

“为了防止疲劳驾驶,我车里有一个专门的摄像头对面部进行拍摄,包括车辆自带的行车记录仪信息、行驶轨迹和位置信息,都能通过绑定在手机里的APP查看,不过,我一直担心万一信息泄露了怎么办?”近日,某车主反映,最近一段时间自己收到了不少房地产推销信息,而此前她只在自己新买的智能汽车上搜索过某地的楼盘价格,她怀疑可能是智能汽车“出卖”了她。

随着智能网联汽车的渗透率不断提高,辅助驾驶、远程泊车、语音交互等智能化功能在带给用户全新驾乘体验的同时,也产生了海量的信息,这些信息容易被相关企业在后台收集、共享和使用,对用户的个人隐私带来一定风险,造成数据安全问题。

消费者缺乏“安全感”

为了了解中国消费者对当前智能网联汽车数据安全和个人隐私数据的关注程度以及顾虑所在,日前J.D.Power(君迪)与《环球时报》联合发起了的“2022中国消费者智能网联汽车数据安全和个人隐私意识与顾虑调查”。

调查结果显示,中国消费者对现阶段智能汽车厂商能否妥善保护个人敏感信息的整体信心不足。其中,仅有约三成受访者表示比较有信心或极其有信心,超过四成表示完全没信心或信心不太足。

而且,用户还高度介意个人敏感信息被车辆手机、使用和共享,数据显示,非常介意或比较介意的受访者比例高达77.4%,只有2.5%的受访者完全不介意。

那么,到底是哪些原因导致消费者对智能汽车数据安全问题信心不足,缺乏“安全感”?

首先,相比智能手机,用户对智能汽车收集个人信息的知晓程度更低。“一直都知道”个人敏感信息被收集的智能汽车用户(21.8%)明显低于智能手机用户(31.2%),而很少知道或完全不知道的智能汽车用户(22.2%)明显高于智能手机用户(16.7%)。

值得注意的是,近半数的受访车主表示从未收到过汽车品牌或经销商对个人信息收集的提示。这表明,很多的数据收集行为是在用户“不知情”的情

数据使用与隐私保护“边界”难定

“用车的过程中,能感觉到车辆在收集我的信息。比如,我在行驶的途中,发现车没电了,通过一键搜索后,汽车会提示我附近哪里有充电桩,哪有换电站。其实这已经在使用我的位置信息了,毕竟智能化的推荐肯定是建立在知晓车辆实际状况的前提下。但我允许这种类型的信息采集,因为这可以及时提供给我需要的资讯。”某新势力品牌车主说。

部分有着类似情形的车主们也会困惑,车辆采集的信息是否都用于了改善车辆使用体验方面。事实上,数据使用与隐私保护的“边界”一直以来也是智能汽车数据安全讨论中的关键。

在上述J.D.Power的调查中,当被问及“在什么情况下你可能愿意考虑共享个人敏感信息”时,大部分用户选择了与行车安全和路线规划相关的场景。其中排名前五的场景为:为了及时获得碰撞提醒和紧急救援,保证行车安全(73.7%);为了避开拥堵道路,精准规划行车路线(53.5%);为了查明车辆故障(41.7%);为了调查事故原因(38.1%);为了查询附近商



汽车数据如何上好「安全锁」?



中国互联网协会发布的《中国互联网发展报告(2021)》显示,2020年,我国智能网联汽车销量为303.2万辆,同比增长107%,渗透率保持在15%左右。对于正处于技术快速演进、产业加速布局阶段的智能网联汽车行业而言,数据安全和隐私泄露已成为发展中必须正视的议题。

事实上,去年以来,《关于加强智能网联汽车生产企业及产品准入管理的意见》《汽车数据安全管理办法(试行)》《个人信息保护法》等相继出台,从政策法规层面对汽车产业的数据使用提出了更为明确的规范和要求,为有序开展汽车领域重要数据和个人信息保护工作指明了方向。

“综合来看,目前我国已经初步形成包括个人信息保护、网络信息安全、数据安全等级别逐步升高、覆盖各个领域的法律法规。其实这里面很多都是来自于实践,也就是说我们在实践中发现了各种各样的问题,然后逐步形成了新的规范。”对外经济贸易大学信息学院副院长华迎



车企安全能力有待提升

车联网发展仍在加速,但业内人士普遍认为,目前车联网安全整体水平仍处于“爬坡提升”阶段。北信源副总裁高曦表示,车联网安全形势不能用乐观来形容,“目前公众关注的安全事件大部分局限在自动驾驶安全上,这类事件虽然更容易引发媒体和公众的关注和探讨,但驾驶安全仅是总体安全的一部分,用户在汽车全生命周期中会产生大量各种各样的数据,就车联网而言,数据安全层面需要引起重视。”

目前,整车厂商的安全能力仍然滞后。一位信息安全行业人士评价,目前市面上大

部分车型在信息安全防护方面水平偏低,车内相关联网部件及控制部件防护可靠性不高,且缺失一定的安全策略,这可能会导致车内敏感信息的泄露或被篡改、车辆行驶中的异常行为,甚至有可能危及人的生命安全。

