

智能“黑科技” “黑”你不客气

随着智能家居概念的普及，以往只有在公共场所才能看到的智能摄像头，开始进入普通家庭，使人们对家居实时远程监控变为可能，给人们的日常生活、工作带来了极大的便利，然而，由此产生的隐私泄露等安全风险如影相随。

■本报记者 张晓鸣

通过智能镜子对身体健康进行评估，提供合理的装扮建议；通过云数据同步，喷淋系统可根据室温及用户身体状况自动调节水温；以及包括可监测排泄物成分的智能马桶、可显示体重和体脂含量的地砖等具体场景……善于造梦的科学家，正在构想出一系列未来人类将在浴室内可体验到的智能化家居装备。

再比如，在家里安装上智能摄像头，年轻的父母可以随时查看孩子的生活学习状况；上班的女性能随时观察家中老人的情形，防止意外发生；离家在外时还能够实时监控房屋财产安全状况，记录下不法人员的体态样貌，甚至还能远程报警……

不过，在看到 WannaCry 电脑病毒闹得人心惶惶的时候，你还敢放心大胆使用这些智能家居吗？

“引狼入室”的摄像头

近日，南京市鼓楼警方就接到一位市民的报警求助。

报警者吴女士称，为了拍摄家中宠物的日常动态，她在客厅、餐厅等区域安装了监控探头，画面可以实时传输到自己的手机上。可最近，吴女士偶然在某萌宠网站上，居然看到了自家宠物的视频，“我肯定没有上传过任何影像资料到这家网站，也没有发给朋友看过，视频怎么会流到网上去呢？”

据警方初步推断，吴女士的摄像头是 24 小时联网状态，而且品牌比较小众，防小偷做得并不牢靠，可能在中了木马病毒后，相关视频被不法之徒截获后上传，然后被不明真相的网站发布。

吴女士的尴尬遭遇，只是智能家居产品隐私泄露的冰山一角。360 攻防实验室发布的《国内智能家庭摄像头安全状况评估报告》就表示，近八成智能摄像头产品存在用户信息泄露、数据传输未加密等问题，黑客可以远程获取用户实时监控画面。

本是为了家人、家宅安全而安装的摄像头，如今在安全上却是漏洞百出。据安全专家介绍，该实验室去年曾经对国内市场上销售的近百个品牌的家庭智能摄像头进行安全评估测试，发现有近八成产品存在用户信息泄露、数据传输未加密、App 未安全加固、代码逻辑存在缺陷、硬件存在调试接口、可横向控制等安全缺陷。这些安全缺陷的存在，让接入网络的智能摄像头，可以轻易被不法分子所控制，随时获取摄像头拍摄的图像和语音信息，对安装摄像头

的家庭或公司进行监控甚至网上直播，从以往披露的拍摄内容看，其中很多连家庭住址、户主姓名等隐私信息都一览无余。

国家信息中心专家委员会主任宁家骏认为，智能摄像头是一种普及率颇高而且发展很快的家庭智能设备。据不完全统计，目前在国内上市销售的智能摄像头品牌多达 107 个，保守估计中国市场年销量超过 400 万台。然而，由于设计生产的相关企业繁杂，目前国内市场上销售的智能摄像头鱼龙混杂，不仅品牌多，而且无品牌的山寨产品更是不计其数，其中很多产品缺乏完善的安全设计，更没有进行过系统的安全风险评估。利用这些设备的安全漏洞，黑客不仅可以接管这些设备的控制权而为所欲为，还可以窃取用户个人信息和个人数据，其危害不容小觑。

专家就智能摄像头的购买和使用给出了安全建议：首先，在购买的时候

能家居在给我们日常生活带来方便的同时，新的安全问题也是如影随形。

目前来看，智能家居产品最大、最直接的安全问题，是更大范围的个人信息收集及隐私泄露风险，不管是善意还是恶意。以目前国外已相当普及的智能电表为例，生厂商可以通过分析家庭的用电情况了解用户家中配置了何种电器、一家人的作息习惯，如果电表和智能冰箱联网，甚至还能看到这家人何时打开电冰箱，还有多少食物等极度私密的信息……而这一切，仅仅是一款智能电表带出的隐私信息而已。

