

众多产业行业与DeepSeek“联姻结对” 将为我们带来什么？

新华社北京2月17日电 DeepSeek在多家医院完成本地化部署；微信测试接入DeepSeek；部分地区政务系统已接入……众多行业产业与DeepSeek“联姻结对”的消息接踵而至，令人不禁想问：AI正在加速接入我们的生活，究竟会带来什么？

中央党校(国家行政学院)国家治理教研部研究员、博士生导师翟云指出，中国经济的快速发展为进一步发挥人工智能的赋能作用提供了广阔的“用武之地”，Deep-Seek的深度接入既有利于加快破解传统

产业数字化、智能化转型过程中面临的“急难愁盼”，也有利于加快消除“智能鸿沟”，让社会共享AI发展带来的技术红利。

“DeepSeek接入微信、医院等场景带来了资源整合的功能，接入微信也集成在搜索功能。”一位清华大学计算机系博士生感到，这一变化为自己正在开展的大模型底层高性能计算技术研究打开了新的视阈，也为普通人提供了更多便利化路径。

“对于微信这种有大量公众号文章、数据的平台，靠人力整合文本资料是很花时间的。有了AI加持，普通用户在寻找资

料方面可以更加便捷，而对于简单的问题，AI也能根据已有资料进行进一步推理并直接给出答案。”他说。

智谱公司的一位算法工程师告诉记者，DeepSeek的接入能提高人工智能应用的整体渗透率，让更多人在触手可及的地方体验最新的AI能力，对培育大众对人工智能的了解和认知很有帮助。但同时也要看到，大模型技术发展目前还在上升期，更好更强的模型还会持续出现，距离真正形成通用人工智能(AGI)级别的生产力还需要大量算法、技术和

工程上的持续创新，希望大家持续关注并且更加大胆地尝试将AI技术运用到生活和工作中。

不少专家在受访时也表示，任何技术都是一把双刃剑，人工智能对人类社会的改变和影响也在引发争议甚至忧虑。

翟云强调，对于DeepSeek这样的新生事物，既要充分释放场景活力，为新技术的应用打造更多“试验场”，从战略层面及时总结提炼科技创新的经验启示，也需正视并妥善应对潜在的数据泄露、隐私侵犯及技术伦理等风险。

智能网联汽车隐私焦虑何解 亟需发展隐私友好的产品设计，增强用户对隐私的可控感

“以前觉得汽车内是安全的私密空间，现在汽车能够联网、更加智能，却担心它收集我的隐私并有可能泄露。”智能网联汽车车主张女士说。

张女士的焦虑并非空穴来风。为更好实现辅助驾驶、智能导航等功能，许多汽车尤其是新能源汽车正加速推进车联网。智能网联汽车通过采集车主行驶轨迹、驾驶习惯、人脸指纹、车内语音等个人信息，提供智能化、个性化服务。

从这个意义上说，智能网联汽车不只是交通工具，更是信息收集器。据了解，一辆智能网联汽车每天能产生TB级(1TB=1024GB)海量数据，这些数据包括高清晰度视频数据、高精度位置信息、高敏感度个人隐私信息等，给车主隐私安全埋下隐患。

这些隐患正在被引爆——2023年，某品牌汽车被曝超215万名用户车辆数据泄露；同年，9名某国外车企前员工爆料，该企业员工曾通过内部系统分享客户车载摄像头记录的部分视频和图像……

当置身其中的汽车同时是一台数据收集器，车主如何对隐私安全安心？

收集处理个人信息 被框定在“必要的最小范围”

汽车智能化步伐加快，让隐私安全攻防战日益胶着。赛迪顾问数据显示，2023年全球智能网联乘用车的新车渗透率已经超过一半；中国市场的新车渗透率达68.2%，预计到2025年达到78.9%，占据乘用车市场主导地位。

多位专家告诉记者，智能网联汽车快速发展趋势下，为维护信息安全，汽车通过摄像头、传感器、麦克风等收集处理个人信息被法律框定在“必要的最小范围”内。

我国民法典、网络安全法、数据安全法、个人信息保护法等为汽车数据收集处理提供了根本遵循。比如民法典要求“处理个人信息的，应当遵循合法、正当、必要原则，不得过度处理”，个人信息保护法规定“收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息”。

也就是说，必要性是个人信息收集的前提。中国政法大学传播法研究中心副主任朱巍说，智能网联汽车采集个人信息须经过用户授权，且只能采集对驾驶目的有意义、必要的信息。“比如，汽车如果不采集路途中的位置信息，就无法实现导航功能，这类信息属于必要。但汽车如果访



在天津(西青)国家级车联网先导区封闭测试场，智能网联汽车测试员在封闭测试开始前进行调试检测(2024年6月14日摄)。 据新华社

问用户通讯录，对用户在车内的通话录音，通过收集的数据给用户精准推送广告，就属于过分收集信息。”

