**Dispute Settlement** 争议解决, 2026, 12(1), 182-191
Published Online January 2026 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2026.121024

Hans汉斯

# 《个人信息保护法》框架下我国智能网联汽车的个人信息保护研究

**黄露茜**

上海政法学院国际法学院，上海

收稿日期：2025年12月16日；录用日期：2026年1月9日；发布日期：2026年1月21日

## 摘　要

**新型汽车的“联网”功能日益普及，在智能网联汽车行业持续扩张、新型智能网联汽车应用和设备层出不穷的今天，妥善收集和处理用户个人隐私信息至关重要。因此，了解驾驶联网汽车及其数据服务所涉及的隐私问题，比了解其他消费品的隐私问题更为紧迫。然而，智能网联汽车应用开发者通常并未充分考虑这些措施，导致不安全的应用被发布。本文对智能网联汽车个人信息领域的安全和隐私问题进行了研究，主要包含三个部分：一是回顾相关学术文献；二是提出当前我国智能网联汽车个人信息保护存在的问题；三是为开发者提出一些建议，以帮助他们创建符合现行安全和隐私法规的智能应用。本文将对现有的安全和隐私标准及认证进行补充，并为应用开发者和研究人员提供一份简明指南。**

## 关键词

**个人信息保护法，智能应用，隐私数据，个人信息保护**

# Research on Personal Information Protection in China’s Intelligent Connected Vehicles under the Framework of the *Personal Information Protection Law*

**Luxi Huang**

School of International Law, Shanghai University of Political Science and Law, Shanghai

Received: December 16, 2025; accepted: January 9, 2026; published: January 21, 2026

## Abstract

**The “connectivity” function of new cars is becoming increasingly widespread. With the continuous**

文章引用: 黄露茜.《个人信息保护法》框架下我国智能网联汽车的个人信息保护研究[J]. 争议解决, 2026, 12(1): 182-191.
DOI: 10.12677/ds.2026.121024

**expansion of the intelligent connected vehicle industry and the emergence of numerous new intelligent connected vehicle applications and devices, the proper collection and processing of users' personal privacy information is crucial. Therefore, understanding the privacy issues involved in driving connected cars and their data services is more urgent than understanding the privacy issues of other consumer products. However, intelligent connected vehicle application developers often do not fully consider these measures, leading to the release of insecure applications. This paper studies the security and privacy issues in the field of personal information in intelligent connected vehicles, mainly in three parts: first, a review of relevant academic literature; second, the current problems in the protection of personal information in intelligent connected vehicles in my country; and third, suggestions for developers to help them create intelligent applications that comply with current security and privacy regulations. This paper will supplement existing security and privacy standards and certifications and provide a concise guide for application developers and researchers.**

## Keywords

**Personal Information Protection Law, Smart Applications, Privacy Data, Personal Information Protection**



## 1. 研究背景

所谓的联网汽车，即配备互联网接入的车辆，正在成为常态，它们的普及为消费者数据隐私倡导者敲响了警钟。根据 Counterpoint Technology Market Research 的数据，到 2030 年，95%以上的乘用车可能都具有嵌入式连接功能。这使得汽车制造商能够提供与安全、预测性维护和预测相关的功能。但这也为公司收集、共享或出售与驾驶习惯相关的数据以及人们可能不想共享的其他个人信息打开了大门。[1]随着智能网联汽车产业的不断发展，各汽车公司及其他第三方主体开始收集、保存和使用大量个人信息用于各种目的，网联汽车的发展已成为数字时代蓬勃发展的无价资源。然而，网联汽车产业的蓬勃发展导致个人信息保护面临风险，例如信息泄露、个人信息的非法和过度使用、侵犯信息隐私等问题。这些风险在世界各地引发了伦理和法律担忧。这些乱象的背后，是网络技术的不合理运用、监管层面的漏洞，以及用户个体特点等因素交织成的结构性难题。由于个人信息本身具有虚拟属性，这使其更易被非法泄露和滥用，不仅严重威胁用户的隐私安全，也对社会稳定和风气产生了不良影响。为了应对技术发展对个人信息带来的挑战，2021 年 8 月，《个人信息保护法》正式出台。这部法律以“告知与同意”为核心原则，强调最小必要原则，明确了个人信息获取和使用的规范流程，赋予用户撤销授权的权利，旨在遏制企业“一揽子授权”“强制同意”等侵权行为。法律要求信息获取方只能在实现既定目标的前提下，以最小范围收集和使用信息，并且必须采取加密存储、定期检查等技术手段保障信息安全。《个人信息保护法》为个人信息保护构筑起一道坚实的法律屏障。它不仅明确了用户的权利，也规定了企业的法定义务，构建起事前预防、事中监督、事后救济的全流程保护体系。但在技术快速迭代的今天，信息强制授权、告知条款缺失、信息泄露盗用等侵权行为依然屡禁不止。基于此，本文聚焦一个关键问题：哪些因素会显著影响智能网联汽车用户隐私保护的实际效果？通过探究这一问题，以期提升《个人信息保护法》的

[1]https://www.cnbc.com/2024/03/23/how-to-stop-your-internet-connected-car-from-selling-your-driving-data.html, 2025-05-17.

