



白皮书

2021年5月

自动驾驶汽车：美国法律及监管动态

自动驾驶汽车技术及其在不久将来的广泛应用有着实现众多社会效益的潜力，包括增进道路安全，提高经济生产率以及优化燃油经济性等。同时，伴随着各类创新的涌现和行业的发展，自动驾驶汽车行业参与者也将面临一系列法律问题。

本篇众达白皮书对我所之前发表的自动驾驶汽车相关法律和监管问题方面的出版物做出了更新。本篇白皮书侧重于自动驾驶乘用车方面，并列述了下列领域的发展动态：(i) 自动化技术；(ii) 相关州及联邦法规；(iii) 产品责任；以及 (iv) 网络安全和数据隐私方面的责任问题。

Table of Contents

目录

背景.....	1
自动化程度等级.....	2
自动化演进时间线.....	3
其他技术挑战.....	4
机器学习.....	4
无线通信.....	5
摘要模型.....	5
相关法规.....	6
概要.....	6
联邦法规.....	7
州法规.....	9
法律问题.....	9
责任注意事项.....	10
收集和储存电子信息.....	10
责任范式.....	11
联邦优先权.....	11
严格产品责任.....	12
违反保证.....	15
网络安全和数据隐私相关的具体责任问题.....	16
网络安全.....	16
数据隐私.....	17
自助--不确定因素不应妨碍行动.....	18
结论.....	19
联系律师.....	20
尾注.....	20

无人驾驶汽车已经出现在我们的生活中。随着这种技术的广泛应用，无人驾驶汽车将会帮助提高效率和促进全球多个行业领域以及交通运输基础设施的创新。与此同时，高水平的汽车自动化也给制造商、供应商、销售商、消费者以及公众带来了独特的安全、网络安全和数据隐私问题。

设备和软件方面的众多技术选择催生出了高度竞争的市场，市场内的众多竞争者都在争相证明自身的价值。到目前为止，美国联邦政府一直在尽力避免从中选取最为成功的技术，或是针对整个行业实施一套综合监管制度。虽然多个州都已颁布涉及自动驾驶汽车的法律，但这些州基本都是采取宽松的方法来鼓励开发和测试。因此，截至目前所通过的法律还远未达到一致统一的程度，这也为那些投资于高度自动化汽车（HAV）研究和技术的公司提供了极大的灵活性。

本篇白皮书对我所 2017 年 11 月份的上一篇同主题白皮书发表之后的美国相关技术、监管和责任问题的发展动态予以更新。本篇白皮书会探讨了 HAV 制造商、供应商和销售商在美国面临的相应产品责任法规，并提出了可能出现的相关法律问题。目前，在缺乏综合全面的州或联邦立法的情况下，通常会适用传统的侵权责任原则，但同时法学教授和评论人士也一直在努力预测未来的责任规则。其中许多人预计，普通法项下的驾驶人过失责任将逐渐不再成为关注重点，因为驾驶人在 HAV 操作过程中发挥的作用将越来越小，甚至最终不再发挥任何作用。HAV 的独立运行将会令产品设计越来越多地成为未来事故发生原因的关注重点，同时，产品设计问题也会涉及常见的产品责任概念。

在解决萌芽起步阶段的 HAV 领域所独有的问题时，产品责任原则很可能会被一如既往地适用。因此，联邦法优先适用会对侵权责任的认定具有重要影响，但由于联邦政府尚未明确立法，所以具体的影响程度和影响方式还有待观察。此外，自动驾驶汽车的制造商及其供应商还会面临网络安全和数据隐私领域的特别问题，并且已有部分意见呼吁联邦政府就这些问题进行特别立法。由于联邦层面较少干预，制造商和供应商可以通过合同风险分配、赔偿协议、担保限制、消费者教育和培训、行业标准以及保险等方式自行解决相关问题。本篇白皮书旨在提供一些实用性建议，以供 HAV 制造商、供应商及销售商参考如何降低产品责任索赔风险。

背景

目前，道路上行驶的许多汽车都带有自动化驾驶功能，完全自动化的汽车也已在开发和测试中。其他类型的自动化交通运输，例如无人机、火车、船舶、班车和卡车，将会给众多行业带来便利。现在，已有部分零售商开始测试利用自动化无人机将在线购物商品送货上门¹，一家公司已经开始使用机器人配送披萨²，而且还有至少一家运输公司正在使用半自动化卡车在整个美国西南部地区进行货物运输³，智能卡车车队和无人驾驶出租车和公交似乎不久也将问世。这种新兴技术甚至会影响那些不直接使用自动驾驶汽车的行业。自动交通的发展进步最终可减少道路交通事故；共享车辆的发展能够降低对传统停车的需求；而汽车功能的优化也会减少汽油、润滑油、化工品以及可降解材料的消耗⁴。但与此同时，这项技术的广泛用途和应用在许多行业中提出了太多的问题，无法在一份白皮书中一一涉及到。在讨论过程中，本篇白皮书将侧重于自动驾驶车辆及其相关法规，以及自动化基础设施所引发的法律问题。

自动化程度等级

国际汽车工程师协会（SAE）按从零到五的顺序对汽车自动化予以定义⁵。

SAE自动化等级



无自动化

人类驾驶员全程完成一切动态驾驶任务，即使在警示或干预系统提供辅助的情况下，仍需人类驾驶员操作。



辅助驾驶

在特定驾驶模式下，由辅助驾驶系统利用驾驶环境相关信息执行方向控制或加减速操作，同时其他所有动态驾驶任务均由人类驾驶员实施。



部分自动化

在特定驾驶模式下，由一项或多项辅助驾驶系统利用驾驶环境相关信息执行方向控制和加减速操作，同时其他所有动态驾驶任务均由人类驾驶员实施。



有条件自动化

在特定驾驶模式下，由自动化驾驶系统完成所有动态驾驶任务，同时人类驾驶员根据系统干预请求做出适当回应。



高度自动化

在特定驾驶模式下，由自动化驾驶系统完成所有动态驾驶任务，即使人类驾驶员未对干预请求做出适当回应，亦由系统进行。



完全自动化

在人类驾驶员掌控的所有道路和环境的条件下，全程由自动驾驶系统完成一切动态驾驶任务。

术语相关备注

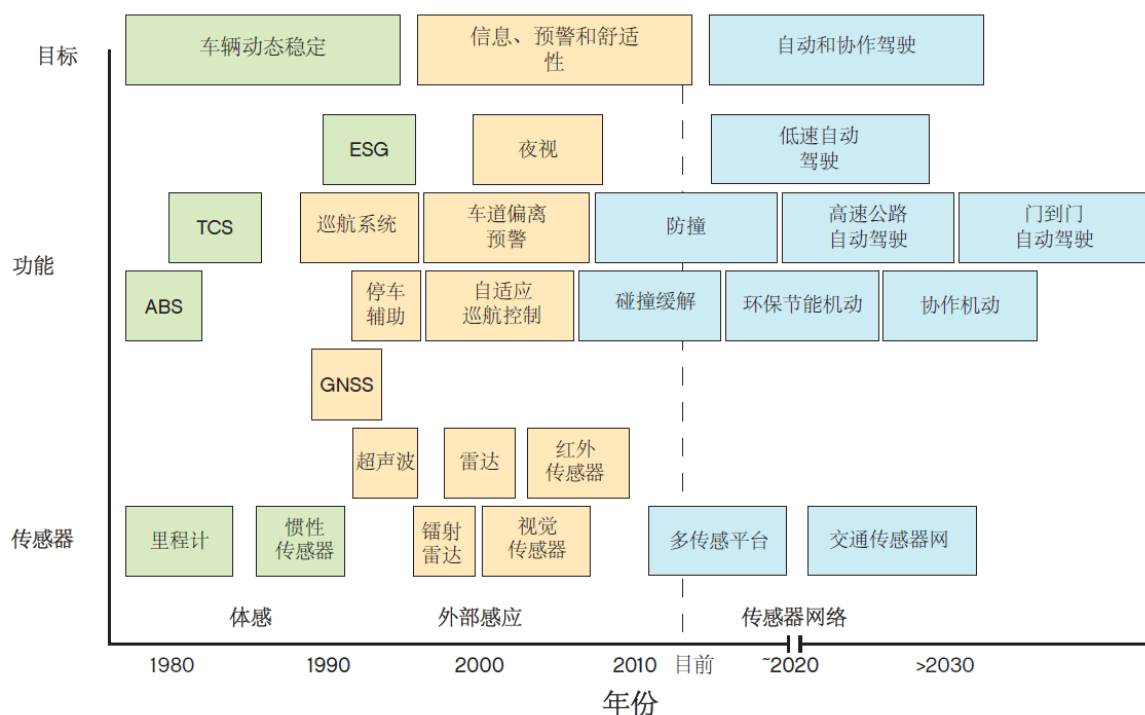
明确且前后一致的术语定义和使用对于展开和推进自动化相关讨论具有重要意义。到目前为之，行业、政府和评论人士用来描述各类路面交通自动化形式的术语可谓多种多样（自动驾驶、自主、无人驾驶、高度自动化等）。虽然无法说哪个术语就是正确的或错误的，但在本文件中，一概使用“自动化”和“自动驾驶汽车”概括描述该主题，同时根据具体情况采用“自动化驾驶系统”或“ADS”等更为精确的语言。

国际汽车工程师协会，J3016_201806：道路机动车驾驶自动化系统相关术语的分类和定义（沃伦代尔：国际汽车工程师协会，2018年6月15日），https://www.sae.org/standards/content/j3016_201806/。

SAE 0 级到 SAE 2 级的车辆需要人类驾驶员驾驶。即使部分驾驶功能是自动化的，人类驾驶员仍需要监控和监督该等功能⁶。该自动化等级范围内的可视化警示和驾驶辅助技术等一系列功能特征已经在消费型车辆中使用多年。HAV 属于 SAE 3 级到 SAE 5 级区间范围，由自动化系统控制车辆移动和决策过程⁷。虽然低自动化等级的 HAV 也会装载自动停车系统等功能特征，但较高等级的 HAV 则可以在部分甚至全部驾驶参数下完全实现自动驾驶，不需要任何人车互动。

自动化演进时间线

现在美国路面上行驶的车辆基本在 SAE 0 级到 SAE 3 级区间范围内。如下页中的图表所示，这些汽车上装载的常见功能包括防抱死制动、牵引控制、加速仪、巡航系统、后视和盲点摄像头、停车辅助、车道偏离预警系统、自适应巡航控制、防撞、节能机动以及高速路自动驾驶等。



完全自动化的 SAE 4 级和 SAE 5 级汽车目前尚在开发和测试中，而且美国全国范围内的真实路面测试也在不断增加⁸。部分实验性使用的案例包括阿利桑纳州菲尼克斯市的无人驾驶出租车服务；佛罗里达州中部连通居民区和商业区的自动驾驶乘用车⁹；以及弗吉尼亚州里斯顿市的低速行驶摆渡车¹⁰。此外，消费型自动驾驶汽车也已经出现在路面上。例如，特斯拉就曾展示过一项名为“智能召唤”的自动化无人驾驶 SAE 4 级功能，该功能可以让停放在停车场内的汽车在用户抵达附近后自行回到用户身边¹¹。此外，亚马逊旗下的 Zoox 公司目前正在拉斯维加斯、旧金山和福斯特城的真实路面上测试一款“马车式”车辆，该款车可以用作机器人驾驶出租车或用于协助进行包裹投递服务¹²。

虽然实现上述进展来自于数百万小时的车辆模拟、测试和优化，但全面部署的预计时间安排仍存在很大争议。作为其中一个极端，苹果公司的联合创始人史蒂夫·沃兹尼亚克（Steve Wozniak）认为，完全自动化的汽车在未来几十年内都不能实现部署¹³。而作为另外一个极端，特斯拉创始人埃隆·马斯克（Elon Musk）则主张，实现全面自动化所需要的硬件组件已经在特斯拉最新款的商用汽车中投入使用；自动驾驶车队目前只待用于控制和优化驾驶指令的“软件更新”¹⁴。但无论前景如何，既往经验一再表明，工程可行性不会是唯一的考虑因素。公众关切、政府决策以及责任风险控制能力都将是重要的因素。

其他技术挑战

从硬件角度而言，有两种类型的传感器可以为完全自动驾驶汽车提供主要的支撑：(i) 被称为光探测和测距（LiDAR）的激光雷达，或 (ii) 光学摄像头。尽管这是两种不同的技术，但却都被设计用于绘制车辆周围环境的综合图像¹⁵。HAV 还装载了一整套其他类型的传感技术，用于实现已存在于商用汽车的多项功能特征：

- 无线电定向与测距（RADAR），通过收发无线电波以测量距离，用于盲点检测和来车警告系统；
- 超声波测距，用于测量声波挠度，从而在辅助停车过程中发现障碍物；
- 全球定位系统（GPS），对汽车位置与轨道卫星的距离进行三角定位，从而提供航行和事实交通情况方面的更新；
- 惯性测量单元，不借助GPS而使用陀螺仪和加速仪探测汽车位置和速度的变化¹⁶；
- 红外摄像头，可以检测到表明有热体存在的波长，帮助识别道路上的人或动物¹⁷；以及
- 非视域成像，可以发现道路下一个拐弯处的物体¹⁸。

整体而言，这些硬件组件据称已达到成熟标准，可以支持规模化部署。

机器学习

软件的进步仍是实现汽车自动化所面临的唯一最大阻碍。HAV 软件会分析所有的传感数据，并以一种功能上类似于人类驾驶员的方式做出汽车控制决策，只不过速度会更快。由于驾驶的复杂性，硬编码规则不能控制所有软件输出。相反，HAV 软件必须具备“机器学习”功能，对系统参数进行迭代式理论处理，形成车辆控制决策模型，并根据收集的数据、真实环境的测试结果以及经验教训不断更新升级。如同人类根据所积累的生活经验改进决策一样，HAV 软件根据收集到的传感数据以及过去成功的汽车控制决策做出不断改进。