“当前,车联网安全市场呈现碎片化、界线强等特点,数据难以打通。”上述人士表示,传统互联网安全已经无法应对车联网安全风险,亟需一种包括安全咨询、产品设计、安全开发、安全测试、运营监管等在内的一体化、可持续、闭环生态式的安全保障体系。亚信安全日前发布的《2022

年网络安全发展趋势及十大威胁预测》显示,汽车制造厂商更需要“安全伙伴”。车联网数据在进行采集、传输、存储、使用、迁移、销毁等全生命周期阶段均存在不同性质的安全风险,充分、全面且深入的风险分析是做好风险应对和安全防护的关键。

高曦也认为,车联网上下游企业安全技术参差不齐,部分整车厂商对车联网安全的重要性认识也有待提高。“对车企而言,安全能力是很难‘一下子就上手’的,因为信息安全能力需要相当长时间的经验和沉淀,尤其要动态研究最新的安全威胁并有能力给出解决方案,当然也需要相当大的成本投入。如果不是从底层安全架构、从车联网平台自身安全开始架构和规划,仅采用‘打补丁’的方式解决安全问题并不可取。”

“这就类似说我的产品做好了,然后请你来搭安全防护,在我的产品周边‘搭篱笆’。”高曦说,“如果系统底层做好了就根本不需要这么多‘篱笆’。”只有通讯、存储、认证三大核心安全的“底座”完备了,才能真正具备系统级的安全能力,“车企没有一个系统级的安全‘底座’,可能导致安全架构后期越来越乱,面临新的安全威胁时,头痛医头、脚痛医脚,就像蜘蛛网一样,稳定性也比较差。”最终影响到车企品牌形象、用户体验和社会安全。

对此,奇安信车联网安全专家孔宪梓也表示,从车联网的历史漏洞来看,不难发

现大多数车联网漏洞本质是多个传统漏洞在车联网框架中的组合利用,“所以保护车联网安全更重要的是将安全基础打牢,避免出现短板漏洞。”

专家建议,应该推动健全合理的漏洞发现、处置与管理机制,加快行业标准制定出台。同时,应建立安全监管责任体系,并将安全责任落实到上线前、运营使用中和事后等生命周期的各个环节。预计未来三年将是国内相关监管法规的集中发布期。

此外,孔宪梓认为,车联网安全水平的提高,一方面需要厂商加强信息安全团队的建设,提升核心基础技术的安全可控能力;另一方面,厂商需要对车联网漏洞持开放与包容态度,发挥广大“白帽子”的力量。此前,一些“白帽子黑客”怕惹事上身,即使发现车联网漏洞也往往不敢报送,未来可以把传统领域已经应用实践效果较好的安全监测预警、应急响应机制,移植到车联网领域中,并且结合车联网环境的特点,更有针对性地做好安全防护与监测。

专家认为,汽车制造厂商需要第三方企业作为“安全伙伴”,更需要将系统和平台安全“底座”打牢。汽车产业链应从产品设计之初就将网络安全考虑纳入产品需求中,形成一体化、可持续、闭环生态式的安全保障体系,并贯穿产品的全生命周期,未来这一领域市场机会将逐渐显现。

多方合力构筑安全“屏障”

说。

不过在国家工业信息安全发展研究中心副总工程师兼信息政策所所长黄鹏看来,尽管政府在推进产业发展和保障数据安全方面无疑具有关键地位,但法规体系、标准体系仍存在多头监管的问题,还需尽快细化一些行业性的管理要求。“从数据安全监管的角度,国家网信部门是牵头部门,但是涉及到具体行业细则的出台,还需要行业主管部门,以及一些重要的行业协会去推动相关工作。”黄鹏认为。

同时,业内一致认为,车企也应从自身层面担当起保护用户数据安全的一道“屏障”。“我们认为,未来除了智能汽车领域技术的竞争,更重要的一环就是不滥用用户信息,让企业品牌的口碑在用户中得到广泛传播,让消费者认为这是一个靠谱的品牌。所以不管是参照以前的互联网行业,还是手机行业,如果智能汽车的数据安全做得好,我相信品牌就会获得更好的口碑和销量,未来肯定会成为一个竞争优势。”J.D.Power中国

区汽车产品数字化用户体验总监裴林说。

蔡硕则建议,未来对数据安全的监管,既应囊括汽车的安全防火本身,也要监管车联网网络安全,同时还要监管车联网服务平台的安全,从三个维度分级分类安全保护的管理。

“车主应该有四方面的权利,第

一是个人信息的自主权;第二,作为消费者应该有拒绝权;第三,作为被遗忘权,当车主和所使用的车辆‘分手’的时候,数据应该是被遗忘而不是留存;第四有救济请求权,当数据处理有异议的时候,司法机构应该向车主敞开救济的途径。”蔡硕说。

(本文综合央广网、每日经济新闻、车云网、中国水运网等相关报道)