社会效能。

## 2. 文献回顾

随着移动智能网联汽车的深度普及，智能汽车在消费、生活服务等场景的渗透率显著提升，随之而来的用户隐私保护问题逐渐成为数字社会治理的核心议题。智能网联汽车下的用户隐私保护的有效性是多方主体协同作用的结果，用户作为隐私数据的提供者、权利主张者及政策参与者，是隐私保护的出发点和落脚点；企业作为数据收集与处理者的核心角色，是监管规则的主要约束对象；监管主体作为规则的制定方、执行方以及公共利益维护者的核心角色，其行为动态始终贯穿着隐私保护的始终。整体逻辑链条贯穿用户隐私保护能动性、企业责任履行与监管制度供给三个维度。现有研究围绕三者的交互作用展开，形成了丰富的理论成果与实证发现。

### (一) 国内研究现状

1、用户认知与行为

用户对隐私的认知和隐私行为是影响用户隐私保护有效性的重要因素之一。用户对隐私的主观认知与防御性操作构成隐私保护的基础环节。张玥和朱庆华(2014)的研究表明，用户对隐私的认知存在差异，这种差异会影响其对隐私保护的需求和行为，且直接影响其保护需求层级[1]。张大伟、谢兴政(2021)发现用户往往会在个性化服务和隐私保护之间权衡，这种权衡行为会对隐私保护产生影响[2]。

智能网联汽车用户的隐私行为，是指个体借助移动终端设备或移动应用程序所具备的隐私防护功能，采取相应措施以避免个人信息泄露的行为表现。具体而言，涵盖用户对个人信息可见权限的设置(如是否允许他人查看个人信息)、对应用程序数据记录权限的管控(如是否允许记录浏览历史)，以及对个人敏感信息采集权限的管理(如是否允许收集身份信息、联系方式、地理位置等隐私数据)等方面。依据贾若男(2021)等学者的观点，在社交网络环境下，用户的隐私保护行为与其隐私保护意愿呈现显著的正相关关系。当个体对自身保护隐私的能力感知较强，即自我效能感较高时，往往会主动采取更为积极且多样化的隐私保护策略。这一行为逻辑源于用户对个人隐私安全的重视，以及对潜在信息泄露风险的预判[3]。曹明增(2024)等作者在《基于位置服务中的位置隐私保护技术综述》中进一步指出，用户在使用基于位置的服务时，对隐私保护的需求和行为存在显著差异，这种差异会影响隐私保护的有效性[4]。

2、企业责任履行

企业的合规操作和隐私保护设计是保障用户隐私的关键环节，企业运营方的合规能力与技术设计，直接决定隐私保护的落地效能。程啸(2018)强调，企业在设计智能应用时，应充分考虑用户的隐私需求，将隐私保护融入产品设计中[5]。欧阳洋、袁勤俭(2016)的研究揭示，在电子商务场景下，消费者的隐私关注度主要受信任水平、网站声誉以及信息重要性这三大关键因素的制约。研究表明，消费者对电子商务平台的信任程度越高、网站在业界积累的声誉越好，以及被收集信息的敏感程度越低，消费者的隐私关注强度就会相应减弱[6]。曹达(2019)从“用户个人信息分类”“收集与存储”“使用与共享”“用户权利”四个方面，对 17 类 104 个社交媒体平台的隐私政策文本展开系统性分析，研究指出我国社交媒体平台个人信息保护政策文本整体处于非规范化状态，普遍存在框架结构不完整、内容表述模糊不清，以及用户知情权、可携带权等权益保护条款缺失或界定不明等问题[7]。

随着信息技术不断发展，部分企业为营销无限制收集用户信息的做法，让消费者的隐私担忧愈发强烈。如何在消费者保护隐私的诉求和企业挖掘用户信息价值的需求之间找到平衡，成为当下急需解决的现实问题。在这样的背景下，越来越多企业通过制定并公布隐私政策，试图缓和两者之间的矛盾冲突。但是目前，我国智能网联汽车的隐私政策还存在不少问题，李青(2022)等学者提出了当前大部分隐私政策存在的问题，认为不少隐私政策文本仍存在“重形式轻实质”的问题，仅机械性地向用户展示一份预先

拟定、旨在规避法律风险的“告知”文件[8]。王娜(2023)等学者在研究用户的隐私规避行为时提到，平台干预和隐私泄露，是影响用户隐私保护的关键。在移动应用领域，这些因素直接左右用户对隐私政策的关注与接受。智能网联汽车运营商作为责任方，需创新隐私政策展示方式，以简洁直观的形式，提高用户隐私保护意识，减少用户对隐私政策的漠视，提升政策执行效果，完善隐私保护体系[9]。