通过机器学习算法进行软件优化是一个极其耗时的过程，因为完成驾驶任务需要海量的数据收集、合成以及快速的决策。以拼车服务为例，乍看这项业务似乎很简单，但其底层任务却极为复杂 – 即使对于有经验的人类驾驶员而言，确保出租车能够接到正确的乘客已属不易，而找出能够确保一辆自动驾驶汽车找到并核实正确乘客的系列规则更是一项不同寻常的挑战¹⁹。因此，相比在繁忙的停车场中操控汽车这种相对复杂的场景，在诸如高速行驶等变量相对较少的环境下，机器学习会更加有效地对驾驶任务做出理论化处理²⁰。真实环境中的驾驶需要用到大量的直觉、技巧和常识，所有这一切都需要通过经验学习获得。而这正是问题的症结之处。真实环境中的测试案例对于积累实现复杂驾驶任务自动化所需要的数据以及提高安全性具有重要意义，但在完成数据积累之前，开展真实环境测试本身又是一项艰巨挑战²¹。

HAV 开发者们想出了一系列创造性方式推进技术进步。他们采取的策略包括在数字平台上积累测试数据²²，找出可通过传感数据做出的非传统推论²³，以及升级道路基础设施，借助可机器读取的标识、车道指示以及警示等为自动化决策提供便利²⁴。上述技术手段最终都可以帮助缩减自动驾驶汽车的上市时间，但没有一项能够完全替代耗时冗长的真实环境测试，所以，各种不可避免的延期和不确定性依旧会存在。

无线通信

在完全自动化的基础设施中，无线通信也具有至关重要的作用，原因在于其可以减少 HAV 软件所需要的推理逻辑。开发者们正在研究“车联万物”（V2X）通信，即在车辆与附近其他车辆、周围的道路基础设施以及交通控制系统之间收发关于其他车辆的速度和位置、路况状态、道路障碍物和交通警示的信息。目前已有两项尝试实现 V2X 目标的技术：专用短距离通信（DSRC）和蜂窝车联网（C-V2X）²⁵。DSRC 通过收发 5.9 GHz 频段（该频段是美国联邦通信委员会（FCC）专为车辆通信和安全划拨的频段）的无线电波实现通信²⁶。C-V2X 则利用蜂窝技术，通过基站和轨道卫星分程传递信号的方式实现通信²⁷。

在这两项技术中，DSRC 率先投入使用，并在业界获得了众多汽车制造商的支持²⁸。而 C-V2X 则在很大程度上需要依靠 5G 技术的发展以及 5G 技术所实现的带宽、速度和蜂窝连接性的提升²⁹。两种通信技术的争论推迟了全面自动化的部署时间。但近期由 FCC 发起的相关进展似乎表明 C-V2X 已经从中胜出（可参见下文中的“联邦通信委员会”章节），同时行业开发者的设计选型 – 至少对于尚未决定采取何种无线通信技术的开发者而言 – 也将有可能因此而在近期最终确定。

摘要模型

在减少责任风险方面，制造商、供应商和销售商需要考虑多项因素（但下表有可能过于简化）。

摘要表
行业实务
车辆功能
• 探测/感知不断变化的车辆驾驶环境（例如，天气、路况、其他车辆、交通信号和标识、行人等）； - 上述条件状况的解读/理解； - 对该等条件状况做出响应的反应时间； - 为了在上述条件状况下安全运行所选择的反应；以及 • 事故无法避免时的撞力承受度。
车辆设计和运行
• 设备和硬件，包括车辆本身的组件和通信组件； • 设备位置，诸如传感器和摄像头等； • 软件； • 机器学习、更新和重建所需要的数据记录和保存；以及 • 撞力承受度，诸如分区设计和约束系统。
驾驶员及消费者信息、教育和培训
• 操作手册及其他书面信息； • 车载警示和预警； • 额外的提高型教育和培训；以及 • 广告。
潜在责任索赔

- 设计方面，包括研究、测试以及适用法律法规或行业标准合规；
- 制造方面，包括质量控制；
- 警示和说明方面，包括售中和售后过程；
- 虚假广告或不实陈述索赔；以及
- 违反明示或暗示保证。

上表展示了适当情况下制造商、供应商或销售商在预测和降低与 HAV 开发、制造和销售相关的潜在责任风险时可能需要单独或整体评估分析的各类问题。本篇白皮书将在其他章节中介绍用于评估潜在责任风险的法律框架，即当前适用的相关联邦及州法律法规，此外还将分析 HAV 风险场景所适用的现有责任概念和先例。

相关法规

概要

美国联邦或州层面均未出台具体的 AV 监管规定。乘用车的安全通常由联邦和州联合监管。国家公路交通安全管理局（“NHTSA”）根据国会的指示通过《机动车辆安全标准》（“FMVSS”）³⁰对机动车辆的测试与安全予以规制。NHTSA 执行合规，管理安全相关缺陷的召回事宜，并与环境保护署（“EPA”）共同对燃油的经济性和排放予以监管。同样，联邦汽车运输安全管理局（“FMCSA”）也制定了载重汽车安全标准，即《联邦汽车运输安全条例》（“FMCSR”）。国家运输安全委员会（“NTSB”）有权对车辆事故开展调查，并就安全改进问题提供建议，但是 NTSB 工作重点是民航、火车和货车领域。各州一直以来也通过向驾驶员发放执照、注册机动车辆、开展安全检查、颁布并强制执行交通法、提供安全基础设施和管制机动车辆保险及机动车交通事故责任等方式对公路安全进行管理。

车辆与汽车零部件制造商在设计和测试其产品时需要考虑整个法律框架。但是，多数法规在起草时并未考虑无人驾驶车辆及其独特的优势、挑战和风险。例如，FMVSS 有关转向系统的测试协定假设有人类驾驶员坐在方向盘后面，但是对于高端 HAVs³¹而言，这些规定均已不再必要。SAE 4 和 SAE 5 车辆本身的设计并不旨在符合且也不需要符合诸多 FMVSS 标准。联邦政府正在谨慎地评估和制定 AV 相关的具体监管法律结构，既要避免压制新技术的发展，又要允许进一步拓展公路使用和测试的经验。³²由于目前缺乏针对 AV 的具体监管框架，必须向 NHTSA 申请临时豁免联邦标准；NHTSA 截止目前已批准了数项豁免。³³

截至目前，联邦或州政府并未以任何全面系统的方式对 HAV 设计参数或技术做出规定。这种自由度允许在车辆设计选择和测试方面，包括安全设备的选择，继续存在竞争。与 5.9 千兆宽带以及 5G 基础设施等确切的规定（参见下文）不同，联邦层面并不存在可以为 HAV 制造商或供应商提供明确指导的有关公路测试协议、最低安全标准或车辆设计的综合性要求。研发者和投资人均可自由选择支持其偏好的技术，自由寻求在国家公路测试和证明该等技术的许可。州和当地政府也对无人驾驶车辆安全和测试持基本宽容态度，但很多州已经开始制定具体的法规，从而拼凑形成了各州之间均不同的且几乎每个月都会变更的监管方案。

联邦法规

与欧洲和日本不同，美国国会并未颁布专门规制 HAV 安全、网络安全或数据隐私的特定法律。³⁴2017 年，美国众议院和参议院曾考虑几个类似的法案，³⁵尽管众议院通过了其法律文本，但《自驾法案》最终并未成为有效法律。³⁶2020 年 9 月，众议院议员兼众议院能源与商业委员会通信与技术分会的成员 Bob Latta 曾推出《自驾法案》的修订版。³⁷国会最近一次有关规制 HAV 安全、网络安全或数据隐私的立法的尝试最终因未能获得立法所需的支持而失败。经修订的《法案》中要求更新 FMVSS，旨在采取措施提供有关自动驾驶车辆的特定安全标准。

如果《自驾法案》生效，则汽车制造商须完成并提交“安全评估认证”，且交通部长将在法律生效两年内确定上述认证的监管要求。³⁸根据法律要求，部长确定的规则将界定“表明该实体的车辆安全系数合规、各项性能正常且包含安全锁定装置等所要求的相关测试结果、数据以及其他内容。”³⁹尽管该举措最终只是立法权限的授予而非通过相关标准，但该法案一旦通过，将会启动更全面的联邦监管法律架构。

另外，在最终立法前的两年过渡期内，法案授权行业内的企业提交“安全评估函”以供 MHTSA 审阅。⁴⁰除了当前已实施的 FMVSS 豁免程序外，该程序将为 HAV 测试和部署建立标准的渠道。与现有的联邦机动车辆安全法类似，经修订的《自驾法案》将通过禁止任何州或地方政府“制定有关高度自动化车辆的设计、生产或性能、自动化驾驶系统或自动化驾驶系统的各部件的任何法律或法规【除非该法律或法规与本章项下规定的标准相同】”形成统一的联邦 HAV 安全标准法律。⁴¹这一法律框架将为制造商在全国范围内测试并部署其 HAV 提供潜在的保护。

修订的《自驾法案》还增加了网络安全及数据隐私方面的要求。最新的法案要求车辆制造商制定“书面网络安全政策”以“识别、评估并减少合理可预见的网络攻击或未经授权入侵漏洞，包括虚假伪造的信息以及恶意车辆控制命令。”⁴²同时还要求公司“采取预防性和纠正措施减少该等漏洞。”同样，车辆制造商须制定有关信息“收集、使用、共享和储存”和“有关车辆所有人或占有者的数据简约化、去身份识别和存档”的“书面隐私计划”。⁴³该修订《法案》有关网络安全和数据隐私的规定与特定行业选择相匹配。

总之，法案旨在促进 HAV 创新，同时开始解决有关安全、网络安全和数据隐私的主要问题。法案将容许更规范的 HAV 测试与部署—首先通过个性化的 NHTSA 安全评估，之后通过最终的机构法规进行测试。法案也将阻止大量不相关的、不一致的州法律法规的发展。⁴⁴但是，目前尚不确定本届国会或近期是否能通过最新版的《自驾法案》。在此之前，由于不存在国会指南，仍由联邦机构提供自愿指导。

交通部。与国会一样，交通部及其分支机构最近才开始采取具体措施全面监管 HAV。交通部的总体方针是支持各州的行为，鼓励汽车行业本身进行一定程度的自我监管。自 2016 年以来交通部共发布了 5 份指导性文件。⁴⁵交通部始终将“安全为重”作为首要原则，并同时促进创新，推动法规现代化。尽管之前的指南强调州和地方政府可发挥的作用，最新发布的指南“自动驾驶汽车 4.0”和“自动驾驶汽车：综合计划”号召采取“一致的联邦措施。”⁴⁶

2020 年 6 月，交通部前任部长 Elaine L. Chao 宣布交通部正在“设立一个联邦、州和当地政府的正式平台，以协调和共享信息。”⁴⁷《自动驾驶汽车透明度与参与安全测试（“AV 测试”）计划的发布是交通部、九家行业内的私有公司⁴⁸和八个州⁴⁹之间共同

努力的结果。目前，52 家公司、州政府和协会⁵⁰正在通过公开分享自动化测试活动及安全信息参与“提高自动化驾驶系统发展的透明性与安全性。”⁵¹

NHTSA 也已采取初步行动，就如何监管 HAV 测试与安全向行业和相关参与方征求意见。2018 年，NHTSA 就其应该考虑的因素征求意见，⁵² 2019 年，NHTSA 和 FMCSA 均就现有的机动车辆法规适用于 HAV 测试和部署时遇到的困难征求意见。⁵³ 2020 年，NHTSA 强调需要“现代化”FMVSS 以适应具有较高自动化程度的车辆。⁵⁴ 2020 年 3 月发布了一项拟议立法通知，力图“移除对配备自动化驾驶系统的汽车（“配备 ADS 的汽车”）以及预期与这些汽车相匹配的非常规内部设计（包括无驾驶控制系统的设计）的不必要的障碍。”⁵⁵ 具体包括对 FMVSS 进行修改，变更有关司机安全气囊、转向控制系统和汽车座位等的定义（这些变更反过来影响安全要求），重点关注人类驾驶员不会发生的情况，例如汽车驾驶舱内无乘客或儿童座位的情况等。⁵⁶

该等拟议变更不再预先假设所有的汽车均有人类驾驶员，从而消除了 HAV 测试和部署监管方面的障碍。如果这些标准最终通过成为法律，将优先于很多之前州法律确定的安全标准。⁵⁷ NHTSA 的拟议规则的公开征求意见期已结束，但最终结果目前尚不确定。⁵⁸

2020 年 12 月，NHTSA 发布了一项拟议立法通知，就一项“专门针对 ADS 安全的政府安全法律框架”的制定公开征求意见。⁵⁹ 最终的框架不仅仅包括正式法规；还会“涉及 NHTSA 的一系列举措，包括有关强调最佳行业惯例的、向消费者提供信息以及描述不同研究方法和总结研究结果的指导性文件，以及较正式的法规，从要求汇报和披露信息的规定到专门针对 ADS 的 FMVSS 标准的通过等。”⁶⁰ NHTSA 就其应如何实施该等法律框架征求意见。⁶¹ 拟议规则的征求意见期于 2021 年 4 月 1 日结束。⁶²

联邦通信委员会。 监管无线电波使用的联邦通信委员会（“FCC”）至今仍在很大程度上影响与 HAV 相关的监管决定：无线汽车通信的最佳方法。20 多年前，FCC 为汽车安全目的将 5.9 千兆赫兹频段中的 75 兆赫兹分配给 DSRC。有些汽车制造商希望能将该频段的上端部分用于 HAV 通信并就此向 FCC 申请豁免。⁶³ 但是，由于非汽车行业也想使用该频段，该问题尚存在争议。

2019 年，FCC 曾提议力图兼顾两项要求的一项规则，对于“上述频段的下端 45 兆赫兹”实行“无许可运营”，而为汽车通信“保留上端 30 兆赫兹的频段”。⁶⁴ 在为汽车通信保留的频段内，FCC 进一步提议将其中的三分之二分配给 C-V2X 方案，并就剩余的频段是否应为 DSRC 继续保留征求意见。⁶⁵ 考虑到在过去的 20 年里已为 DSRC 保留了几近整个频段，FCC 的提议标志着思维方面的巨大转变。除了行业内的争论外，在联邦政府内部对 FCC 的提议也存在异议。交通部以及众议院交通和基础设施委员会的多个成员均对该计划持反对意见。^{66 67}