也有专家指出，需根据用户对汽车功能要求的变化，综合研判哪些信息收集属于必要。中国电动汽车百人会供应链研究与合作中心主任高翔说：“比如开车时电话响了，有的汽车会自动语音提示是谁打来。实现这个功能就需要连接手机和汽车，让汽车读取手机通讯录。汽车为了提升用户体验和安全性会发展新的功能，功能的实现又依赖于数据收集。”

2021年10月施行的《汽车数据安全管理若干规定(试行)》提出明确的数据安全要求，倡导汽车数据处理者在开展汽车数据处理活动中坚持四大原则，即车内处理原则(除非确有必要不向车外提供)、默认不收集原则(除非驾驶人自主设定，每次驾驶时默认设定为不收集状态)、精度范围适用原则(根据所提供功能服务对数据精度的要求确定摄像头、雷达等的覆盖范围、分辨率)、脱敏处理原则(尽可能进行匿名化、去标识化等处理)。

尽管法律法规对智能网联汽车的隐私保护做出规定，但在实操层面尚存在细化程度不足、数据权责界定不清晰等难点，消费者较难举证车企侵犯隐私权。

“很多车企声明数据所有权为消费者所有，但当一些消费者和车企因为数据收集发生争执时，消费者很难从车企拿到相关数据作为证据。”汽车资讯平台“懂车帝”汽车安全测试相关负责人说，车企应做好数据管理，和消费者充分沟通，尽量

满足消费者提出的合理数据获取要求。

如何建好隐私安全“防火墙”？ 需要相关供应链企业形成合力

智能网联汽车不仅要保障功能安全，还要保障信息安全，给相关技术“防火墙”的构筑提出更高要求。

据了解，目前智能网联汽车的数据存储方式按存储位置可划分为车内、云端、边缘存储等。车内存储通常会利用车载硬盘等设备，云端存储将大量数据上传到云端服务器，边缘存储则是在靠近车辆的边缘节点，如路边的基站、智能交通设施等存储数据。

车内存储的敏感数据由于不离开车辆，在三种存储方式中泄露风险相对较低，有利于隐私保护，但受限于存储容量和计算能力。因此车企倾向于将数据存储于云端和边缘节点。这就让智能网联汽车在数据访问控制、数据加密解密、抵御网络攻击等方面面临更大挑战。

据了解，目前较多车企在车辆设计之初就倾向于建立一体化的数字平台整合数据资源，并在此基础上建立统一的数据安全架构。一些车企还在进行数据访问控制、数据脱敏与匿名化处理等常规操作之上构建数据安全评估大模型，实现数据安全管理的智能化、自动化发展。

专家认为，随着智能网联汽车用户、相关个人信息数据不断增多，车企数据安全团队可加快探索应用前沿数据保护技术。比如，利用区块链的分布式存储、不

可篡改等特性，建立车联网数据访问控制的去中心化体系，提高访问控制安全性。

与此同时，筑牢智能网联汽车信息安全网还需要相关供应链企业在责任、技术等方面形成合力。有专家指出，智能网联汽车是一个垂直领域数字生态系统，它将汽车与手机、电脑、摄像头、各种传感器、道路基础设施、服务器、数据中心等诸多要素建立起基于网络的互联互通关系。因此需要整个供应链上所有包含数字元素的部件或系统制造商共同担负网络安全责任，而不是把安全责任简单“打包”交给整车企业，甚至转嫁给用户。

守护移动的私域 隐私友好的智能设计引关注

当智能网联汽车等智能产品日益融入生活，消费者需要确保对自身隐私的控制权，需要感受到隐私友好的智能产品氛围。

记者采访多位智能网联汽车车主了解到，部分车主在日常驾驶中，会因担心隐私问题分心，无法充分享受智能技术带来的便利和乐趣。还有部分车主出于隐私安全考虑，不愿使用一些创新、便捷但需要收集更多个人隐私的智能服务。

显然，车主对隐私安全的焦虑，以及由此产生的技术抵触心理，亟需智能网联汽车发展隐私友好的产品设计文化，增强用户对隐私的可控感。

2024年下半年，“懂车帝”测试了120余款热门车型，超过半数的车型拥有车内摄像头，但约60%的车型没有为摄像头配备可调节的物理遮挡，还有约24%的车型摄像功能无法被手动关闭。

对此，专家认为手机信息权限管理的发展为车企提供了一定思路，车企可以参考手机信息权限管理设置，让用户自行决定是否启用车内摄像头、麦克风等硬件设备，避免过度收集信息。

隐私友好的智能汽车设计正引起更多关注。2024年11月，中国汽车工业协会发布“汽车隐私保护”标识，授权首批通过测评的20余种车型相应车辆使用该标识。中汽协重点围绕隐私协议、麦克风、车内摄像头、定位信息、车外摄像头和用户体验等六项内容开展汽车隐私保护能力测评，涉及信息收集授权、收集提示、访问授权、数据删除、传输加密等方面，以此提升消费者对汽车的信任感。(据新华社社《瞭望》新闻周刊记者 魏雨虹)