 17, at 196. *See also* Richard M. Thompson II. The Fourth Amendment Third-Party Doctrine, report, (2014), https://digital.library.unt.edu/ark:/67531/metadc807192. Numerous critics of the "Third-Party Doctrine" point out that the online environment allows collecting vast amounts of personal online data at very low cost. *See, e.g.*, Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 Minn. L. Rev. 1, 19 (2008); Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & Pol'y 211, 242-44 (2006), Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 Pepp. L. Rev. 975, 976 (2007).

87 United States v. Jones, 132 S. Ct. 945, 956 (2012).

88 *Id.* at 957 (Sotomayor, J., concurring).

89 *See* Saby Ghoshray, *Privacy Distortion Rationale for Reinterpreting the Third-Party Doctrine of the Fourth Amendment*, 13 Fla. Coastal L. Rev. 33, 63 n.10 (2011).

90 Twomey, *supra* note 80, at 413.

91 Stephen Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and its State Analogs to Protect Third-Party Information from Unreasonable Search*, 55 Cath. U. L. Rev. 373, 376 (2006).

92 United States v. Miller, 425 U.S. 435 (1976).

93 Smith v. Maryland, 422 U.S. 735 (1979).

94 Twomey, *supra* note 90, at 416.

95 For more details, see *id.* at 415-16.

96 Matthew Tokson, *Automation and the Fourth Amendment*, 96 Iowa L. Rev. 581 (2011).

97 *Id.*

98 Glancy, *supra* note 14, at 1207.

99 United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).

100 *Id.* (citing United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

101 Glancy, *supra* note 14, at 1208.

102 *Id.* at 1209.

103 *Jones*, 132 S. Ct. at 945.

104 Glancy, *supra* note 14, at 1209-11.

105 *Id.* at 1212-14.

106 *Id.* at 1226. *See also* Kaori Ishii, *Comparative Legal Study on Privacy and Personal Data Protection for Robots Equipped with Artificial Intelligence: Looking at Functional and Technological Aspects*, 34 Artificial Intell. & Soc'y 509 (2019).

107 Helen F. Nissenbaum, Privacy in Context 1-10 (2010).

108 Fed. Trade Comm'n, Report: Protecting Consumer Privacy in an Era of Rapid Change (2012), www.ftc.gov/os/2012/03/120326privacyreport.pdf; F.T.C. Docket No. C-4336 (Oct. 13, 2011).

109 White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in The Global Digital Economy (Feb. 2012), https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf.

110 Transp. Rsch. Board, *Using Vehicle Integration Data, Part 2: Cross-Cutting VII Data Issues* (87th Annual Meeting, Sess. 682, Jan. 16, 2008).

111 Ishii, *supra* note 106, at 521.

112 *Id.* at 527-28.

113 *Id.* at 528.

114 Chasel Lee, *Grabbing the Wheel Early: Moving Forward on Cybersecurity and Privacy Protections for Driverless Cars*, 69 Fed. Commc'n. L.J. 25, 43-52 (2017).

115 Gregory C. Brown, *Nowhere to Run, Nowhere to Hide: Applying the Fourth Amendment to Connected Cars in the Internet-of-Things Era*, 32 J. Civ. Rts. & Econ. Dev. 311, 338-39 (2019); Barret, *supra* note 17, at 205.

 © 2024 Thomson Reuters. No claim to original U.S. Government Works.

116 Dorothy J. Glancy, *Autonomous and Automated and Connected Cars: Oh My! First Generation Autonomous Cars in the Legal Ecosystem*, 16 Minn. J. L. Sci. & Tech. 619 (2015).

117 Jack Boeglin, *The Costs of Self-Driving Cars: Reconciling Freedom and Privacy with Tort Liability in Autonomous Vehicle Regulation*, 17 Yale J.L. & Tech. 171 (2015).

118 *Id.* at 175-76.

119 *Id.* at 179.

120 *Id.* at 179.

121 *Id.* at 179.