2020 年 10 月底，FCC 前任主席 Ajit Pai 发表声明称相较于 DSRC 更赞成 C-V2X，且 FCC 发布了一项最终规则命令草案，提议将 5.9 千兆赫兹频段重新运用 Wi-Fi 和 C-VX 汽车通信的专用频段之间。⁶⁸ 做出此决定是因为在 COVID-19 大流行性流感初期（在 FCC 授予特别临时授权以允许互联网提供商使用 5.9 GHz 频段后），频谱使用取得了显著成功。⁶⁹ 2020 年 11 月 18 日，FCC 批准了一份报告，并下令将 45-30 频段在未经许可的 Wi-Fi 用途和 C-V2X 技术之间分摊，以提高汽车安全性。⁷⁰ FCC 预期该命令将为 C-V2X 拓展其“提供汽车与障碍（包括其他汽车、骑自行车的人、行人以及公路工人）之间的直接通信，以及从路边发射器接收安全信息”的扩展能力的途径。⁷¹ 该 FCC 命令的目的是为 HAV 部署提供便利。

州法规

只要联邦政府尚未承担主导性角色，州和地方政府将有更大的自由度进行监管。⁷²

目前，37 个州及华盛顿特区已颁布部分 HAV 相关法规。⁷³若干州长也下发了相关行政令。这些规定中有一些是最低限度的，仅授权队列行驶或建立咨询委员会来进行研究。⁷⁴至少 29 个州已经发布了有关 HAV 测试的政策或法规，⁷⁵其中大多数是通过行政令方式发布的。⁷⁶

各州所采取的方法存在很大差异。比如，加利福尼亚州的监管范围较为宽泛。⁷⁷该州有一项监管法规是专门针对 HAV 测试和部署的。⁷⁸截止 2021 年 2 月 25 日，该州共发布了 56 项有驾驶员的 HAV 测试许可、6 项无人驾驶测试许可，并授权一家实体部署无人驾驶汽车。⁷⁹

在加州，任何测试许可均要求制造商证明可就潜在的责任判决提供实质性担保。⁸⁰另外，驾驶员在进行特定的 HAV 测试之前必须完成培训项目，如果某汽车制造商希望进行无人驾驶测试，公司必须遵守其他特定的程序要求。⁸¹

亚利桑那州的情况类似，进行无人驾驶测试必须证明汽车符合 FMVSS 标准、已实施碰撞减缓措施；测试须遵守所有交通法规，且 HAV 须满足注册和保险要求。⁸²但是，在 2018 年阿利桑纳州发生重大车祸后，NTSB 建议亚利桑那州和其他州扩展其法律规定，要求提供具体测试和安全计划，包括降低操作员注意力不集中的风险。⁸³作为回应，宾夕法尼亚（该州允许队列行驶⁸⁴）等若干州通过了额外法规，限制无人驾驶测试并要求在任何公路 HAV 测试之前实施额外的申请和审批程序。⁸⁵

大多数州均竭力为 HAV 发展创造一个有利的环境。但是，法规的不一致性导致制造商合规很困难，且导致冗余的认证程序。而且，各州尚未以任何整合方式解决与网络安全和数据隐私相关的行业问题。⁸⁶尽管城市⁸⁷和州具有在地方层面塑造法律监管环境的权限，但似乎有些州和地方政府一直在等待联邦介入，以协助解决在设备测试协定、网络安全和数据隐私方面的主要问题。

法律问题

鉴于迄今有限的强制性法规⁸⁸，HAV 制造商和供应商拥有很大的自由度来选择如何管理其潜在责任。

除非实现更全面的联邦或州监管框架，通常是传统的州侵权和保证法规来管辖因 HAV 事故引起的民事责任。法院将需要考虑是否修改这些规则来适应不同自动化水平的 HAV。现有的赔偿责任计划和规则，以及通过调整规则创造新的先例，将有助于厘清制造商，供应商和销售商对受伤人员的潜在责任，以及赔偿责任在制造商，供应商和销售商之间的潜在分摊。⁸⁹

根据过失理论，原告必须证明被告违反了应当对原告承担的义务，造成了伤害，以及和赔偿金额。涉及到 HAV 则产生了许多问题，包括谁能够并且应当承担责任。传统上，驾驶员应在没有机械故障的情况下对交通事故负责。如果没有驾驶员控制车辆（取决于自动化程度），不考虑车辆的维护或驾驶员在情况需要时恢复控制的能力，

那么在许多事故中驾驶员的失误可能不再是问题。的确，HAV 的长期目标是消除驾驶员（据报道他们造成了 94% 的事故）的控制。⁹⁰

根据各个州不同的法律规定，过失原则仍可适用于评价 HAV 制造商和供应商的过错，包括制造缺陷，不充分测试或质量控制，不合理的设计选择，不准确的说明或不充分的警告。⁹¹ 以下问题仍有待解决：（i）如果警告不充分，自动化系统的制造缺陷，或对车主的训练或教育不适当或不充分，是否将由销售商承担过失责任；（ii）此类责任如何或可能不会扩展至所有者或其他车辆中的乘客或旁观者；（iii）乘客和行人承担自负风险的程度。在考虑过失责任时，事故的情况和原因将仍然相关。同样，车辆的自动化程度会影响到责任分析，在达到完全自动化之前，责任分析的复杂性最高。

早期评论员预测，规制 HAV 制造商、供应商和销售商的责任将是严格的产品责任，并以制造、设计或警告的缺陷为前提。现在的趋势正是如此。目前来看，原告可以期待在可能的情况下就欺诈和虚假陈述提出普通法和法定的索赔主张。基于合同的索赔，例如违反担保的索赔，也可能适用。但是，如果联邦政府颁布 HAV 法规，则其可能会取代某些或所有州的普通法索赔规定。

在没有联邦干预和指导的情况下，制造商还可能面临因网络安全和数据隐私造成的其他责任。因此，制造商、供应商和销售商可通过赔偿协议、通过合同安排分配风险、免责声明（在州法律允许的范围内）、帮助制定行业标准和保存来自车辆及其系统的电子数据和保险等方式来保护自己。⁹²

责任注意事项

收集和储存电子信息

作为出发点，自动化技术及其大量数据收集将从根本上影响传统诉讼。例如，在所谓的机械故障的情况下，对车辆数据的所有权以及获取途径将成为利益相关者需要解决的关键问题。电子证据开示可以帮助识别证明因果关系和责任相关事实所需的相关数据。联邦民事诉讼规则第 37 条和类似的州法得到修订，以反映电子数据的可用性并为未保留的数据提供治愈措施。⁹³

因此，制造商将需要评估从车辆和事故环境中收集的数据类型。法规或行业标准可能规定了最低的限度。⁹⁴ 然后，制造商可以评估其需求，以进行责任或产品改进、调整并了解如何使用和保存自动驾驶汽车收集的数据类型，以评估事故的情况和原因。⁹⁵ 数据收集还将有助于根据各种条件改进 HAV 的设计，并提出是否需要改进基础结构的建议。

对于 HAV 碰撞事故，数据可以显示车辆的速度和位置以及事故发生时哪些自动功能正在运行（即制动器，油门，转向和检测）。数据对于决定车辆传感器所探测到什么以及车辆如何解释所感知的环境至关重要。记录的数据还可以显示驾驶员是否接管了对车辆功能的控制，或者车辆是否警告驾驶员接管控制权。如果是这样，那么如果车辆在碰撞过程中以其自主模式运行，则可能需要考虑驾驶员的作为或者不作为是否恰当，而不仅仅是制造商的行为和车辆的设计。

在 2018 年亚利桑那州发生的致命事故中（请参见上文的“州法规”），电子存储的信息显示自动制动系统已关闭，而驾驶员未能干预。此外，来自驾驶员在线媒体帐户的

数据显示，她在事故发生前正在播放电视节目，因此可能未给予适当的关注。⁹⁶第三方数据源可以帮助了解事故原因，而这些来源反过来可能会引发数据隐私问题。

记录和存储的数据类型取决于制造商、供应商、监管机构和保险公司事故前的决定。电子数据和证据的保存将在完全自动化的基础架构中进一步影响侵权诉讼。一方获得或保留此类电子数据的能力可能会改变有关驾驶员过失，第三方过错或产品缺陷的诉讼。

责任范式

联邦优先权

关于赔偿责任的一个首要问题是联邦立法的优先权以及个人是否可以基于 HAV 事故造成的伤害提起州法的诉讼。现存法律已经为某些 HAV 相关的州侵权诉讼的联邦优先权奠定了基础。⁹⁷在 *Geier v. American Honda Motor Co., Inc.*案中⁹⁸，美国最高法院根据联邦机动车安全法（FMVSA）和 1984 年 FMVSS 的规定，对明示和默示的优先权进行了审议。联邦法规要求汽车必须配备被动约束装置，但没有指定约束装置的类型，制造商可以选择包括哪种约束装置。该法规反映了政府有意制定的政策，允许制造商使用不同类型的被动约束，而监管机构和行业则积累了在各种事故情况下每种类型的有效性所需的数据和经验。原告在系安全带时发生碰撞而受伤，他辩称制造商应该为汽车配备安全气囊。最高法院裁定，此类诉讼违背联邦政府的制造商选择政策，虽然没明示被优先，但是默示被优先。

相反，在随后的 *Williamson v. Mazda Motor of America, Inc.*案⁹⁹中，新版本的 FMVSS 允许制造商为后排座椅配备仅膝部或膝部和肩部安全带。原告声称，根据州法律，制造商有责任安装膝部和肩部安全带。法院区分了 *Geier* 案，未发现本案有任何明示或默示的优先权，因为没有明确的联邦政策支持制造商进行设计选择。

根据现行法规和 *Geier / Williamson* 范式，如果联邦监管机构故意允许自动汽车制造商在行业发展的过程中选择不同的安全增强技术，那么州普通法的诉因将不再适用。。但是在 *Williamson* 案之后，需要做的不仅仅是避免采取行动，就像联邦政府到目前为止所做的那样，监管者必须采取慎重的制造商选择政策。

国会也可以选择为 HAV 建立单独的优先权范式。Latta 代表的法案将禁止任何州或地方政府“实施任何有关高度自动化车辆、自动驾驶系统或自动驾驶系统组件的设计、构造或性能的法律或法规，除非该法律或法规与本章规定的标准相同。”¹⁰⁰其中包含一个保留条款。¹⁰¹这两种措施虽然是针对自动汽车的，但它们都记录 FMVSA 中的相似语言，因此不可能对有关联邦优先权的 *Geier / Williamson* 范式进行实质性的更改。

但是还有其他优先权模式。例如，根据联邦铁路安全法，联邦法规“包含”了安全法规领域，只有在声称违反联邦标准或被告自己制定的自我安全标准的情况下，州侵权诉讼才能继续进行。¹⁰²这种方法可以减少国家侵权法的影响。国会也可以选择针对设计选择或性能标准的优先权，但保留基于不充分警告、普通法或法定欺诈或虚假陈述的侵权法索赔。¹⁰³或者，如果联邦政府采用欧洲方法¹⁰⁴，并采用了基本的安全标准¹⁰⁵，例如要求车辆配备功能自检和数据记录器，则可以说不会有优先权的影响，因为这些功能仅有助于确定后续责任。它们本身并不能阻止各州制定制造商必须遵守的安全标

准。与通常一样，联邦优先权的范围不仅取决于适用的法定语言，还取决于随后的司法解释。

在联邦政府采用 HAV 的特定规则之前，一个特定的争议领域可能是临时许可的优先效力，例如那些早前提议的联邦立法所考虑的临时批准，这将需要 NHTSA 在立法颁布和发布全面安全法规之间的两年时间内批准对 HAV 制造商的安全评估。NHTSA 目前被授权提供的豁免可能会造成类似的问题。现有法律为此类情况下的优先权提供了一些支持，因为：

（i）联邦法规授权了批准，并且（ii）机构对联邦法规的豁免可以具有与法规本身相同的优先作用。例如，在 *Rollins v. Bombardier Recreational Products, Inc.* 一案¹⁰⁶中，美国海岸警卫队豁免了个人船只关于 1971 年联邦船只安全法规定的通风系统要求。由于海岸警卫队的豁免是根据国会明确的授权授予的，因此法院裁定，与该豁免相抵触的原告的国家产品责任索赔被优先。¹⁰⁷

联邦优先权的未来仍然是一个悬而未决的问题。只要 NHTSA 和 FMCSA 继续执行遵从的标准，或者仅仅要求行业成员开发和记录他们自己的安全协议和测试程序，他们的规则的优先性的效果将是值得怀疑的，并且这些行业成员将更有可能面临州法律责任的风险。但是，由于联邦机构表示希望 HAV 行业进行某种程度的自我监管，因此制造商和供应商可以帮助制定行业认可的标准，这些标准可能会成为联邦优先权的标准。行业安全倡议可能（至少部分地）决定联邦机构最终决定监管的方式。

严格产品责任

除非联邦政府有进一步举措，否则州法律将起到重要作用，这首先体现在严格产品责任方面。普通法的严格产品责任认可对制造商、供应商和销售商的索赔，索赔因设计、制造、警告或说明中的产品缺陷而造成的人身损害或财产损失。

对于 HAV，一些评论员预计过错责任的作用会逐渐减弱，也许会朝着无过错责任制迈进。他们认为，全自动 HAV 旨在防止大多数事故发生。因此，一旦发生任何事故，很可能是制造商、零件供应商或销售商承担责任的某些车辆缺陷引起的。¹⁰⁸虽然制造商、供应商或销售商之间的责任分配可能仍然存在争议，但根据该理论推定了他们对受害人的责任，因此，对 HAV 制造商，以及适当时对零部件供应商和 HAV 销售商施加的无过错责任体系兼顾了公平和高效。但是，我们离全自动 HAV 时日尚远，“无过失”理论的基本前提尚有争议。同时，传统的严格产品责任框架可能会决定 HAV 事故责任的确定。¹⁰⁹

在产品责任框架下，HAV 制造商、零部件供应商和销售商可能因将缺陷的产品卖给消费者被要求承担责任，即使他们付出了合理的注意。¹¹⁰他们对售后车辆状况的重大变化（例如，售后设备或车主缺乏维护）不承担任何责任。这个严格的责任框架非常熟悉，并且每天都应用于汽车事故。那么，HAV 可能会提出哪些具有挑战性的新问题呢？