此前，国内有媒体曾爆出 LG、三星智能电视收集用户信息的问题。据相关媒体的报道，有部分细心的 LG 智能电视操作系统 Web OS 用户反映，他们即便不换台、不使用互联网应用，LG 电视依然会向后台发送数据包，由此怀疑 LG 违规收集用户个人信息。用户对此投诉后 LG 表示，之所以启动这一功

目前在国内上市销售的智能摄像头品牌就多达 107 个，市场上销售的无品牌的山寨产品更是不计其数，然而由于参与智能摄像头设计生产和推广的相关企业繁杂，品牌众多，其中的很多产品都缺乏完善的安全相关设计，很容易被黑客控制。

360 攻防实验室发布的智能家庭摄像头安全状况评估报告显示，该企业在对国内市场上销售的近百个品牌的家庭智能摄像头进行的安全评估测试发现，近八成产品存在用户信息泄露、数据传输未加密、App 未安全加固、代码逻辑存在缺陷、硬件存在调试接口、可横向控制等安全漏洞。安全专家介绍，这些安全缺陷的存在，让接入网络的智能摄像头可以轻易被不法分子控制，随时获取摄像头的图像和语音信息，对安装摄像头的家庭或公司进行监控、甚至网上直播。

要对所选品牌的摄像头进行一些调查，看看网上能不能搜索到相关品牌设备漏洞一类的问题，用户口碑如何。其次，要选择有一点品牌知名度、价格合适（太便宜请慎入）的摄像头。开始使用之前，第一步要做的就是设置一定强度的密码，平时要及时关注智能家庭摄像头软件的提醒，如果发现请求验证码的短信，就需要立刻修改密码。与此同时，用户还应该经常登录摄像头进行查看，如发现角度不对等情况，就需要注意自己的账号安全了。此外，还要注意网络安全咨询，关注智能家庭摄像头安全方面的消息，如果有报道称设备出现漏洞，就需要等待厂家更新，要保证所使用的摄像头是最新版本……

智能家居产品 “请神容易送神难”

不仅仅是摄像头存在安全隐患，智

能，是为了向其他 LG 智能电视用户提供收看建议。公司从来都不会存储用户个人数据，未来将开发一种新的固件更新，以确保数据收集设置完全由用户控制。

LG 风波刚刚平息，三星智能电视又被用户投诉。媒体报道称，三星智能电视配置的语音识别功能，能够在未经用户许可的情况下捕捉用户的会话，还会将其传输给第三方。

三星智能电视最大的卖点之一便是其语音识别功能。“可以捕捉到语音命令，并将其转换成文字命令”，这对于那些厌倦使用遥控器的人来说，是极具诱惑力的。不过，在三星提供的隐私条款上，却明确标注着“请注意，智能语音识别系统能够捕捉到您的语音，个人信息以及其他一些敏感信息也会随着捕捉到的数据一同传输到第三方”。对此，三星方面称，“三星很注重用户的个人隐私。三星智能电视采用行业标准的信息维护准则，

其中就包括数据加密。这一措施能确保用户的个人信息不被泄露，不会在未经授权的情况下被收集或使用”。

事实上，不仅仅是智能电视，我们身边所有接入互联网、配置语音操控功能的智能家电设备，都存在隐私泄露的可能。比如，Xbox 游戏机、互联网电视盒，甚至是智能恒温器，都存在数据收集带来的安全风险。考虑到这些设备的平台都十分容易被黑客攻破，这些用户数据显然不仅仅是被用于分析数据、进行营销那么简单，更有可能被传播或贩卖至商业公司。

如果说智能家居设备生产商按惯例读取信息、用户尚能承受的话，那么黑客通过网络入侵终端 App，借助智能家居产品获得家中控制权，则已经不仅仅是电影中的恐怖场景，而是活生生的现实……通过盗取用户智能家居 App 的账号和密码，登录用户家的网关，黑客可轻松“接管”整个智

能家居系统，实现门窗、电视、空调、灯具等各种设备的开关，换句话说，你的远程控制权已移交至黑客的手中。更让人防不胜防的是，黑客通过窃取的用户隐私数据，可轻松获得用户的家庭住址，并通过智能家居 App 打开用户家的智能锁……对比之下，之前用户的智能摄像头被黑，只能说是小菜一碟。

即使没有被黑客盯住，病毒也是一个大麻烦。现阶段，智能能源管理、远程门锁、室内监控等智能家居设备大部分采用蓝牙无线连接，通过智能手机、平板电脑和网页来实现操作。一旦智能家居 App 被病毒感染，由此带来的麻烦，也够你喝一壶的。