122 Such a comparison is not new in the literature. *See, e.g.*, Megan Rose Dickey, *Get Ready for Self-Driving Cars that Chauffeur Us Around*, Bus. Insider (Jan. 16, 2013), www.businessinsider.com/get-ready-for-self-driving-cars-that-chauffeur-us-around-2013-1; Martin LaMonica, *Google Self-Driving Car Chauffeurs Legally Blind Man*, CNET (Mar. 29, 2012), https://law.stanford.edu/press/inside-googles-quest-to-popularize-self-driving-cars/. Google calls the software that empower its flagship AV "Google Chaufeur." Adam Fisher, *Inside Google's Quest to Popularize Self-Driving Cars*, Popular Sci. (Sept. 18, 2013), www.popsci.com/cars/article/2013-09/google-self-driving-car.

123 *See, e.g.*, Perez v. Von Groningen & Sons, Inc., 41 Cal. 3d 962, 967 (1986); King v. Stuart Motor Co., 52 F. Supp. 727, 728 (N.D. Ga. 1943); *Agency--Master and Servant--Automobiles--Liability of the Owner of a Family Car*, 36 Harv. L. Rev. 102, 103 (1922).

124 Boeglin, *supra* note 117, at 188-89.

125 *Id.* at 190-92.

126 *See, e.g.*, Villasenor, *supra* note 15; Andrew P. Garza, *"Look Ma, No Hands!": Wrinkles and Wrecks in the Age of Autonomous Vehicles*, 46 New Eng. L. Rev. 581 (2012).

127 Villasenor, *supra* note 15, at 15

128 Garza, *supra* note 126, at 595.

129 Graham, *Of Frightened Horses and Autonomous Vehicles: Tort Law and Its Assimilation of Inventions*, 51 Santa Clara L. Rev. 1241, 1270 (2012). *See also* Abraham & Rabin, *supra* note 5, at 143 ("judicial and jury assessment of the acceptable limits of engineering capability for alleged design defects, through reliance on expert assessment of risk-utility analysis, will come to be needlessly contentious and costly").

130 Jeffrey Gurney, *Sue My Car Not Me: Products Liability and Accidents Involving Autonomous Cars*, 2013 J.L. Tech. & Pol'y 247, 258.

131 Abraham & Rabin, supra note 5, at 143.

 © 2024 Thomson Reuters. No claim to original U.S. Government Works.

132 Ryan Calo, *Open Robotics*, 70 Md. L. Rev. 571, 597 (2011); Marchant & Lindor, *supra* note 10, at 1328-29.

133 Marchant & Lindor, *supra* note 10, at 1328.

134 Dylan LeValley, *Autonomous Vehicle Liability: Application of Common-Carrier Liability*, 36 Seattle U. L. Rev. Supra 5, 6 (2013).

135 Sophia H. Duffy & Jamie Patrick Hopkins, *Sit, Stay, Drive: The Future of Autonomous Car Liability*, 16 SMU Sci. & Tech. L. Rev. 453, 453 (2013).

136 See Adam F. Scales, *Not So Fast: A Brief Plea for Muddling Through the Problems of Autonomous Vehicle Liability*, 13 J. Tort L. 189, 194 (2020).

137 Boeglin, *supra* note 117, at 186.

138 *See, e.g.*, Samir Chopra & Laurence White, *Artificial Agents and the Contracting Problem: A Solution via an Agency Analysis*, 2009 U. Ill. J.L. Tech. & Pol'y 363, 392; Stephen T. Middlebrook & John Muller, *Thoughts on Bots: The Emerging Law of Electronic Agents*, 56 Bus. Law. 341, 354 (2000)

139 Boeglin, *supra* note 117, at 186.

140 Gurney, *supra* note 130.

141 Marchant & Lindor, *supra* note 10, at 1336.

142 *Id.* at 1338.