3、监管制度供给

伴随互联网与智能应用对个人信息采集使用频次攀升，数据主体隐私风险加剧，我国持续完善相关立法。2012 年《关于加强网络信息保护的决定》率先确立互联网个人信息使用原则与权责。2017 年《网络安全法》搭建隐私保护法律架构，《民法总则》明确个人信息受民法保护。2021 年《民法典》人格权独立成编，深化隐私权与个人信息保护，凸显立法重视。《中华人民共和国个人信息保护法》第 17 条第 3 款规定：“个人信息处理者须公开其个人信息处理规则。履行自己的告知义务。”《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》第 12 条规定：“网络用户或者网络服务提供者利用网络公开自然人基因信息、病历资料、健康检查资料、犯罪记录、家庭住址、私人活动等个人隐私和其他个人信息，造成他人损害，侵权人请求其承担侵权责任的，人民法院应予支持。”这些法规既为运营商提供行为准则，也为评估 APP 隐私政策合规性提供依据。

当前学界对我国监管体系的研究，主要聚焦于监管方式与监管力度的现存缺陷及优化路径。刘璐(2025)在研究中指出，我国当前隐私保护监管体系存在结构性缺陷，突出表现为缺乏独立的专门监管机构，现有职能分散于多部门的监管模式难以形成治理合力，直接导致执法效率低下，成为制约隐私保护有效性提升的关键瓶颈[10]。雷丽彩、郭芷欣(2024)在研究中指出：相比之下，政府监管主要发挥辅助与支撑功效，旨在激励平台在现有隐私保护基础上进一步优化升级。然而，仅依靠政府补贴尚无法单独促使平台从本质上转变其隐私保护策略[11]。俞成峰(2024)提出，当前法律监管在隐私保护领域面临显著局限性。现有法律框架在应对跨国数据流动、算法黑箱等前沿问题时存在规则空白，导致跨境数据泄露、算法歧视等行为缺乏明确法律规制。这种局限性不仅削弱了法律的威慑力，更使得用户隐私在技术迭代中面临持续威胁[12]。李畅畅(2024)在研究中指出，目前，我国移动应用行业常态化监管机制不足。行业快速发展，短期内问题频发，短期专项治理仍有必要。但长远来看，必须建立常态化监管。这需要制定清晰的监管执法规范，明确标准流程；加强部门间协同，优化信息共享和执法协作。同时，推动监管模式转变：从突击整治转为长效治理，从注重事前监管转为事中事后全程监管，尤其要强化数据全流程监管，形成闭环管理，保障行业健康发展[13]。

**(二) 国外研究现状**

1、基于用户同意的隐私政策的研究

过去五十年，尤其是在二十一世纪，世界各地涌现出许多隐私法。这些法律通常主要基于“个人控制模型”，旨在赋予个人权利，帮助他们控制自身数据的收集、使用和披露，正如 Paul Schwartz 和 Karl-Nikolaus Peifer 指出的那样，GDPR 中的同意基于信息隐私不可剥夺的前提(Paul Schwartz and Karl-Nikolaus Peifer, 2017) [14]。《个人信息保护法》遵循欧盟 GDPR，将个人同意作为数据处理的法律基础，同意为数据处理提供了法律依据，隐私政策是实现这一权利的重要途径。毫无疑问，隐私政策对用户至关重要，但是基于同意的隐私政策受到了隐私学界和强制披露学界的批评，主要批评之一是其无法充分告知受试者，在线服务提供商广泛使用隐私政策来规范他们所收集的个人数据的使用，但用户经常跳过阅读，并且不知道有关他们的信息是如何被处理的，也不知道如何控制这些信息被收集、存储或共享的方式。首先，一些研究者在先前的研究中表明，这些隐私政策常常被用户忽视(Acquisti and Grossklags, 2005) [15]；有研究者认为，数据主体需要阅读大量的隐私政策，一项披露本身可能看起来微不足道，但大量披露则令人难以承，用户很少阅读公司披露的信息，即使他们留意，也往往只是略读(Ben-Shahar and Schneider,

2011) [16]；还有研究者指出，数据主体必须花费大量时间阅读他们必须同意的所有隐私政策，导致他们没有足够的动力去阅读冗长乏味的隐私政策(Lorrie Faith Cranor, 2012) [17]。

其次，隐私政策的内容过于复杂，个人难以理解。理解个人数据收集和使用的解释通常需要超出大多数数据主体理解能力的专业知识(Solove, 2012) [18]。随着社会生活日益数字化，隐私政策变得越来越专业和复杂，数据主体理解起来也更具挑战性(Charlotte A. Tschider, 2020) [19]。根据先前的研究，大多数热门网站上的隐私政策都超过了大学的阅读水平(Kevin Litman-Navarro, 2019) [20]。有学者指出数据主体，尤其是那些缺乏专业知识的数据主体，很容易误解此类政策，就像普通人无法理解微积分一样(Patricia A. Norberg, Daniel R. Horne *et al*., 2007) [21]。例如，大多数数据主体无法区分动态和静态 IP 地址，他们很可能无法识别包含其个人数据的地址。