设计缺陷。法院通常使用两个测试之一来确定设计缺陷是否存在。历史上第一个但现在很少运用的测试是消费者期望测试。¹¹¹该测试考虑 HAV 或零部件的功能是否如普通公众中的合理消费者所期待的一样运转。因为法院已经认识到消费者对复杂技术应该如何运作几乎没有概念，所以这项测试已不受欢迎。在 HAV 的背景下，如果适用该测试，“合理的消费者”可能期望车辆能够避免所有或几乎所有事故。

例如，在最近的一起悲剧案例中，一位父亲在驾驶中无意撞倒了他的孩子，起诉某汽车后视摄像头系统存在设计缺陷。该诉讼称，摄像机的后视能见度无法识别直接位于车辆后面的人员，尤其是儿童和残疾人。¹¹²由于识别移动车辆背后的人员是该技术的主要功能之一，也是消费者希望从车辆的后视摄像头获得的功能，因此，制造商应承担责任。

消费者会对 HAV 技术有何期望？制造商、供应商和卖方可能期望面对各种各样的消费者态度。¹¹³一些消费者和陪审员的直觉是害怕会夺走他们的控制权以及他们不理解的技术。人类倾向于给不能感知的事物（如核辐射）和无法控制的事物（如飞行）分配更多的风险。他们不太可能理解该技术的局限性，尤其是在 HAV 达到完全自动化级别 5 之前。然而，在另一方面，将是消费者和陪审员拥护该技术，但期望过多，认为该技术将万无一失，能够防止所有事故和伤害。

与往常一样，制造商和供应商将需要根据适用法律的规定，评估 HAV 车辆和技术的合理可预见的使用和滥用，包括合理可预见的故障模式。他们将能很好地全面记录所使用的可靠设计、测试和安全程序、以及支持其设计选择的原因。而且，重要的是，他们将需要能够证明设备继续按预期学习和改进。

如竞争技术所示，制造商和供应商将面临许多技术选择，包括传感器的类型及其位置、隔间设计时乘客安全性与舒适性和便利性之间的权衡、使用约束装置的类型，通讯系统、驾驶员接管车辆控制权（如果有）以及软件设计。这些技术选择超出了大多数消费者的视线。然而，对于汽车和零部件制造商而言，至关重要的是提供准确描述 HAV 所包含技术的手册或其他书面信息，解释其功能和局限性，讨论风险，并强调车主和驾驶员的持续责任。竞争对手很可能会继续宣传他们的汽车的设计选择优于其他公司，但同时也会提供不同的价格点和消费者的喜好来反映出不同的选择和安全性。由于消费者正在使用新技术，因此制造商、供应商和销售商可以在告知和管理公众期望和对其技术的认知方面发挥重要作用。HAV 制造商、供应商和销售商可以通过减少承诺但增加披露来减轻其责任风险。

但是，正如《侵权行为重述（三）：产品责任》，大多数州法院已从消费者期望测试转移到风险效用测试。¹¹⁴在风险效用测试中，法院平衡产品的效用与造成伤害的危险。最新的《重述》还要求证明合理的替代设计。尽管公众对风险的认识仍然很重要，但该测试将更多的重点放在了更客观的因素上，例如在制造和销售时替代技术的可行性、风险、成本和收益。

涉及自动车辆技术的案例具有启发性。在 *Honda of Am. Mfg., Inc. v. Norman* 案中，一名驾驶员意外将其车辆驶入水体中，而自动系上的安全带肩带据称由于设计缺陷未能脱开而死亡。¹¹⁵适用风险效用测试，法院要求原告通过专家证词表明合理的设计选择“在技术和经济上都是可行的。”¹¹⁶当原告不这样做时，法院裁定自动安全带并非不合理的危险或设计有缺陷。¹¹⁷在该案中，有利于制造商抗辩的事实是，自动约束系统“是汽车制造时使用的最昂贵的安全带系统”，而且“没有证据表明在汽车制造出来的时候，Honda 的被动约束系统存在合理安全的替代设计。”¹¹⁸

在此测试下，责任取决于对制造商或供应商所作设计选择的合理性进行客观、科学的分析（与可用的替代技术的比较分析）。虽然特定事故的情况及其可预见性为诉讼提供了依据，但责任分析更广泛地考虑了在所有预期事故场景中，针对合理可预见风险而进行设计选择的优势。在驾驶员事故和 HAV 事故之间进行有利的安全比较也可能有助于校准和抵消新技术带来的固有伤害风险，尤其是在设计替代方案仍然有限的情况

下。各种设计替代方案的测试和模拟、严格的故障模式工程分析以及精心记录的决策制定对于抗辩仍然很重要。

制造缺陷。制造缺陷产生于生产线，即一个不合理的危险被引入了一个原本安全的设计。制造过程中的错误会引起缺陷，从而导致产品或零件不符合其设计规格。例如，在 *Fitzpatrick v. Currie* 一案中，一个自动安全气囊系统展开并碎裂，释放出导致原告外伤和化学灼伤的气体。¹¹⁹ 目击者“在安全气囊的下方观察到一个垂直缝隙或撕裂”，原告将其归因于制造缺陷。¹²⁰ 法院最终裁定支持汽车制造商，因为初步证据显示安全气囊在离开其控制时没有制造缺陷，并且因为原告未能提供任何证据表明安全气囊的缺陷导致他受伤。¹²¹

与往常一样，对零件和材料以及最终产品进行高水平的质量控制对于降低制造错误的风险很重要。而且由于该技术高度复杂和综合，制造商和供应商可能希望考虑包括自我诊断的系统设计，以报告功能损失或组件故障。检测软件错误将比硬件和设备复杂得多，并且可能需要系统收集并响应现场报告和客户投诉，才能检测到这些错误。

制造缺陷责任的一种新兴的潜在法律风险包括在 HAV 离开制造商工厂后产生的制造缺陷。因为期望 HAV 不断从经验中学习并接收软件更新，所以它们的软件和决策必然会与出厂时有所不同。但是，同样的责任分析将适用：是否存在导致软件决策错误的的设计缺陷？

未能警告。不充分的警告或说明也可能导致严格责任的缺陷索赔。HAV 技术的复杂性的提高及其局限性，尤其是在达到 5 级自动化之前，可能会导致更多由于驾驶员和消费者的无知或困惑而引起的事故索赔。¹²² 特别是当该技术是新技术并且不为公众所熟悉，并且该自动化水平要求驾驶员进行控制或监控时，车辆和零部件制造商可以考虑提供可靠的驾驶员和消费者信息、教育、培训以及车载警告和警报。

涉及 HAV 相关技术的案例对于该责任将如何影响零件制造商具有一定的指导意义。在一个案件中，一名妇女在穿越农村公路时因疏忽的驾驶员而受伤，法院认定 GPS 公司尽到了警示义务，部分原因是该公司没有法律义务保护她免受来自于第三方过失的伤害。¹²³ 这与另一种情况形成对比，乘客在公共汽车与桥梁相撞后受伤，而 GPS 未能识别出该桥梁高度受限。¹²⁴ 乘客起诉 TomTom 和 Garmin 等，认为他们违反了对适销性的默示保证、过失以及严格责任。¹²⁵ 这些案例表明，原告可能会指控零部件制造商有义务向最终用户提供准确的警告和安全的使用说明。

相同的原理不仅适用于组件，还适用于车辆的自动驾驶功能。在涉及飞机自动驾驶技术的案件中，法院发现飞机制造商没有义务对飞行员进行自动驾驶系统使用方面的培训，但它有义务提供足够的说明以确保安全使用。¹²⁶ 因此，法院将考虑车辆制造商是否在车上或在用户手册和车主手册中提供了足够的安全说明。此外，根据 HAV 设计中技术水平的高低，除手册外，制造商或销售商还可以考虑进行消费者培训。¹²⁷ 一个典型的 HAV 操作人员可以有区别于飞机飞行员的、可以被合理预期到的专业知识和培训。制造商对 HAV 操作人员理解和遵守业主手册指示的能力的合理期望，很可能成为在未警告责任的情况下确定制造商责任的一个重要因素。¹²⁸

很少有诉讼涉及全自动化或接近全自动化的汽车，而这些案件要么悬而未决，要么在没有判决¹²⁹的情况下和解结案。¹³⁰ 但是，尽管全自动车辆尚未大量配置，法院和评论员已经开始探索传统的侵权概念将如何适应全自动驾驶车辆，在这样的场景中，人类驾驶员与技术之间不存在或存在较少的互动，因而也存在较少的过失机会。

在建立无过错责任制之前，普通法背景下的侵权责任确定问题将仍然是专家意见和陪审员期望之间的复杂争论点，而普通法将需要做出适应性调整。

售后责任。对于普通消费品，根据普通法背景下的侵权责任法，制造商、供应商和销售商侵权责任在始于销售时，也终于销售时。但是，在某些州，普通法在某些情况下对出售给特定消费者的专用重型设备或机械施加了持续性的售后责任，这些特定购买者可以由制造商或卖方进行识别，并且制造商或卖方可以与他们进行售后沟通。¹³¹ 尽管很少存在对出售时相当安全的产品进行改造或升级的义务，但普通法正在不断发展以适应具有可识别购买者的特定产品的情况。

HAV 制造商确实存在承担售后责任的可能性，因为 HAV 可被追踪，制造商和供应商正在根据更多经验和售后测试来开发升级车辆软件。一些 HAV 制造商可能会自愿提供这些升级软件以提高消费者的满意度、说服消费者购买车辆并降低诉讼风险。迄今为止，这些升级似乎仅限于软件，就像手机通常会提供软件升级一样。升级是否会扩展到硬件和设备尚待观察，但是制造商承诺升级或放弃承担设备或软件升级的责任的行为可能会影响扩展是否发生。售后责任可能包括警告新发现的与产品相关的风险、¹³² 更新软件决策方式以包含更安全的算法，或召回发现存在导致会严重伤害的缺陷产品。

133

当然，像当前的汽车制造商一样，HAV 制造商无疑将继续承担报告和召回有安全缺陷的车辆的监管责任。对于制造商而言，一个有趣且困难的决策难点将是，是否以及在什么情况下提供算法安全更新，并作为持续免费服务的一部分，抑或是对更新收取费用，以及向消费者做出与这些更新信息有关的何种承诺。侵权法、法规、行业标准和实践操作是否会以就这一复杂问题提供指导，尚待观察。

根据严格的责任规则，如果零部件在出售时没有缺陷，HAV 零部件供应商可能拥有 HAV 制造商无法获得的抗辩权。例如，向高级用户提供零部件的大宗供应商通常没有义务警告最终产品的购买者。¹³⁴ 警告消费者的义务由终端产品制造商承担。另外，如果终端产品制造商使用或修改无缺陷的部件而造成危险，部件供应商通常不对终端产品制造商或消费者负责，前提是部件供应商不知道有不当的使用或修改，¹³⁵ 或没有参与将其部件整合到终端产品中。¹³⁶ 这些抗辩是否会被提出，部分取决于供应商如何构建他们与制造商的关系，包括他们的合同、承诺（或没有承诺）和行为。此外，当零部件涉及到旨在不断学习和变化的人工智能时，可能会出现不同的分析。

违反保证

违反保证的索赔根据合同法提出。这类索赔存在三种情况：明示担保、对特定目的的默示担保和默示的适销性担保。¹³⁷ 根据美国《统一商法典》，明示保证是通过申明、产品描述或样品作出的。¹³⁸ 因此，产品制造商、供应商或销售商可以控制是否作出任何明示保证。默示保证取决于特定的买方和市场对产品的期望。

虽然技术水平可能是更新的，但对 HAV 商业交易中保证的法律分析仍然可以与任何自动化技术行业的保证相比较。例如，在 *Auto-Teria, Inc. 诉 Ahern* 一案中，一本小册子将一个自动洗车系统描述为“自动-投币操作-无需手洗劳动”。¹³⁹ 在投币器损坏后，该系统的买方将其断开，并由操作人员对该系统进行操作。¹⁴⁰ 法院认为破损的投币器违反了系统手册中的明示保证。¹⁴¹ 此外，法院认为自动刷洗功能违反了适销性和适用性的默示保证，因为该系统未能“有效地清洗汽车而不敲落其外部配件”。¹⁴²

为了避免违反保证的诉讼，HAV 制造商、零部件供应商和销售商可以认真考虑他们在广告、营销资料、销售材料、操作手册与消费者签订的合同中所声称的功能和承诺的范围。除了明确声称的功能外，广告、营销和销售材料可以根据技术能力和局限性进行调整。制造商还可以查阅各州的法规、条例和判例法，以确认哪些类型的声明被认为是明示的保证，以及相关法律要求和限制，包括免除默示保证的法律规定、补救措施的限制性和获得救济的法律程序。如果系统需要维护或周期性的安全检查，可以将这些信息传达给消费者，制造商可以考虑进行自动安全检查并报告制造商。此外，制造商和销售商将需要考虑机器学习，并考虑如何确保系统持续学习以及按照保证所称的方式进行。

网络安全和数据隐私相关的具体责任问题

除侵权和合同责任外，HAV 技术还带来了网络安全和数据隐私方面的责任风险。

网络安全

网络威胁已经成为人们对自动驾驶汽车安全性的担忧。¹⁴³如果制造商不能合理地解决这些风险，他们可能会因安全和数据泄露而承担责任，比如与黑客攻击或车辆盗窃有关的风险。与物联网一样，这些风险目前都是理论上的，但工程师和评论员对这类风险的预见引起了立法、监管和公众的关注，并提出对这些风险进行评估和预防。几年前，一位记者在一个精心设计的演示中展示了网络风险，黑客远程玩弄车载显示器和车辆功能，最后在高速公路上切断了车辆的电源--而司机仍在驾驶。¹⁴⁴虽然这是一个精心设计的演示，并且这种风险在缺乏实际控制的情况下可能很难实现，但制造商可能会考虑如何防止这些理论上的风险，并可能对那些他们无法完全防止的风险提出警告。