143 *Id.*

144 Gurney, *supra* note 130, at 269. For the problems related with this approach *see* Jessica S. Brodsky, *Autonomous Vehicles Regulation: How an Uncertain Legal Landscape May Hit the Breaks on Self-Driving Cars*, 31 Berkley Tech. L.J. 851, 865-66 (2016); Marchant & Lindor, *supra* note 10, at 1336-37.

145 Marchant & Lindor, *supra* note 10, at 1337. *See also* Wendell Wallach, *From Robots to Techno Sapiens: Ethics, Law and Public Policy in the Development of Robotics and Neurotechnologies*, 3 Law, Innovation & Tech. 185, 194, 196 (2015) (discussing incentives of autonomous product manufacturers to seek legislation providing liability protection); Calo, *supra* note 132, at 601-09 (proposing limited immunity from liability for manufacturers of autonomous systems).

146 Duffy & Hopkins, *supra* note 135, at 113.

147 Mark A. Geistfeld, *A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation*, 105 Calif. L. Rev. 1611, 1612 (2017).

148 *Id.* at 1621-22.

 © 2024 Thomson Reuters. No claim to original U.S. Government Works.

149 *Id.* at 1611.

150 *Id.* at 1622-23, 1651-60.

151 *Id.* at 1612.

152 *Id.* at 1623-24, 1677, 1684-91.

153 *Id.* at 1613.

154 Abraham & Rabin, *supra* note 5. *See contra* Adam F. Scales, *Not So Fast: A Brief Plea for Muddling Through the Problems of Autonomous Vehicle Liability*, 13 J. Tort L. 189 (2020); Ryan Calo, *Commuting to Mars: A Response to Professors Abraham and Rabin*, 105 Va. L. Rev. 84 (2019).

155 Abraham & Rabin, *supra* note 5, at 132.

156 *Id.* at 150-51.

157 *Id.* at 156.

158 *Id.* at 159-60.

159 *Id.* at 161.

160 *Id.* at 164.

161 *Id.* at 164-69.

162 *Id.* at 169.

163 *Id.* at 169-71.

164 David C. Vladeck, *Machines Without Principals: Liability Rules and Artificial Intelligence*, 89 Wash. L. Rev. 117, 129 n.39, 146-48 (2014).

165 Kyle Colonna, *Autonomous Cars and Tort Liability*, 4 J.L. Tech. & Internet 81, 122-25 (2012)

166 Nat'L Rsch. Council Nat'l Acads., Transp. Research Bd., Special Report 308: The Safety Promise and Challenge of Automotive Electronics: Insight from Unintended Acceleration 182 (2012), http://onlinepubs.trb.org/onlinepubs/sr/sr308.pdf.

167 U.S. Dep't Transp., Federal Automated Vehicles Policy: Accelerating The Next Revolution in Roadway Safety 10 (2016), www.transportation.gov/AV/federal-automated-vehicles-policy-september-2016.

 © 2024 Thomson Reuters. No claim to original U.S. Government Works.

168 *Id.* at 46.

169 *Id.* at 37.

170 *Id.* at 7.

171 *Id.* at 37.

172 *Id.* at 7.

173 *Id.* at 46.

174 Geistfeld, *supra* note 147, at 1677.

175 In field of civil liability, see Abraham & Rabin, *supra* note 5; Colonna, *supra* note 165. All aspects of AV regulation should be federal according to Lee, *supra* note 114, at 43-52.

176 *Hands Off: The Future of Self-Driving Cars: Hearing Before the S. Comm. On Commerce, Sci., & Transp.*, 114th Cong. (2016).

177 Abraham & Rabin, *supra* note 5, at 148 (when pleading for MER as a single-national rule adopted by the U.S. Congress, preempting al inconsistent state legislation and common law rules).

178 *Id.* at 148-49

179 Geneva Convention on Road Traffic, Sept. 19, 1949, 125 U.N.T.S. 3; Vienna Convention on Road Traffic, Nov. 8, 1968, 1042 U.N.T.S. 17.

70 AMJCL i39

End of Document

© 2024 Thomson Reuters. No claim to original U.S. Government Works.