最后，有学者认为数据主体对阅读隐私政策毫无兴趣。2019 年的一项调查发现，只有 9%的美国人定期阅读隐私政策(Brooke Auxier *et al*., 2019) [22]。此外，“隐私悖论”的支持者认为，个人对数据隐私保护的关注仅存在于个人意识中，其行为所反映的态度存在显著差异(Ari Ezra Waldman, 2020) [23]。行为主义者将隐私悖论归因于个人数据泄露风险和危害的不确定性和非即时性(Long Chen *et al*., 2021) [24]。探究数据处理的风险和危害需要付出高昂的信息成本。因此，个人不太可能有动力去阅读和了解隐私政策。

2、基于企业隐私政策合规性研究

学者 MegJones 和 Margot Kaminski 所指出的，GDPR 中问责制的核心是企业能够证明其遵守该制度(Meg Leta Jones and Margot E. Kaminski, 2020) [25]。对于企业而言，证明其能力的一个重要方式是在隐私政策中承诺其实践将遵守法律。Ari Waldman 认为，数据处理者对数据隐私法的遵守只是表面的(Ari-Ezra Waldman, 2022) [26]。数据处理者可能会制定全面且注重隐私的隐私政策，但不会严格遵守(Ari Ezra Waldman, 2019) [27]。Paul M Schwartz 指出，隐私政策最好被理解为数据处理者用来构建其“隐私剧场”的工具，隐私剧场实际上增强了人们对隐私保护的感觉，但并未提供任何实质性的保护(Paul-M. Schwartz, 2008) [28]。然而，隐私政策的读者仍然可以成为“剧场批评家”，根据公司实际行为与其在隐私政策中承诺的差距来评估其做法(Christopher G Bradley, 2022) [29]。Bamberger Mulligan 采访的首席隐私官所说，隐私政策必须由公司所有部门支持的跨职能团队制定(Kenneth A. Bamberger and DeirdreK Mulligan, 2015) [30]。隐私专业人员与其他部门之间的合作经常会边缘化前者的意见，有时甚至会完全放弃它，数据隐私法应该承认隐私部门和专业人员的责任和权限，使他们能够在制定全面的隐私政策方面履行其专业角色(Ari-Ezra Waldman, 2018) [31]。Waldman 认为，数据处理者有必要在个人数据收集和处理的整个生命周期中将隐私专业人员整合到设计部门，以行使隐私政策作为自律宪章的职能(Ari Ezra Waldman, 2018) [32]。当前数据隐私法已经认识到将隐私政策融入产品或服务的优势，欧盟 GDPR 采用了设计和默认的数据保护原则；中国 PIPL 要求数据处理者有义务采用“相应的安全技术措施，如加密和去标识化”，然而，在实践中，信息的传播可能通过从设计部门到法律专业人员的单向流动进行，导致隐私政策中的信息披露滞后。

3、监管制度供给研究

监管机构的数据隐私执法与市场主体交易息息相关，学者 Daniel Solove 和 Paul-M Schwartz 指出隐私政策往往是监管机构的首要调查对象，并且由于监管资源始终有限，隐私政策往往是判断个人数据处理者是否损害消费者利益的重要参考(Daniel Solove and Paul-M Schwartz, 2021) [33]。例如，在美国，联邦贸易委员会(FTC)在开展调查时，总是首先审查隐私政策，以确定公司在个人数据的收集和处理过程中是否存在欺骗性或不公平的行为[34]。在欧盟，数据保护机构将隐私政策视为关键的监管对象，其模糊性正是谷歌被法

国国家自由和信息委员会(CNIL)罚款 5000 万欧元的原因。[2]同样，在中国，隐私政策问题也是国家互联网信息办公室执法的主要发动因素。[3]世界各地的司法管辖区都要求企业在其网站上发布隐私政策，例如，欧盟通过《通用数据保护条例》(GDPR)等法律来规范此类披露；在美国，隐私政策法规由州一级制定，例如《加州隐私权法案》，一些研究人员表示，这些法律遵循通知和选择原则，通知是指条款的呈现在本条例中是隐私政策，而选择则是表示接受这些条款的行为，例如点击“接受”链接或继续使用该网站。一些司法管辖区的数据隐私法要求监管机构对数据主体进行教育。例如，中国《个人信息保护法》(PIPL)规定国家有义务加强个人信息保护的宣传和教育。[4]欧盟《通用数据保护条例》(GDPR)也将提升公众意识纳入监管机构的工作范围。[5]目前尚不清楚这些监管机构应如何对数据主体进行教育，考虑到隐私政策在教育方面的潜在优势，要求公司提供更详细的隐私政策可能是监管机构履行其义务的一种方式。