法院和监管机构将在 HAV 网络安全方面进行何种程度的审查，尚待观察。在美国加州的一起民事诉讼中，原告称福特、通用和丰田在其车辆中采用了易受到黑客攻击的技术。¹⁴⁵法院以缺乏资格为由驳回了此案，裁定“潜在”的黑客攻击不是事实伤害。在这一裁决之后，加州通过了美国第一部物联网法律，要求连接设备的制造商为设备配置合理的安全功能，这些功能（i）适合设备的性质和功能，以及设备可能收集、包含或传输的信息，以及（ii）旨在保护设备和其中包含的任何信息，免受未经授权的访问、破坏、使用、修改或披露。¹⁴⁶对设备的广泛定义可能包括需要连接互联网的 HAV 组件。据推测，短期内在没有额外的法规、条例或保证的情况下，传统判例法中的过失、产品责任和消费者保护的规则经过调整后，将被适用于网络安全背景下的制造商责任的确定。

根据网络安全方面的过失标准，诉讼理由必须包括证明汽车制造商违反了其对因安全漏洞而受伤的个人所负有的合理注意义务（有时称为一般注意义务）。在没有联邦或州政府的规定或自愿性的行业标准来设定最低的网络安全标准的情况下，对这种客观的合理注意义务的尺度和范围仍然不明确。到目前为止，大多数对于网络安全的保护工作都是自发的，因此制造商可采用的安全标准很少。

根据最近提出的联邦立法——其代表了国会在监管 HAV 网络安全风险方面最深入的一次尝试——关键网络安全条款主要要求制造商“限制对自动驾驶系统的访问”，并指定一名网络安全官员，以及对员工进行网络安全方面的培训。¹⁴⁷尽管当时的联邦法案要求制造商制定自己的网络安全计划，以“检测和响应网络攻击、未经授权的入侵以及虚假的信息或车辆控制命令”，但这些计划的具体内容由制造商决定。¹⁴⁸议员 Latta

的议案将强制要求网络安全政策包括如下内容 (i) “识别、评估和减轻可合理预见的漏洞的程序”；以及(ii) “采取预防和纠正措施以减轻[这些]漏洞的程序”。¹⁴⁹目前在美国，对于制造商必须采取什么行动，几乎没有具体的、有约束力的指导。

此外，由于没有额外的关于 HAV 网络安全的联邦立法，该行业有关网络安全和数据隐私的行为将受到美国联邦贸易委员会（“FTC”）根据《联邦贸易委员会法》第 5 条（“第 5 条”）的消费者保护条例的执法监管，以及具有类似执法权的州检察长根据其类似的州法律进行执法监管。第 5 条禁止企业从事不公平或欺骗性的行为，涉及不充分的 HAV 网络安全或消费者个人数据的保护，或对这些事项的欺骗性“承诺”。¹⁵⁰联邦贸易委员会还有权执行相关部门的隐私法，并可能适用于 HAV 的相关问题。¹⁵¹联邦贸易委员会可以利用这一权力来处理作出安全和数据隐私的欺骗性“承诺”的联网设备供应商，包括 HAV 供应商。¹⁵²

由于美国的法律或法规没有额外的要求，潜在的原告可能会寻求域外法律规则的指导。因此，制造商和供应商最好能够持续关注与 HAV 网络安全和数据隐私相关的外国法律、法规和标准。制造商和供应商也可以关注 NHTSA 关于车辆网络安全的最佳实践的非约束性指导。¹⁵³

如果有更多的联邦标准颁布，行业参与者应确保遵守所有的网络安全要求，并提供符合要求的文件。由于这些车辆中的自动化系统在配置后将继续学习和适应，如果没有强有力的报告和文件，将很难确定车辆基础设施的状态、漏洞，以及在受到特定指控时遭到的破坏。

数据隐私

数据隐私是未来 HAV 消费者的另一个潜在担忧，因为该技术可以收集、存储和分析重要的敏感信息。在最近的 NHTSA 研讨会上，行业参与者讨论了收集的数据类型和这些数据的用途。¹⁵⁴一些数据被整体收集以为终端用户服务，例如汽车功能信息。地理定位数据可用于交通管理或应急响应。所有这些数据--特别是定位数据--在本质上可能是敏感的，但更微妙的信息是识别终端用户和车主的偏好或行为。例如，个人的音乐偏好或互联网浏览记录，可能被收集并出售给第三方广告商。此外，对于 HAV，收集的个人信息可能是司机的指纹或虹膜。虽然数据可用于改善产品功能或实施安全措施，但收集的数据的广度和细节可能具有极高价值。事实上，麦肯锡公司发现，到 2030 年，全球汽车数据货币化的潜在收入池将达到 7500 亿美元。¹⁵⁵

数据的价值和隐私性质将引发重要的法律问题：(i) 应该允许收集哪些数据；(ii) 谁拥有这些数据，谁可以在什么条件下将数据货币化；以及(iii)从业者应该如何存储和保护数据，以保证隐私安全--无论是货币化、黑客攻击还是身份盗窃。消费者可能希望保留对其个人信息控制权，而制造商希望至少获得一些信息，用以整合和优化其 HAV。为了解决这一冲突，各方可能会同意发布数据以换取某些功能或补偿，或者在供应商合同、销售合同、甚至车主手册和隐私声明中分配 HAV 的数据所有权。¹⁵⁶但是，对于谁拥有数据的终极问题仍没有任何统一的解决方式，而且很可能会引发争议。¹⁵⁷

无论数据归谁所有，都可能因数据使用违反隐私政策和自律监管准则、数据丢失和身份盗窃而产生责任。若未能遵守个人信息收集和保护、禁止数据销售的州法，或未能尊重消费者对其个人信息的访问权、在需要时对其个人信息的修正或删除权，或未能尊重对其数据销售的选择权，也可能产生民事责任。¹⁵⁸因此，公司将需要考虑有关数据收集、保留、共享和防止丢失的企业政策和做法。

在全球、州、甚至某些地方，都存在正式的数据隐私标准。例如，在欧盟和欧洲经济区域，个人的隐私权包括对其个人数据的人权和财产利益，而公司必须遵守具体标准以保护这些利益。¹⁵⁹

在美国国内，一些州也试图规范类似的隐私问题。例如，加州的《消费者隐私法》赋予了数据泄露的个人诉讼权。¹⁶⁰它的保护措施涵盖了某些涉及特定个人信息的数据泄露行为。此外，在消费者有权获得赔偿之前，公司有机会纠正违规行为。但是，加州的数据隐私诉讼权标志着公司有很大的诉讼风险，因为该州本身可以提起民事处罚的诉讼。¹⁶¹虽然其他州的数据隐私法的范围更窄，¹⁶²但各州法律的不同做法给 HAV 制造商和销售商带来了不确定性和统一性的缺乏。¹⁶³

联邦政府还没有对车辆引起的数据隐私问题进行监管。SELF DRIVE 法案将要求公司制定有关信息“收集、使用、共享和存储”的书面计划，以及“车主或乘客数据最少化、去识别化和保留”的做法。¹⁶⁴但即使这些要求被采纳，也不会解决有关谁拥有数据等问题。因此，在美国，数据隐私问题仍在继续发展。

自助--不确定因素不应妨碍行动

尽管围绕着责任的诸多不确定性，车辆和部件制造商和销售商仍可以采取保护措施来保护自己。

与供应商签订赔偿协议。HAV 制造商和供应商可以通过赔偿协议，寻求他们之间责任界定和分摊。对于车辆制造商和供应商来说，这种合同定义和责任分配可以简化诉讼程序，降低诉讼成本。例如，如果摄像头出现故障并导致事故发生，赔偿协议可以允许车辆制造商将责任主体转移给摄像头制造商以进行辩护，或要求摄像头制造商配合并协助辩护，或允许车辆制造商的辩护诉讼费用得到补偿。

零部件供应商同样可以就其任何部件的使用和整合向车辆制造商寻求赔偿，他们可以试图限制向零部件购买者提供的任何赔偿。《侵权法注释（第三版）：产品责任法》¹⁶⁵和州法律为零部件制造商提供了避免或限制潜在责任的指导。零部件供应商面临着一种权衡：他们可以通过不“实质性地参与将[其]部件集成到其他产品的设计中”来最大限度地降低责任风险，¹⁶⁶但商业需求可能会要求他们与制造商合作，“设计一个能作为集成产品的特定部件”，或者甚至“协助修改集成产品的设计以接受卖方的部件”，从而承担责任风险。¹⁶⁷

对于 HAV 的零部件供应商来说，需要权衡的问题可能包括如何通过与终端产品制造商在产品设计和开发方面的合作来促进技术创新、产品改进和未来的销售，同时减轻随之而来的责任风险。由于 HAV 在从制造商出厂后，其运行能力会继续发生变化，这一点尤其复杂。因此，至少在某种程度上，赔偿或供应商协议可能允许公司控制对未来责任风险的容忍度。

合同方面的考虑。制造商也可以通过在销售协议或车主手册中加入某些条款和条件，使车主在车辆使用过程中承担某些风险，来寻求风险分配。在 HAV 自动化水平发展的早期，销售协议可以要求买方同意不在某些道路、某些天气条件下或在高风险的人口密集区使用车辆，或在这些条件下保持控制或合理注意。车辆功能的局限性同样可以在车主手册中进行概述和声明。此外，车主手册可以限制与不安全使用车辆有关的责任，如在没有标志的、未铺设的道路上行驶，或要求定期维护。

例如，汽车制造商可以要求车主定期测试车辆的传感器，以确保功能正常，以及可以要求车主定期更新系统软件，以优化车辆安全或修补安全漏洞。若车主不遵守定期维护或软件更新的规定，则可以免除制造商责任、限制赔偿或担保失效。¹⁶⁸在 **Carter** 案中，一位卡车车主在他的卡车发生故障后，声称车辆制造商有违约行为。¹⁶⁹但法院将卡车的故障归因于车主“过度使用车辆”，而不是“在购买之前就存在的任何缺陷”，因为车主没有遵守车主手册中列出的“定期维护”，同时还超出了操作手册中限制的卡车装载量。¹⁷⁰依靠这类判例获得胜诉的关键是对该等义务明确通知消费者并征得其同意。

保险。保险可以在当事人可能面临因 HAV 技术而产生的责任时，保护当事人的经济利益，HAV 技术包括硬件、软件、网络安全和数据管理。虽然保险公司可能会要求采取预防措施来换取保险，但他们可能会“根据被保险人的自我保护水平来确定保险费”，从而使司机和制造商在赔偿责任方面具有灵活性。¹⁷¹对于司机来说，投保 HAV 的费用预计会随着时间的推移而降低，因为大多数公路事故是由司机的错误而不是机械故障造成的。¹⁷²新的市场刺激了风险资本家和企业家为 HAV 保险公司打下基础，一些主要制造商倾向于自己提供保险。¹⁷³当然，所有这些保险都是适用于车主的责任保险，而不是针对制造商在广泛的产品责任框架下的潜在责任。

车辆制造商的保险水平和方式仍不清楚，但保险业已将这一机会确定为增长领域。¹⁷⁴ HAV 制造商、供应商和销售商的保险可用性和成本将部分取决于适用的法律责任规则。学者和评论家已经在发表关于潜在的保险条款的言论。¹⁷⁵建议 HAV 制造商、供应商和销售商关注保险条款的发展，并在需要时仔细审查他们的保单是否涵盖 HAV。

行业标准。监管上的空白为制造商、供应商和销售商与其他利益相关者一起制定行业自律标准留出了空间，这些标准可以作为监管的基础。到目前为止，交通部一直鼓励制定行业标准，因为没有人比制造商和供应商更了解技术的能力和局限性。此外，制造商和供应商最能够确定什么在技术上可行、什么在经济上有利。行业标准也可以帮助指引判例法下的责任，尽管这些标准不是决定性的。最后，制造商和供应商应该抓住这个机会，塑造自己的未来和 HAV 的未来。¹⁷⁶

结论

在缺乏综合性的州法律以及统合性联邦法律法规的情况下，随着 HAV 行业的进一步发展，HAV 制造商、供应商和卖方可考虑通过以下若干方式降低发生产品责任索赔的风险：

- 列出合同义务、责任、陈述与保证以确定在与零部件或最终产品的交互中可能存在的潜在风险；
- 与利益相关方共同推动行业标准以及联邦、州和地方法规的发展，从而为部署与测试提供便利；
- 调查消费者对产品使用、广告和介绍的观点，以了解消费者的期待以及无意的潜在的误解；
- 开发产品预警自动注册系统，包括售后警告和召回，从而可直接向消费者传达重要讯息；
- 关注州责任法的制定，必要时介入和推动有利于HAV部署与测试的普通法规则；
- 密切关注可在美国适用的外国法律、法规和指南的发展；

- 为可预见的风险购买充分的保险；
- 就产品开发和消费者使用相关的网络安全和数据隐私事宜制定联邦和州合规规定。

联系律师

Barbara M. Harding 华盛顿 +1.202.879.4681 bharding@jonesday.com	底特律/哥伦布 +1.313.230.7950 / +1.614.281.3950 jjjones@jonesday.com	Charles H. Moellenberg Jr. 匹兹堡 +1.412.394.7917 chmoellenberg@jonesday.com	Mauricio F. Paez 纽约 +1.212.326.7889 mfpaez@jonesday.com
Jeff Rabkin 旧金山/硅谷 +1.415.875.5850 / +1.650.739.3954 jrabkin@jonesday.com	Charlotte H. Taylor 华盛顿 +1.202.879.3872 ctaylor@jonesday.com		

Keeton H. Christian, Autumn Hamit Patterson, and Stephen C. Scott 协助撰写本白皮书。

尾注

¹ Jillian D'Onfro, [亚马逊将在数月内开始使用无人机递送包裹](#), 《福布斯》(2019年6月5日)。基于对未来空中送货上门服务的预期, 美国联邦航空管理局在2021年1月公布相关新规。规则要求无人机必须进行远程识别, 并且允许小型无人机在特定条件下在人群上空以及在夜间飞行。“小型无人驾驶飞行器系统越人运行”, 《联邦公报》第86卷第4314页(2021年1月15日); “无人驾驶飞行器远程识别”, 《联邦公报》第86卷第4390页(2021年1月15日)。

² Kim Lyons, [Nuro 公司自动驾驶机器人将为休斯顿的达美乐顾客提供披萨配送服务](#), THE VERGE (2021年4月12日)(自2021年4月起, 休斯顿特定居民区内的达美乐顾客可以选择由机器人作为其配送披萨。)。