## 3. 网联汽车中的个人信息保护面临的困境

### (一) 数据泄露与第三方滥用数据的风险

丰田披露了一起重大数据泄露事件，由于云存储桶配置错误，2013 年 11 月至 2023 年 4 月期间，超过 215 万客户的数据被泄露。此次泄露影响了丰田基于云的 Connected 服务的敏感信息，这些信息在 2013 年 11 月至 2023 年 4 月期间未经授权即可访问。虽然此次泄露仅影响日本客户，但丰田强调，个人客户的身份并未受到损害，也没有第三方滥用被泄露数据的报告。但该说法遭到客户质疑。此外，大众汽车及其子公司奥迪遭遇数据泄露，影响了 330 万客户，主要在美国和加拿大。此次泄露发生在 2019 年 8 月至 2021 年 5 月之间，泄露了用于销售和营销目的的客户数据，包括姓名、地址、电子邮件地址和电话号码，以及购买或查询的车辆的详细信息。虽然大多数记录包含基本联系信息，但美国约 90,000 名奥迪客户的更敏感数据遭到泄露，包括驾驶执照号码和社会安全号码。此次泄露被追溯到一家未具名的关联供应商。[6]网联汽车数据泄露的案例层出不穷，数据泄露、数据盗窃现在已经成为网联汽车中个人信息保护领域极为突出的问题。

### (二) 第三方滥用数据风险

根据上海市发布的《汽车销售行业个人信息保护合规指引》第四条第四款：未经消费者同意或请求，或消费者个人明确表示拒绝的，不得将消费者个人信息交第三方处理。需经由第三方处理个人信息的，应当征得消费者个人的同意，并于第三方合作协议中明确规定个人信息的保护责任、保密义务、违约责任、突发处置措施等条款。但现实中，汽车公司经常与第三方企业共享数据，有时甚至出售这些数据。这些第三方可以包括各种各样的实体，例如服务提供商、数据经纪人和其他公司。84%的汽车品牌将用户数据分发或出售给数据经纪人和其他企业等实体。令人震惊的是，超过一半的汽车品牌愿意在没有法院命令的情况下与政府或执法机构共享这些数据。[7]隐私政策在描述数据接收者时往往使用模糊的语言，让人不清楚究竟是谁在接收数据。汽车制造商可能会将从车主的网联汽车收集的数据与从第三方获得的个人信息相结合，从而形成更全面的用户的个人资料，这些信息通常用于营销和其他目的。许多汽车公司在其隐私政策中明确表示，他们有权出售用户的个人数据。这些数据可能包括从驾驶行为到个人偏好等

[2]The sanctions issued by The CNIL. https://www.cnil.fr/en/investigating-and-issuing-sanctions/sanctions-issued-cnil, 2025-05-17, 星期六。

[3]国家网信办依法集中查处一批侵犯个人信息合法权益的违法违规 APP。https://www.cac.gov.cn/2022-11/03/c1669106604621340htm，2025 年 5 月 17 日。

[4]《中华人民共和国个人信息保护法》第十一：“国家建立健全个人信息保护制度，预防和惩治侵害个人信息权益的行为，加强个人信息保护宣传教育，推动形成政府、企业、相关社会组织、公众共同参与个人信息保护的良好环境。”

[5]《欧盟通用数据条例》第五十七条：“promote public awareness and understanding of the risks, rules, safeguards and rights in relation to processing. Activities addressed specifically to children shall receive specific attention。”

[6]https://privacysos.org/blog/your-car-is-tracking-you/2023/9/18，2025 年 5 月 17 日。

[7]https://heydata.eu/magazine/navigating-the-road-of-data-privacy-what-your-car-knows-about-you/2023/10/18，2025 年 5 月 17 日。

各种信息。从汽车收集的某些数据可能会在共享或出售之前进行汇总和匿名化。汽车公司还可能与数据经纪人或汽车数据中心合作，后者充当收集、汇总和分发车辆数据的中介。这些数据经纪人可能会将数据出售给各种企业，包括保险公司、广告商和研究人员。可以肯定的是，出于安全和功能目的收集驾驶员和汽车数据是有正当理由的，而且一些基本服务(如紧急情况和安全相关的数据共享)可能很难或不可能选择退出。这些活动导致车主对于收集的其个人的信息几乎没有控制权。

**(三) 个人信息过度收集**

汽车可以收集大量关于我们的数据，包括我们的行踪、驾驶行为、语音互动，甚至生物特征细节，本质上演变成我们日常生活中接触的强大监听机器。这些数据对汽车制造商来说很有价值，他们可以利用这些数据来改进产品和服务，但这也引发了重大的数据隐私问题。学者 Jen Caltrider、Misha Rykov 和 Zoë MacDonald 在一项研究中审查了 25 个汽车品牌，并针对这些公司收集和使用数据和个人信息的方式给出了 25 个“批评”，并表示其审查的每个汽车品牌都收集了超出必要范围的个人数据，并且将这些信息用于除操作车辆和管理与车主关系之外的其他目的。[8]网联汽车的连接性是数据收集的一个关键因素。联网汽车能够收集有关车主的位置、交通状况，甚至车主如何与信息娱乐系统互动的实时数据。此外，如果车主选择将汽车与制造商的应用程序同步，其隐私又会有被再次侵犯的的隐患。这些看似无害的应用程序会悄悄收集车主的一举一动的数据——包括使用模式、确切行踪以及独特偏好——所有这些数据都将被整齐地打包并交给汽车制造商。当前，网联汽车包括但不限于收集有关车主的下列信息：位置数据、语音录音、财物数据、个人资料、人照片和图像、日历和活动、航线历史、就业信息等。

根据欧盟 GDPR 的规定，公司只有在数据主体同意的情况下，才可以在特定条件下收集和处理个人数据。通知和同意(选择)是公平信息实践原则下的关键原则，是许多隐私法和框架的基础。在传统环境中，例如在网站和移动应用程序上，可以通过隐私通知、弹出消息、按钮和复选框提供和获得通知和同意。但是，当车辆可能以用户可能不知情的方式持续收集信息时，提供通知和获得同意可能会很困难或难以操作。我国《个人信息保护法》第十三条第一款、《汽车数据安全管理若干规定》第八条规定，只有在数据主体取得同意的情形下，才可以收集用户的个人信息。但是在实践中，汽车隐晦地操纵客户同意的方式。一些汽车公司经常会忽略车主的同意。有时，他们会假定车主已经同意。汽车公司这样做的原因是，在车主踏入汽车之前，他们假设车主已经阅读并同意了他们的政策。斯巴鲁的隐私政策规定，即使是使用联网服务的汽车的乘客，只要坐在车内，也“同意”允许他们使用，甚至出售用户的个人信息。因此，当汽车公司说他们得到了用户的“同意”或不会在“未经你同意”的情况下做某事时，这通常并不意味着他们会这么做。特斯拉给了用户选择退出数据收集的选项，但这可能会限制汽车的某些功能：“如果您不再希望我们收集车辆数据或 Tesla 车辆的任何其他数据，请联系我们以停用连接。请注意，某些高级功能(例如无线更新、远程服务、与移动应用程序的交互以及位置搜索、互联网广播、语音命令和 Web 浏览器功能等车载功能)依赖于此类连接。如果您选择退出车辆数据收集(车载数据共享偏好设置除外)，我们将无法实时了解或通知您有关您车辆的问题。这可能会导致您的车辆功能下降、严重损坏或无法操作。”选择退出的选项应该是透明的，绝不能被用作操纵消费者的工具。这同样也造成了一种现象，即客户对于商业主体以及第三方收集了多少数据以及如何使用这些数据失去了主导权。

## 4. 网联汽车中个人信息保护的对策讨论

网联汽车领域的个人信息保护是一个极为复杂的问题，除了需要系统完善的法律规范加以规制以外，还需要各方主体的配合与协调。对于这一问题需要公权力机关、商业主体以及私人主体的多元参与才能

[8]https://foundation.mozilla.org/en/privacynotincluded/articles/its-official-cars-are-the-worst-product-category-we-have-ever-reviewed-for-privacy/, 2023-10-06, 2025-05-17.

促进网联汽车个人信息保护的健康发展。

**(一) 强化用户权利实现，提升用户隐私意识**

强化用户隐私保护行为的前提是帮助增强用户维权能力。建立专门的用户隐私保护咨询平台，为用户提供专业的隐私保护咨询和维权指导。线上搭建集成化数字平台，设置智能检索系统与 24 小时 AI 咨询机器人，用户输入关键词，就能快速获取《个人信息保护法》条款解读、常见侵权场景识别指南等基础资料。平台还可智能优化，依据用户搜索习惯推送相关内容，像不同行业隐私侵权的典型案例分析，详细剖析电商、社交软件等场景中可能出现的信息泄露方式，让用户更直观地了解侵权风险。同时提供维权流程说明，从收集证据的具体方法，如保存聊天记录、截图授权页面等，到向平台投诉、向监管部门举报的具体步骤都一一阐述，帮助用户清晰知晓维权路径。线下在社区、商圈设立实体咨询点，安排持法律职业资格证的专业顾问驻点。这些顾问可为老年群体或网络使用障碍者提供一对一纸质资料解读服务，用通俗易懂的语言讲解隐私保护知识和维权要点。此外，还能提供法律援助指引，告知用户在复杂侵权案件中如何寻找合适的律师，以及申请法律援助的条件和途径等，让用户在遇到隐私问题时，能及时、有效地维护自身权益。