³ Sean O'Kane, [UPS 一直悄无声息地使用自动驾驶卡车运输货物](#), THE VERGE (2019年8月15日)。

⁴ Shay Eliaz, Robert Krumpf, Tom Aldred, [《打造移动未来: 电动汽车、自动驾驶汽车以及共享汽车中的化学品和特殊材料》](#), 德勤(2018年4月19日)。

⁵ [国际汽车工程师协会发布最新版“驾驶自动化等级”标准的可视化图表](#), 国际汽车工程师协会(2018年12月11日)。

⁶ 同上。

⁷同上。

⁸路面测试在全球范围内都有所增加。例如，沃尔沃公司在瑞典推出了 Drive Me 项目。[Drive Me - 全球最为大胆先进的自动驾驶公共试点项目今日启动](#)，沃尔沃公司（2016 年 9 月 9 日）。上海成为中国首个颁发自动驾驶车辆牌照的城市。Ryan Daws，[上海在中国率先允许自动驾驶汽车运载乘客](#)，IOTNEWS（2019 年 9 月 19 日）。此外，韩国专门建设一座占地约 89 公顷的城镇，用于测试自动驾驶汽车。Will Sabel Courtney，[韩国为测试自动驾驶汽车建设整个城镇](#)，《THE DRIVE》（2017 年 5 月 9 日）。

⁹[Move Nona 出行技术项目](#)，BEEP（上次访问时间 2021 年 3 月 12 日）；Alan Ohnsman，[Waymo 公司将推出更多“仅有乘客”（Rider Only）的自动驾驶汽车服务](#)，《福布斯》（2019 年 10 月 28 日）。黄石国家公园将于 2021 年 5 月推出自动驾驶摆渡车。Brandi Vincent，[美国国家公园管理局探索推出新兴自动驾驶技术试点项目供公众选择参与](#)，NEXTGOV（2020 年 10 月 30 日）；亦可参见 David Welch，[通用汽车旗下自动驾驶公司 Cruise 将于 2023 年在迪拜推出自动驾驶出租车服务](#)，彭博网（2021 年 4 月 12 日）。（2023 年，Cruise 公司将在迪拜启动自动驾驶出租车服务，该公司预计，其自动驾驶车队的无人驾驶穿梭车数量将会在 2030 年前扩充至 4,000 辆。）

¹⁰Ian Duncan，[弗吉尼亚州北部郊区的自动驾驶班车充分揭示机器人车辆未来进展缓慢的原因](#)，《华盛顿邮报》（2019 年 10 月 12 日）。

¹¹Kevin Todd，[技术不可预测的情况下，监管机构能否跟上形势？](#)，《密歇根法律评论》（2019 年 10 月 7 日）。

¹²Tim Levin，[亚马逊旗下自动驾驶初创公司 Zoox 近日推出一款无方向盘的自动驾驶电动出租车，一次充电续航 16 小时-看看外观是什么样](#)，《商业内幕》（2020 年 12 月 14 日）。

¹³Joshua Dowling，[苹果联合创始人史蒂夫·沃兹尼亚克抨击自动驾驶汽车，称其“在我有生之年”都不可能实现](#)，《汽车咨询》（2019 年 10 月 29 日）。

¹⁴Aarian Marshall，[埃隆·马斯克承诺在 2020 年推出真正的自动驾驶特斯拉汽车](#)，《连线》（2019 年 2 月 19 日）。2020 年 12 月，特斯拉称其自动驾驶（Autopilot）和完全自动驾驶（Full Self-Driving）功能为 SAE 2 级自动化的代表功能，并表示该等功能性预计在未来近期“基本保持不变”。Timothy B. Lee，[Tesla：“Full”特斯拉：自动驾驶测试版并非为完全自动驾驶功能设计](#)，《科技艺术》（2021 年 3 月 9 日）。2021 年 2 月，美国国家运输安全委员会建议国家公路交通安全管理局对相关保护措施予以监管，确保驾驶人在使用自动驾驶系统时不超出超出系统预期运行的条件。[美国国家运输安全委员会主席罗伯特·萨姆沃特致国家公路交通安全管理局的函](#)（2021 年 2 月 1 日）。

¹⁵Steve Crowe，[研究人员对特斯拉自动驾驶汽车不采用激光雷达技术表示支持](#)，《机器人报告》（2019 年 4 月 25 日）。

¹⁶Shahian-Jahromi Babak 等，[自动驾驶地面车辆的控制：简要技术评论](#)，《2017 年英国物理学会会议系列：材料科学与工程》第 224 卷 012029，2017 年第 4 期。

¹⁷John R. Quain，[该等高科技传感器或成自动驾驶汽车的关键](#)，《纽约时报》（2019 年 9 月 26 日）；亦可参见 Chris Wiltz，[FLIR 公司的热传感器将在 2021 年用于自动驾驶汽车](#)，DESIGNNEWS（2019 年 11 月 6 日）。

¹⁸Ryan Whitwam，[麻省理工学院为自动驾驶汽车开发出利用阴影探查拐角的功能](#)，《尖端技术》（2019 年 10 月 29 日）。

¹⁹Arun Ganesan，[自动驾驶时代，面部识别能否保护我们的数据？](#)，INFO. SEC. BUZZ（2018 年 5 月 30 日）。

²⁰Aarian Marshall，[停车场何以成为自动驾驶汽车的难题？](#)，《连线》（2019 年 10 月 28 日）。

²¹中国正在快速扩大自动驾驶汽车测试规模。Meghan Han，[北京 2019 年自动驾驶汽车路面测试距离居全球之首，高达百万公里](#)，SYNCED（2020 年 3 月 14 日）。今年又有一家中国公司取得无人驾驶汽车公共道路测试许可。[百度连续三年蝉联北京自动驾驶汽车道路测试报告排名首位](#)，美通社（2021 年 2 月 5 日）。

²²Allie Arp，[研究人员开发出自动驾驶汽车安全性可扩展测试的平台](#)，（2019 年 10 月 25 日）。

²³ Darrell Etherington, [麻省理工学院利用阴影帮助自动驾驶汽车探查拐角](#), (2019年10月28日)。

²⁴ Tom Stone, [TTI 德州农工交通研究所试用可提供驾驶信息的新型机器可读路标](#), TRAFFIC TECH. TODAY (2017年12月21日)。相关公司正在致力于开发相关基础设施,帮助HAV降低驾驶场景处理难度,但有评论人士质疑,如果HAV软件能够在无需高成本升级的情况下适应环境,更换现有基础设施是否属于可行和审慎之举。Matt McFarland, [自动驾驶汽车尚不成熟,但更为智能的道路有可能扭转这一情形](#), CNN (2021年3月5日)。

²⁵ Gary Elinoff, [C-V2X 正在赶超 DSRC 成为车对车通信的主流技术?](#), ALL ABOUT CIRCUITS (2019年3月5日)。

²⁶ 同上。

²⁷ 参见同上。

²⁸ [DSRC 与 C-V2X 在安全性应用方面的比较](#), AUTOTALKS 公司网站(上次访问时间2021年3月15日)。

²⁹ 参见同上;亦可参见Sieeka Khan, [Verizon 与本田公司合作开发基于5G和移动边缘计算的安全驾驶措施](#), 科技时代网站(2021年4月8日美国东部时间1:23 PM)(本田与Verizon拟就基于5G和移动边缘计算的互联自动驾驶汽车开展合作,旨在实现行人、车辆与基础设施间更快更优质的通信)。尽管目前仍处于大力发展5G技术的阶段,但6G已经成为设想的下一个发展方向。

³⁰ 参见国家公路交通安全管理局(NHTSA)网站的[法律法规](#)(上次访问时间2021年3月15日)。

³¹ 参见NHTSA [《FMVSS 203 的实验室测试程序:转向控制系统驾驶员防撞保护》](#),交通部TP-203-02(1990年5月4日)。

³² NHTSA要求各制造商根据联邦安全与测试标准进行自检,但也许可豁免。参见《联邦法规汇编》第49篇第555.1-555.18条;同时参见Laura Fraade-Blanar & Nidhi Kalra所著的[《无人驾驶汽车和联邦安全标准:对规则的豁免?》](#), RAND CORP (2017年)。

³³ 参见[《无人驾驶汽车对NHTSA的FMVSS规定的豁免》](#), 共享出行中心(2020年2月1日)。

³⁴ 例如,对于无人驾驶安全标准,联合国的欧洲经济委员会去年举办了世界车辆法规协调论坛,研究并通过了针对不同自动化程度车辆的具体法规。比如,临时议程, [《有关自动车道保持系统车辆批准的统一规定的新联合国条例提案》](#), 联合国欧洲经济委员会(2020年4月6日)。尽管欧洲并不符合SAE的自治定义,该等条例主要管辖SAE3和SAE4等效车辆。该等条例之一包括要求只能在无行人的公路上进行操作、使用备用驾驶员并实施诸如自动驾驶系统功能自检和协助推断事故障碍的数据记录仪等设计特性等新安全标准。参见同上。日本同样颁布了对其《道路运输车辆法》的修订案,对SAE3级及更高级别的车辆予以管制。参见Takeyoshi Imai, [自动驾驶技术的法律规制:日本当前状况与问题](#), 国际交通安全学会杂志(2019年)第43期第263页。该修订案实施最低的使用与部署安全标准、限制该等自动系统的使用条件(具体包括公路、环境和地理限制)、要求定期维修以确保传感器和自动驾驶系统功能正常,并要求提供授权访问协议,即要求用户只有在获得制造商授权后方可修改车辆系统或电信功能。参见,同上。

在网络安全和数据保护方面,为保护消费者利益,其他国家已实施公司必须遵守的正式程序。例如,根据欧盟的《通用数据保护条例》,该等程序包括强制性数据清单和数据流整理、根据请求清除个人信息的正式程序、披露数据隐私操作实践,以及与服务提供商签订书面合同等。参见Jacob M. Victor, 欧盟通用数据保护条例:建立保护数据隐私的财产制度, 123 YALE L.J. 513 (2013); [加州消费者隐私法案](#)事实说明,加州司法局。代表欧洲委员会的独立分析小组发布了一项报告,列出了自动化驾驶汽车未来发展的20项伦理建议。参见,欧洲委员会,联网自动化驾驶汽车伦理(2020年9月)。该报告部分与隐私和数据保护有关,鼓励利益相关者相互合作以更好地实施该等建议。参见众达, [欧洲委员会专家组发布联网自动驾驶车辆隐私相关建议](#)(2021年4月)。

美国交通部部长皮特·布蒂吉格称,与已经拥有“非常强健策略”的其他国家不同,“美国的政策框架尚未真正赶上技术平台或正在发展的其他事物。”参见政府将交通基础设施作为优先事务,第117届国会(2021年)52:11-30(交通部部长皮特·布蒂吉格的作证)。

³⁵ 参见法案H.R. 3388, 115th Cong. (2017); S. 1885, 115th Cong. (2017)。

³⁶ [H.R.3388](#) - 《无人驾驶法案》，CONG（上次访问时间 2021 年 3 月 21 日）；[《自动驾驶启动方案》](#)，CONG。（上次访问时间 2021 年 3 月 21 日）

³⁷ 参加法案 [H.R. 8350](#), 116th Cong.（2020）。

³⁸ 参见[同上](#)。

³⁹ 参见[同上](#)。

⁴⁰ 参见[同上](#)。

⁴¹ 参见[同上](#)（重点强调）。

⁴² 参见[同上](#)。

⁴³ 参见[同上](#)。

⁴⁴ 议员 Thune (R-S.D.)和议员 Peters (D-Mich.)曾共同支持自动驾驶立法，并且两人都曾关注在议会中再次推进两党立法。Maggie Miller，[议会再次推进自动驾驶车辆法案](#)，《国会山报》（2021 年 2 月 17）。

⁴⁵ 美国运输部，[自动驾驶：综合计划](#)（2021 年 1 月）；国家科学科技会议和美国运输部，[保障美国在自动驾驶技术方面的领导能力：自动驾驶 4.0](#)（2020 年 1 月）；美国运输部，[自动驾驶 3.0：为未来的交通方式做好准备](#)（2018 年 10 月）；美国运输部和美国高速公路安全管理局，[自动驾驶系统 2.0：安全前景](#)（2017 年 9 月）；美国运输部和美国高速公路安全管理局，[联邦自动驾驶车辆政策：加速道路安全的变革](#)（2016 年 9 月）。

⁴⁶ 车辆 4.0，前注 45，第 5 页；综合计划，前注 45，第 4 页。

⁴⁷ [美国运输部长 Elaine L. Chao 宣布首次参与新型自动驾驶倡议网络试点，以提高安全性、性能测试和公众参与度](#)，美国高速公路安全管理局（2020 年 6 月 15 日）。

⁴⁸ Beep、Cruise、快意佳士拿汽车、Local Motors、Navya、Nuro、丰田，优步和 Waymo 是最早参与“自动驾驶车辆透明度和参与度的安全测试计划”的公司。参见[同上](#)。

⁴⁹ 加利福尼亚州、佛罗里达州、马里兰州、密歇根州、俄亥俄州、宾夕法尼亚州、德克萨斯州和犹他州参与“自动驾驶车辆透明度和参与度的安全测试计划”。参见[同上](#)。

⁵⁰ [美国交通部宣布扩大“自动驾驶车辆透明度和参与度的安全测试计划”](#)，美国高速公路安全管理局（2021 年 1 月 11 日）。

⁵¹ 新型自动驾驶计划，前注 47；参见副局长 James Owens，[评论“自动驾驶车辆透明度和参与度的安全测试计划”](#)，美国高速公路安全管理局（2020 年 6 月 15 日）。公众可以使用交互式测试追踪工具浏览参与者的测试信息。[“自动驾驶车辆透明度和参与度的安全测试计划”：测试追踪工具](#)，美国高速公路安全管理局（2021 年 3 月 15 日）。

⁵² 美国高速公路安全管理局，具有高性能自动驾驶或全自动化驾驶的机动车辆合作研究的试验计划；意见征询期延长，83 Fed. Reg. 59353（2018 年 11 月 23 日）。

⁵³ 美国交通部联邦汽车运输安全管理局，配备自动驾驶系统的商用车辆的安全集成，84 Fed. Reg. 24449（2019 年 5 月 28 日）；美国高速公路安全管理局，消除自动驾驶系统车辆的监管障碍，84 Fed. Reg. 24433（2019 年 5 月 28 日）。

⁵⁴ 参见，例如，美国运输部，自动驾驶系统的乘务人员保护措施，85 Fed. Reg. 17,624（2020 年 3 月 30 日）。

⁵⁵ 参见[同上](#)。

⁵⁶ 参见[同上](#)。

⁵⁷ 参见第 II(A)(2)(a)部分。

⁵⁸ [美国高速公路安全管理局首次就无手动控制车辆乘务人员的保护措施提出全标准现代化的建议](#)，美国高速公路安全管理局（上次访问时间 2021 年 3 月 17 日）（处置方式为“未决”）。

⁵⁹ 美国高速公路安全管理局，自动驾驶系统的安全结构，85 Fed. Reg. 78058（2020 年 12 月 3 日）

⁶⁰ 同上。

⁶¹ 同上。

⁶² 美国高速公路安全管理局，自动驾驶系统的安全框架：意见征询期延长，85 Fed. Reg. 78058（2021年1月29日）。美国交通部长 Pete Buttigieg 表示支持发展自动驾驶汽车，并表示其认为有必要在这一领域作进一步监管。部长 Buttigieg 在他的听证会上说，“自动化车辆技术即将来临；它发展迅速....并且极具变革潜能[，]我认为政策在多方面未能予以支持。”Luke Bellos, [运输部长提名人 Pete Buttigieg 推进有关基础设施政策的新兴技术](#), IOT EVOLUTION（2021年1月25日）。此后，Buttigieg 部长在众议院交通和基础设施委员会前澄清称，他优先考虑建立“监管的确定性以及为消费者和公司提供安全基础设施，以便让这种技术充分发挥其潜力。”参见[政府将交通基础设施作为优先事务](#)，前注 34，3:42:24–36。

⁶³ 参见 5GAA 弃权申请，[见关于：请求放弃在全部（C-V2X）技术中采用智能交通系统移动车辆](#)，案卷号 18-357（2018年11月21日）；Ford 向美国联邦通讯委员会致函提出弃权申请（2019年1月24日）。

⁶⁴ 美国联邦通讯委员会，关于建议制定规则的通知：使用 5.850- 5.925 GHz 频段，案卷号 19-138，11（2019年12月12日通过）

⁶⁵ 同上，第 28 页。

⁶⁶ [美国运输部部长 Elaine Chao 向 Ajit Pai、美国联邦通讯委员会主席所作的致函](#)（2019年11月20日）；参见 David Shepardson, [政府机构质疑联邦通信委员会将汽车频谱转为无线网络的计划](#)，《美国汽车新闻》（2020年10月29日）。国务卿 Pete Buttigieg 在众议院交通和基础设施委员会声明，他和两党一样关注 5.9 GHz 频段的重组，并计划在整个政府范围内参与如何以最好的方式处理和共享与安全性一致的频谱，及目前和未来的通信形式。参见 31:00–39，前注 34，[政府将交通基础设施作为优先事务](#)。

⁶⁷ [议院成员向 Ajit Pai、美国联邦通讯委员会主席和专员所作的致函](#)（2020年1月22日）。

⁶⁸ 参见 Monica Allevan, [美国联邦通讯委员会授权 5.9 GHz 频段的 C-V2X](#)，《无线新锐》（2020年10月29日）。

⁶⁹ 参见同上。

⁷⁰ 关于 5.850-5.925 GHz 频段的使用，备案号 No. 19-138, 11 的美国联邦通信委员会，第一次报告及命令，后续拟议规则制定通知，拟议修改命令。（于 2020 年 10 月 18 日通过）。

⁷¹ 参见 [美国联邦通信委员会供 Wi-Fi 和汽车安全使用的现代化 5.9 GHz 频段](#)（2020 年 10 月 18 日）

⁷² 现有的联邦法律确实对 HAV 领域的州法规设置了一些限制。例如《美国联邦航空管理局授权法案》（“FAAAA”）禁止各州通过“与财产运输有关的任何汽车承运商的价格、路线或服务等方面的”立法。49 U.S.C. § 14501(c)(1)。法院对这一优先条款作出了广义解释，将对汽车承运商的价格、路线和服务产生“间接”影响的条款包括在内。Rowe v. New Hampshire Motor Transp. Ass’n, 552 U.S. 364, 370 (2008)（引自 Morales v. Trans World Airlines, Inc., 504 U.S. 374, 386（1992））。但是 FAAAA 明确允许各州对安全、保险要求和“机动车的型号或重量或【其】货物的危险性质”进行监管。49 U.S.C. § 14501(c)(2)。

⁷³ [自动驾驶车辆国家法案追踪数据库](#)，国家立法机构的全国会议（2021 年 3 月 15 日）。

⁷⁴ 参见 e.g., Okla. Stat. tit. 47, § 11-310 (e), (f)（废除“机动车以电子协调速度统一行驶”的尾随禁令）；明尼苏达州州长 Tim Walz 第 19-18 号行政命令（2019 年 4 月 8 日）（成立“关于联网和自动化车辆的州长顾问委员会”）。

⁷⁵ [2018 年 3 月 18 日，美国亚利桑那州坦佩市高速公路事故报告：试验型自动驾驶系统控制的车辆与行人相撞](#)。国家运输，SAFETY BD. 55（2019 年 11 月 19 日）。

⁷⁶ 参见 [自动驾驶车辆国家法案追踪数据库](#)，见前注 73（表明 11 个州已通过关于 HAVs 测试的立法）

⁷⁷ 参见同上。（列出了 10 项加州通过的 AV 相关法案，其中包括几项与测试相关的法案）。

⁷⁸ 参见 Cal. Veh. Code § 38750(d)（授权加州机动车辆管理局通过有关自动驾驶车辆的法规）；Cal. Code Regs. tit. 13, §§ 227.00–227.54（自动驾驶车辆的测试）；Cal. Code Regs. tit. 13, §§ 228.00–28（自动驾驶车辆的投入使用）。

⁷⁹ [许可证持有人（与司机一同测试）](#)，加州机动车辆管理局；[许可证持有人（无人驾驶测试）](#)，加州机动车辆管理局；[许可证持有人（投入使用）](#)，加州机动车辆管理局。

⁸⁰ Cal. Veh. Code § 38750(b)(3); Cal. Code Regs. tit. 13, §§ 227.04(c); 227.30(a)(1)（多达 10 辆 HAVs 和 20 名司机的费用）

⁸¹ Cal. Code Regs. tit. 13, §§ 227.32, 227.34, 227.36, 227.38.

⁸² [2018 年 4 月行政命令：推进自动驾驶车辆的检测及运行](#)；优先保护公共安全；[无人驾驶的自动驾驶车辆的检测及运行](#)，亚利桑那州，交通部。

⁸³ 高速公路事故报告，见前注 75，第 55–59 页。

⁸⁴ 参见 75 Pa. Stat. and Cons. Stat. §§ 102, 3317.

⁸⁵ [自动驾驶车辆测试指南](#)，宾夕法尼亚州，交通部。2（2018 年 7 月 23 日）。优步在匹兹堡郊外开辟了一个区域来测试自动驾驶汽车技术。内部人士 Lisa Eadicicco 称，[优步不久前悄悄购买了 600 英亩土地，用以在匹兹堡建立一个新的自动驾驶汽车测试轨道](#)（2019 年 12 月 26 日）。其他几家公司，包括 Aptiv, Argo AI, Aurora 以及卡内基梅隆大学也在匹兹堡测试无人驾驶汽车。VENTURE BEAT 的 Kyle Wiggers 称[各公司正在匹兹堡测试 55 辆自动驾驶汽车](#)（2019 年 4 月 26 日）。

⁸⁶ 参见 [generally, e.g., Volvo Car Corp 在美国众议院能源和商业委员会上关于自动驾驶汽车所作的声明：自动驾驶汽车的投入使用工作](#)（2017 年 2 月 14 日）；Daniel A. Crane et. al., [自动驾驶和联网车辆的使用引起的法律问题调查](#), 23 MICH. TELECOMM. & TECH. L. REV. 191, 222 (2017)（收集关于一致性要求的声明）。

⁸⁷ 各州通常将某些道路监管权下放给地方政府，如分区、道路标志、交通信号、限速、交通摄像头和道路维护。这些地方问题可能会影响到 HAV 制造商。例如，亚利桑那州钱德勒的一项分区条例被用来鼓励当地财产所有人提供 HAV 停车场。参见 Katherine Shaver, [城市规划者着眼于自动驾驶车辆，以纠正 20 世纪关于汽车领域的失误](#)，《华盛顿邮报》（2019 年 7 月 20 日），Aarlan Marshall, [亚利桑那州钱德勒 32 小时，世界自动驾驶汽车之都](#)，《连线》（2018 年 12 月 8 日），[钱德勒是美国第一个将自动驾驶车辆和拼车纳入分区法规的城市](#)，钱德勒，亚利桑那州（2018 年 4 月 27 日）。地方法规除了激励和阻碍 HAVs 外，对自动驾驶汽车的测试和使用也产生了重要影响。例如，匹兹堡已经与 HAV 制造商签订了一系列非正式协议，允许在没有实质性监督的情况下进行检测。参见 Lucy Perkins, et al., [全美自动驾驶车辆驾驶员：市政行动指南](#)，全美城市联盟 26–27 (2018)。其他城市，如波士顿，明确限制了测试的时间和地点，并要求在任何测试之前，需提交正式申请和审查。参见[波士顿自动驾驶车辆政策制定的行政命令](#)，波士顿市（2016 年 10 月 20 日）；[自动驾驶车辆：波士顿的方法](#)，波士顿市（2021 年 1 月 19 日；也可参见[波士顿自动驾驶车辆测试谅解备忘录模板](#)（2017 年 1 月 20 日）。

⁸⁸ 国务卿布蒂吉格已经承认目前许多安全法规与 HAV 不兼容，因为他们假定人类驾驶员驾驶车辆。参见[政府将交通基础设施作为优先事务](#)，前注 34，在 3:41:31–42:00。

⁸⁹ 当然，其他自然人或实体也可能需要对导致 HAV 事故负责，比如那些进行了故障维修或未能安装软件升级的人或实体。

⁹⁰ 但是，目前，一些立法者坚持认为，HAV 允许驾驶员自行决定接管控制权。John Bonazzo, [参议院讨论对无人驾驶汽车立法的安全担忧](#)，《观察家》（2018 年 2 月 12 日，下午 4:38）。

⁹¹ 参见 [《有关自动驾驶和联网汽车发展的法律问题》](#)，JONES DAY (Nov. 2017)（讨论了驾驶员培训，可能在使用消费者期待测试来认定严格责任的州影响此分析）

⁹² 这些保护方法中的每一种都需要对适用的联邦和州法律进行透彻的分析，这超出了本白皮书概述的范围。保险范围的可用性和条款以及州法对保险的要求引发了市场和监管机构需要解决的复杂问题。请参阅 [《通往无人驾驶汽车之路：保险的含义》](#)，JONES DAY（2017 年 4 月）（概述了有关自动驾驶汽车行业参与者潜在产品责任的一些关键保险问题）。

⁹³ Michael J. Miles & Jeffrey E. Jakob, [《根据修订后的第 37（e）条进行的发现制裁：安全港》](#) AM. BAR ASS'N（2016 年 8 月 30 日）。

⁹⁴ NHTSA 在 2016 年发布的指导文件中指出：“车辆至少应记录与车祸事故和系统性能有关的所有信息，以便可以重新模拟事件的发生。”《联邦自动驾驶汽车政策：加速道路安全的下一次革命》，同前注 45。2021 年 3 月，英国标准协会在英国发布了“在自动驾驶汽车试验期间收集、整理、存储和共享信息的要求” [PAS 1882: 《2021 年用于事故调查的自动驾驶车辆试验数据收集和管理—规范》](#), BSI (2021 年 3 月)。

⁹⁵ 参见如《事件数据记录器》，美国国家公路交通安全管理局（最后访问 2021 年 3 月 13 日）（讨论了车辆事件数据记录器基于其复杂性的多方面使用）

⁹⁶ 亚利桑那州 Uber 车手乔纳森·斯珀林 (Jonathan Sperling) 在致命自动驾驶汽车撞车事故发生前在 Hulu 上播放了“The Voice” (2018 年 6 月 22 日，上午 9:43)。尽管本白皮书着眼于民事责任，但亚利桑那州事故进一步表明，在某些情况下可能会产生刑事责任。该事故的后备驾驶员被指控犯有过失杀人罪，定于 2021 年 2 月接受审判。 [Uber 驾驶员 Jay Ramey 在致命 2018 年自动驾驶车中被起诉](#), AUTOWEEK (2020 年 9 月 16 日)。后备司机的过失杀人罪指控仍待处理，没有最终处置。 [State of Arizona v. Rafael Stuart Vasquez](#), No. CR2020-001853-001 (Ariz. Super. Ct.)，（最后访问时间 2021 年 3 月 13 日）。法国已开始起草法律，在诸如亚利桑那州事故之类的与 HAV 相关的事故中，在驾驶员和制造商之间分配刑事责任。请参阅 [《法国计划对自动驾驶汽车采用新规则》](#), JONES DAY (2021 年 4 月)

⁹⁷ 参见 49 U.S.C. § 30103

⁹⁸ 529 U.S. 861 (2000)。

⁹⁹ 562 U.S. 323 (2011)。

¹⁰⁰ 参加法案 [H.R. 8350](#), 116th Cong. (2020)（着重强调）。

¹⁰¹ 参见同上。

¹⁰² 参见 49 U.S.C. §§ 20106(b)(1)(A), (B); *Ryder v. Union Pac. R.R. Co.*, 945 F.3d 194, 203 (5th Cir. 2019)。

¹⁰³ 参见，例如，*Cipollone v. Liggett Grp., Inc.*, 505 U.S. 504 (1992)。

¹⁰⁴ 参见前注 34。

¹⁰⁵ 参见，例如 ECON. COMM'N FOR EUROPE，前注 34。

¹⁰⁶ 366 P.3d 33 (Wash. App. 2015)

¹⁰⁷ 同上，见 36-39 页。

¹⁰⁸ Kenneth S. Abraham & Robert L. Rabin, 《自动驾驶汽车和制造商对事故的责任：新时代的新法律制度》，105 VA. L. REV. 127 (2019)。