**(二) 促进不同法律规范之间的协调、加强权力机关的监督义务**

中国已成为网联汽车的领先国家之一，并拥有全球第一大网联汽车市场。随着近年来数字化的不断发展进步，中国政府自 2003 年以来一直致力于规范数字化过程中的个人信息保护，并颁布了多部相关法规，形成了初步的法规体系。当前，《网络安全法》《数据安全法》《民法典》和《个人信息保护法》为中国的网络安全、数据治理和个人信息保护奠定了法律基础[36]。但是有一套法规基础并不能保证遵守所有法律。此外，每项法律都包含许多条款，这些条款可能适用于某一情况，但不适用于另一情况，并且所有法规都可能发生变化。这种复杂程度使得一致且适当地实施合规性变得困难。不管是通过哪个单一的路径都无法为个人信息的保护提供最周全的保护，因此，促进不同法规规范之间的协调，提高法规规范保护个人信息的有效性。

政府监管部门在个人信息保护的监管中应发挥其关键的作用，加强对商业主体的监督。例如，欧洲数据保护委员会和加州隐私保护局等各种监管机构都关注客户隐私。因此，为了解决这些问题，这些部门正在考虑对平台捕获的数据进行监管。例如，欧盟通过的《通用数据保护条例》(GDPR)法案(2018 年)旨在规范各公司对欧洲公民数据的收集和使用(GDPR, 2023 年)。2018 年，加州立法机构通过了《加州消费者隐私法案》(CCPA)，以保护加州任何企业收集的居民数据(加州司法部，2023 年)，该法案还规范了公司对加州居民数据的使用。此外，网联汽车领域的个人信息保护需要不同的部门相互配合，加强不同部门之间的协调，明确各部门的职责义务，以便形成高效的多部门综合治理的治理体系。

**(三) 提高商业主体的行业标准，规范其商业行为**

由于数据保护是一个复杂的问题，涉及多方主体的参与与协调，尤其是企业对于收集的客户信息具有一定的控制权，对于企业来说，需要更加严格的要求以规范其行为。首先，面对大量的数据泄露现状，公司应当承担更高的保护义务，采取各种额外措施来确保数据保护(防止数据被盗)。例如，一项重要措施是对员工进行个人数据处理培训。毕竟，导致数据泄露的往往是人为错误。此外，如果发生数据泄露，必须在 72 小时内向主管监督机构报告。如果这些泄露行为可能对其权利和自由造成高风险，还必须告知数据主体。其次，对收集的设计用户隐私的个人信息应当进行匿名化处理；匿名化( anonymization)，是指通过对个人信息的技术处理，使得个人信息主体无法被识别或者关联，且处理后的信息不能被复原的过程。在《个人信息安全规范》规定的需要匿名化和去标识化的一些具体应用场景时，应当主动对信息进行处理。网联驾驶汽车的数据可以进行匿名化处理，但应采取措施确保数据无法被重新识别，同时考虑到技术发展和监管指导。再次，公司应当“从一开始就将用户个人信息保护安全措施融入设备中，而不

是事后再考虑，并尽可能做到：1) 进行隐私或安全风险评估；2) 尽量减少收集和保留的数据；3) 在推出产品之前测试安全措施。最后，作为公司，必须采取适当的技术和组织措施来确保个人数据的安全。当汽车公司在与有权访问个人信息的第三方供应商合作时，必须与第三方签订隐私协议。与第三方所签订的隐私协议是一项旨在加强消费者数据保护的措施，在签订协议时应当综合考量各方因素，对数据主体的权利、义务等加以明确。在涉及到关于姓名、地址、电子邮件联系信息、电话号码、账户/信用卡信息、出生日期、IP 地址、物理特性等非常敏感的个人数据。在处理这些信息时，必须始终小心谨慎，以确定外部访问是否对于执行某项活动是绝对必要的。

## 5. 总结

个人信息保护是任何收据数据行业中都存在的一个热门问题，在网联汽车领域中也不例外。在网联汽车快速发展的今天，为我们提供便捷智能化的驾驶体验以外，也对个人信息保护带来了前所未有的挑战。面对庞杂的网联汽车所收集的个人信息、隐私信息以及第三方主体的滥用和攻击等现实挑战，网联汽车中的个人信息保护安全问题亟待解决，想要应对这些现实的问题，需要各参与方积极协调配合，从政府机关和商业主体两个层面入手，以推动网联汽车领域个人信息的保护，实现个人利益、国家利益、商业利益三方平衡，只有用户积极行动、企业主动担责、监管严格到位，三方协同配合，才能真正提升智能网联汽车下个人隐私保护水平，让《个人信息保护法》得到有效落实，切实守护好用户的个人信息安全。

## 参考文献


[1] 张玥, 朱庆华. 国外信息隐私研究述评[J]. 图书情报工作, 2014, 58(13): 140-148.

[2] 张大伟, 谢兴政. 隐私顾虑与隐私倦怠的二元互动: 数字原住民隐私保护意向实证研究[J]. 情报理论与实践, 2021, 44(7): 101-110.

[3] 贾若男, 王晰巍, 范晓春. 社交网络用户个人信息安全隐私保护行为影响因素研究[J]. 现代情报, 2021, 41(9): 105-114+143.

[4] 曹明增, 张磊, 李晶. 基于位置服务中的位置隐私保护技术综述[J]. 计算机技术与发展, 2024, 34(6): 1-9.

[5] 程啸. 论大数据时代的个人数据权利[J]. 中国社会科学, 2018(3): 102-122+207-208.

[6] 欧阳洋, 袁勤俭. 电子商务中消费者隐私关注对行为意向的影响研究[J]. 情报科学, 2016, 34(5): 75-80.

[7] 曹达. 我国社交媒体隐私政策文本与个人信息保护水平研究[D]: [硕士学位论文]. 北京: 中国政法大学, 2019.

[8] 李青, 苏明雪, 聂含韵. 教育类 App 隐私保护评价指标构建和保护现状研究[J]. 中国远程教育, 2022(9): 69-77.

[9] 王娜, 杨宇婷, 张灿灿, 等. 运动健康类 App 用户隐私政策规避行为形成机理研究[J]. 数字图书馆论坛, 2023, 19(12): 1-10.

[10] 刘璐. 电商平台用户隐私保护策略与路径设计研究——基于国内主流电商平台隐私条款的分析[J]. 企业经济, 2025, 44(4): 89-97.

[11] 雷丽彩, 郭芷欣. 基于政府监管的社交媒体用户隐私保护演化博弈分析[J]. 数字图书馆论坛, 2024, 20(8): 39-50.

[12] 余成峰. 平台媒介的兴起: 隐私保护的范式与悖论[J]. 东方法学, 2024(5): 74-87.

[13] 李畅畅. APP 个人信息保护政策困境与应对路径[J]. 信息安全研究, 2024, 10(2): 177-183.

[14] Schwartz, P.M. and Peifer, K.N. (2017) Transatlantic Data Privacy Law. *Georgetown Law Journal*, **106**, 115-179.

[15] Acquisti, A. and Grossklags, J. (2005) Privacy and Rationality in Individual Decision Making. *IEEE Security and Privacy Magazine*, **3**, 26-33. https://doi.org/10.1109/msp.2005.22

[16] Ben-Shahar, O. and Schneider, C.E. (2017) The Failure of Mandated Disclosure. *Russian Journal of Economics and Law*, **4**, 146-169.

[17] Cranor, L.F. (2012) Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice. *Journal on Telecommunications and High Technology Law*, **10**, 273.

[18] Solove, D.J. (2012) Introduction: Privacy Self-Management and the Consent Dilemma. *Harvard Law Review*, **126**, 1880-1903.

[19] Tschider, C.A. (2020) Beyond the "Black Box". *Denver Law Review*, **98**, 683.

[20] Litman-Navarro, K. (2019) We Read 150 Privacy Policies. They Were an Incomprehensible Disaster. *The New York Times*.

[21] Norberg, P.A., Horne, D.R. and Horne, D.A. (2007) The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *Journal of Consumer Affairs*, **41**, 100-126. https://doi.org/10.1111/j.1745-6606.2006.00070.x

[22] Auxier, B., Rainie, L., Anderson, M., *et al*. (2019) Americans and Privacy: Concerned, Confused and Feeling Lack of Control over Their Personal Information.

[23] Waldman, A.E. (2020) Cognitive Biases, Dark Patterns, and the 'Privacy Paradox'. *Current Opinion in Psychology*, **31**, 105-109. https://doi.org/10.1016/j.copsyc.2019.08.025

[24] Chen, L., Huang, Y., Ouyang, S., *et al*. (2021) The Data Privacy Paradox and Digital Demand. National Bureau of Economic Research.

[25] Jones, M.L. and Kaminski, M.E. (2020) An American's Guide to the GDPR. *General Data Protection Regulation*, **98**, 93.

[26] Waldman, A.E. (2022) Privacy, Practice, and Performance. *California Law Review*, **110**, 1221.

[27] Waldman, A.E. (2019) Privacy Law's False Promise. *Washington University Law Review*, **97**, 773.

[28] Schwartz, P.M. (2008) Reviving Telecommunications Surveillance Law. *The University of Chicago Law Review*, **75**, 287-315.

[29] Bradley, C.G. (2022) Privacy Theater in the Bankruptcy Courts. *Hastings Law Journal*, **74**, 607.

[30] Bamberger, K.A. and Mulligan, D.K. (2015) Privacy on the Ground: Driving Corporate Behavior in the United States and Europe. MIT Press.

[31] Waldman, A.E. (2018) Privacy's Law of Design. *University of California*, *Irvine Law Review*, **9**, 1239.

[32] Solove, D.J. and Schwartz, P.M. (2021) ALI Data Privacy: Overview and Black Letter Text. *University of California*, *Irvine Law Review*, **68**, 1252.

[33] Solove, D.J. and Hartzog, W. (2014) The FTC and the New Common Law of Privacy. *Columbia Law Review*, **114**, 583-676.

[34] Cui, S. and Qi, P. (2021) The Legal Construction of Personal Information Protection and Privacy under the Chinese Civil Code. *Computer Law & Security Review*, **41**, Article 105560. https://doi.org/10.1016/j.clsr.2021.105560