¹⁰⁹ 向严格责任的转变始于 1990 年代早期交通事故的背景下。参见如 *Macpherson v. Buick Motor Co.*, 111 N.E. 1050 (N.Y. 1916)。严格责任被证明能够适应科技的变化和由此引起的事故和损害。

¹¹⁰ 《侵权法重述（第三）》产品责任第 2 条 (AM. L. INST. 1998)，也可参见如 *Zamora v. Mobil Corp.*, 704 P.2d 584 (Wash. 1985)（阐述了这些原则植根于以下理论：销售商和制造商是最不会避免成本的人，并且最适合确保设计安全性和功能性。）

¹¹¹ 参见 [《消费者期待测试》](#)，LEGAL INFO. INST., 《康奈尔法律评论》（最后访问于 2012 年 3 月 13 日）

¹¹² Andrea Dearden, [诉讼认为福特的后视系统造成幼儿车道死亡](#), SE. TEX. RECORD (2014 年 9 月 10 日)

¹¹³ 许多州认为消费性包装品的销售商承担有限的产品责任。像目前的汽车一样，HAV 是否会落入该限制范围尚不确定。但是，经销商协议或普通法可能赋予销售商对制造商的赔偿权。参见 2 FRUMER & FRIEDMAN, PROD. LIAB. § 15.03(1)(e) (Matthew Bender, Rev. ed. 2021)（讨论了每个州适用普通法赔偿的可行性）由于销售商可能会继续与 HAV 的购买者和用户保持直接联系，因此他们还可以在教育消费者有关 HAV 技术及其局限性以及所有者和驾驶员责任方面发挥作用。销售商可以指出不同车辆上的各种技术选择。他们还可以提供保修方面的限制。销售商也可以通过自己的广告和对买方的陈述为

责任索赔建立事实依据。参见 2 James B. Astrachan et al., THE L. OF ADVERT. § 14.03 (Matthew Bender 2021) (概述与卖方广告说明有关的潜在责任范围)。一些汽车制造商也正在考虑一种未来直接向消费者销售的模式,其中可能包括新形式的信息传播。参见如 Aria Alamalhodaiei、[电动汽车竞争对手特斯拉和 Rivian 联合制定直接销售法案](#), TECHCRUNCH (2021 年 3 月 3 日,上午 11:59) (讨论公司采用直接面向消费者的销售模式,并游说所有 50 个州对直销立法)

¹¹⁴ Cami Perkins, 《在设计缺陷索赔中对侵权法重述 (三) 风险效用分析的接受度越来越高》, 4 NEV. L.J. 609 (2004).

¹¹⁵ 104 S.W.3d 600, 602–03 (Tex. App. 2003)

¹¹⁶ 参见同上, 见第 605 页 (着重强调)。

¹¹⁷ 参见同上, 见第 608-09 页。

¹¹⁸ 参见同上, 见第 603、608-09 页。

¹¹⁹ 861 N.Y.S.2d 431, 432–33 (N.Y. App. Div. 2008)

¹²⁰ 参见同上。

¹²¹ 参见同上, 见第 434 页。

¹²² 消费者混淆或误解的索赔也可能导致根据州消费者保护法针对制造商或销售商的欺诈或欺骗行为的索赔。参见 Gregg v. Ameriprise Fin., Inc., No. 29 WAP 2019, 2021 WL 607486 (Pa. Feb. 17, 2021). 此外, 某些州还制定了针对虚假广告的法规来保护消费者。参见, 如, Cal. False Advert. L, Cal. Bus. & Prof. Code §§ 17500 et seq

¹²³ Rosenberg v. Harwood, No. 100916536, 2011 WL 3153314 (D. Utah Dist. Ct. May 27, 2011).

¹²⁴ 参见 Jo Ciavaglia, [针对 GPS 造成学生受伤的波士顿交通事故、价值 1500 万美元的诉讼](#), BUCKS CNTY COURIER TIMES (2015 年 1 月 26 日)。

¹²⁵ Cruz v. Talmadge, 15-0222 (Mass. Super. Ct. Jan. 23, 2015).

¹²⁶ Glorvigen v. Cirrus Design Corp., 796 N.W.2d 541 (Minn. Ct. App. 2011).

¹²⁷ 各州是否会修改其对 HAV 的驾驶执照要求, 例如在操作 HAV 之前必须通过 HAV 的驾驶考试的要求, 还有待观察。参见《高度自动化车辆的安全测试和部署的管辖权准则》29-31, 自动驾驶汽车最佳做法工作组, AM. ASS'N OF MOTOR VEHICLE ADM'RS (May 2018) (讨论自动驾驶汽车驾驶员执照考试的标准化程序, 具体取决于其自动化程度); Ben Husch and Anne Teigen, [《规制自动驾驶汽车》](#) NAT'L CONF. OF STATE LEGISLATURES (Apr. 2017) (说明了佛罗里达州是第一个根据当前驾驶执照要求允许拥有有效驾驶执照的自动驾驶汽车运营的州); Mark Harris, [《您需要自动驾驶汽车的新执照吗?》](#), IEE SPECTRUM (Mar. 2, 2015 15:00 GMT), (解释说, 对 HAV 的驾驶员执照要求的潜在修订可能包括“关于自动驾驶技术的能力和局限性的课程, 故障计算机模拟, “脱离接触”实践以及自动车辆设置和系统停用教程)

¹²⁸ 参见 Glorvigen, 796 N.W.2d at 552 (解释说提供足够的安全使用说明的义务包括“培训最终用户熟练操作的义务”是前所未有的) (强调)。

¹²⁹ 参见 Hudson 诉 Tesla, Inc.案 (涉及一起自动驾驶车辆与停滞在行车道上的残疾车辆相撞的事故)。

¹³⁰ 参见 Nilsson 诉 Gen. Motors LLC 案 (一辆处于自动驾驶模式的车辆, 放弃了最初的并线尝试, 最终与一辆摩托车相撞, 导致司机受伤)。

¹³¹ 参见 Kozlowski 诉 John E. Smith's Sons Co.案。

¹³² 参见《侵权法注释 (三)》: Prods. Liab. §10 (AM. L. INST. 1998) (商业产品销售商或分销商对销售后未发出警告造成的伤害的责任); 另见同上, §13 (继承人对继承人自己销售后未发出警告造成的伤害的责任)。

¹³³ 同上, 参见§ 11 (商业产品销售商或分销商对销售后未召回产品所造成的伤害的责任)。

¹³⁴ 参见《侵权法注释（第三版）》。Prods. Liab. § 5 cmt. a (AM. L. INST. 1998) (讨论了“大宗销售/高级购买者规则”，该规则认为“未参与将零件整合到产品设计中的零件销售商不应仅仅因为零件的整合导致产品有危险缺陷而承担责任”)。

¹³⁵ 参见同上，§5 cmt.e (“一个零件卖家如果只是按照买方的规格设计一个零件，而没有实质性地参与将该部件整合到产品设计的过程中，则不承担责任...”)。

¹³⁶ 参见同上。

¹³⁷ 参见 Sean P. Wajert, 有关产品责任的索赔、抗辩和救济, PRAC. LAW LITIG, (最后访问时间 2021 年 3 月 13 日); 另见 Stephanie E. Niehaus & Huu Nguyen, 人工智能和侵权责任: 发展前景, PRAC. LAW LITIG. (最后访问时间: 2021 年 3 月 13 日)。

¹³⁸ 参见《美国统一商法典》§ 2-313 (AM. L. INST. & UNIF. L. COMM'N 2020 ed.)。

¹³⁹ 参见判例 352 N.E.2d 774, 777 (Ind. Ct. App. 1976)。

¹⁴⁰ 同上, 参见判例 778 页。

¹⁴¹ 同上, 参见判例 781 页。

¹⁴² 同上, 参见判例 781-82 页。

¹⁴³ Buttigieg 部长解释说, 交通部将在解决网络和数据隐私问题和威胁方面“坐镇”。见政府对交通基础设施的优先权, 前注 34, 1:35:00-14。

¹⁴⁴ 参见 Andy Greenberg, 《黑客远程操控我乘坐的吉普车》, WIRED (2015 年 7 月 21 日)。

¹⁴⁵ 参见 Cahen 诉 Toyota Motor Co.案。

¹⁴⁶ 参见《加州民法典》§§ 1798.91。

¹⁴⁷ 参见法案 H.R. 8350, 116th Cong. (2020)。

¹⁴⁸ 同上。

¹⁴⁹ 同上。

¹⁵⁰ 见《美国民法典》15 U.S.C. § 45(a)(2)。

¹⁵¹ 例如, 联邦贸易委员会有权执行不遵守适用于直接数字营销的《控制非请求的色情和营销的攻击, CAN-SPAM 法案》, 以及适用于在线收集儿童数据的《儿童在线隐私保护法》。见《美国民法典》15 U.S.C. § 7706; 15 U.S.C. § 6505。

¹⁵² 参见《车辆数据隐私》, NHTSA (最后访问时间: 2021 年 5 月 4 日) (“虽然 NHTSA 对乘用车的安全有广泛的监管权, 但 FTC 才是负责保护消费者隐私的主要联邦机构。”); 另见《车辆技术和服务的隐私原则》, GLOBAL AUTOMAKERS (2014 年 11 月)。

¹⁵³ 参见《现代汽车的网络安全最佳实践》, NHTSA (2016 年 10 月); 另见《NHTSA 征求对现代汽车安全的网络安全最佳实践的意见》, NHTSA (2021 年 1 月 8 日) (宣布对更新现代汽车的网络安全最佳实践草案的公众意见)。

¹⁵⁴ 参见《联系汽车工厂》, FED. TRADE COMM'N (2018 年 1 月)。

¹⁵⁵ 参见《车辆数据货币化》, MCKINSEY & CO. (2016 年 9 月)。

¹⁵⁶ 参见 Sylvia Zhang, 谁拥有你的智能汽车产生的数据? 32 HARVARD J.L. & TECH. 299, 311-12 (2018); 与自动驾驶、自动化和联网汽车发展有关的法律问题, 前注 91。

¹⁵⁷ 参见前注 156。

¹⁵⁸ 参见《加州民法典》§§ 1798.100 et seq.; 另见 VA S.B. 1392 § 59.1- 571 et seq。

¹⁵⁹ 另见 Victor, 前注 34 (讨论欧盟的《通用数据保护条例》如何规定数据发明标准、数据流的映射、选择退出程序、以及披露和合同要求)。

¹⁶⁰ 参见《加州民法典》§§1798.100 等; 《加州消费者隐私法》概况介绍, 前注 34。

¹⁶¹ 参见《加州民法典》§ 1798.155(b) (版本有效期至 2023 年 1 月 1 日)(部分规定,“每次违规的民事处罚不超过两千五百美元(\$2,500),或每次故意违规的民事处罚不超过七千五百美元(\$7,500),这将在总检察长提起的民事诉讼中评估和赔偿。”) ; 但见同上, §1798.155(a) (2023 年 1 月 1 日执行的版本) (部分规定相同,但对每次故意违规或“涉及企业、服务提供者、承包商或其他人实际知道未满 16 岁的消费者的个人信息的违规行为,可处以行政罚款和 7500 美元”)。

¹⁶² 参见《2019 年消费者数据隐私立法》, NAT'L CONF. OF STATE LEGISLATURES (Jan. 3, 2020)。

¹⁶³ 虽然制造商和销售商不必遵守加州或欧洲对其他地方的产品销售规定的标准,但考虑普通法索赔的法院可能会参考这些标准来评估制造商或销售商的行为是否合理。

¹⁶⁴ 参见议案 H.R. 8350, 116th Cong. (2020)。

¹⁶⁵ 参见《侵权法注释(第三版)》: Prods. Liab. §5 (AM. L. INST. 1998)。

¹⁶⁶ 同上, 见§ 5 cmt. a。

¹⁶⁷ 同上, 见§ 5 cmt. e。

¹⁶⁸ 参见 Lawrence 诉 S. Recreations, LLC 案; 见 Carter v. Chrysler Motors Corp 案。

¹⁶⁹ 参见 Carter 案, 384, 839–41。

¹⁷⁰ 同上, 见 842–43。

¹⁷¹ 参见,《网络安全保险》, CYBERSECURITY AND INFRASTRUCTURE SEC. AGENCY (最后访问时间: 2021 年 4 月 9 日)。

¹⁷² 参见 Eric Schneider,《自动驾驶汽车和自动驾驶汽车的保险》, FOUNDER SHIELD (2019 年 7 月 23 日)。

¹⁷³ 同上。

¹⁷⁴ 参见埃森哲和史蒂文斯理工学院,《从现在到 2025 年,为自动驾驶汽车投保是一个 810 亿美元的机会》, ACCENTURE (2017)。

¹⁷⁵ 同上。

¹⁷⁶ 参见《Vehicles 4.0》, 前注 45 (概述了联邦政府在制定和实施标准和监管政策方面与行业和政府当局的协调努力); 国际汽车工程师学会宣布成立合作自动化驾驶系统委员会, SAE INT'L (2020 年 11 月 24 日) (宣布委员会制定有关自动化车辆和其周围环境(包括行人、其他驾驶者和基础设施)之间的通信标准); 另见《安全驾驶倡议, 自主车辆治理生态系统: 决策者指南》, WORLD ECON. FORUM (2021 年 4 月) (白皮书提供了“相关产业联盟、财团和其他团体的情况”, 并“[强调]关键标准机构”); Laura Fraade-Blanar et al., RAND CORP,《衡量自动驾驶汽车安全: 发展中的框架(2018)》(为公共和私人利益相关者提供一个高度自动驾驶车辆的安全测量框架)。

众达出版物不应被视为针对某事件或情形发表的法律意见。众达出版物旨在为读者提供一般信息。未经众达书面同意, 任何人不得在其它出版物或诉讼中引用或引述众达出版物的内容。众达保留批准他人引用或引述众达出版物内容的权利。如需申请众达出版物的转载许可, 请使用众达网站 (www.jonesday.com) 上的“联系我们”表格。众达发表出版物的目的并非试图与读者建立律师和客户的服务关系; 读者收到众达出版物也不表示律所与读者之间会构成律师和客户的关系。众达出版物中的观点仅属于作者的个人观点, 并不一定代表律所的观点。