先学会走路 再想着怎么“飞起来”

从市场发展趋势来看，智能家居很有希望成为下一个大“风口”。

如果对智能家居产业链进行梳理，可以发现智能家居是一个整合性的行业，参与方众多。有提供软硬件技术支持的厂家，比如谷歌、百度、阿里等；有智能家居产品厂商，有家电企业、照明安防企业等；有平台企业，如苹果、华为、阿里、京东、微软、亚马逊等巨头。此外还有提供整体智能家居解决方案的集成商等。

这些企业及其在智能家居领域的探索，构成了智能家居近千亿级的市场。有数据显示，我国智能家居市场规模 2015 年为 431 亿元，同比增长 41.80%，2016 年为 660 亿元，同比增长 53.10%，2017 年预计为 988 亿元，同比增长 49.60%。到 2020 年，全球智能家居产业规模将达到 620 亿美元，届时我国智能家居市场规模将达到 1396 亿元。无论从规模上还是增长速度上，我国的智能家居市场的发展都在全球市场保持领先地位。

所有人都在等待智能家居这一“风口”到来，但如果对智能家居产品存在的安全隐患没有足够的防范意识，智能家居产品的普及，可能会带来一场灾难。“便利”向来是把双刃剑，在互联网以及正在快速普及的物联网上，你传输的数据越多，信息暴露的可能性就越大，存在的安全隐患也因此而剧增。以目前的技术，对于物联网设备，可以采取的安全措施大概可以分为四类。一是前端，即用户的设备端，通过增加设备本身的可靠性来降低风险，比如提高生物识别模块的准确度；二是网络，即防范数据传输过程中可能出现的安全风险；三是系统和数据库，即防范操作系统、通用应用平台系统方面存在的风险以及威胁到信息数据库的安全风险；四是应用、管理、终端，即防范实现业务应用自身及应用交互过程中的安全风险，防范网络和系统管理不善产生的风险，防范控制终端及其操作系统面临的风险。

不过，放眼整个智能家居行业，很少有企业能在上述四个环节都做到万无一失，毕竟这其中涉及的领域太广泛了。比较靠谱的解决方案是企业间的合作，而这又涉及到众多纠缠不清、一言难尽的利益关系……这一行业当中一些最基本的环节，恰恰是最不堪一击的，比如统一的安全标准、用户个人数据的所有权归属、用户隐私保护政策、一旦隐私泄露责任归谁，诸如此类，都有待行业巨头配合管理机构一一落实。

在互联网时代，智能家居是大势所趋。不过，想借“风口”起飞之前，还是请先把路走稳。

数据的成本大约是 200 美元。目前，东航和南航虽然标明空中 WiFi 的价格在 258 元，但是只要提前申请，获得体验名额后即可免费使用，国航、海航的空中 WiFi 目前不收费。现实情况是：国内的空中 WiFi 服务并没有为航空公司带来多少看得见的直接收益，它只是客舱服务的一项增值业务，但就为这个小小的“噱头”，航空公司必须为高额的数据传输费买单。

免费很难撑起空中 WiFi 的未来，商业化才是未来趋势。国际上，虽然也有航空公司免费提供空中上网服务，但是大多数航空公司都收取服务费。各国航空公司空中 WiFi 收费模式主要有按航段、流量、使用时间、设备数量和-content 点播以及 24 小时共享模式收费，也有包年和包月的计费方式。业内人士表示，为了覆盖成本，空中 WiFi 不可能一直免费，但如果参考外国航企的收费情况，则价格偏高，国内乘客、尤其是非商务旅客恐怕难以接受。

从我国家航空旅客运送的体量来看，空中 WiFi 的市场预期是一片蓝海。2016 年我国旅客吞吐量高达 10.16 亿人次，如果按照 70% 愿意付费计算，也有 7 亿人次使用。在目前空中数据流量单价不低的情况下，一位长期研究空中 WiFi 的业内人士认为，这个市场达到百亿元级还是可能的。

空中 WiFi 带来的衍生商业模式——空中购物有可能是乘客的一个消费兴奋点，因为空中 WiFi 逐渐普及后，空中购物网络产业生态也会迅速成熟，空中购物这一新消费模式有望成为时尚潮流。

风向

共享出行商机

电动汽车 要分一杯羹

■佳康

尽管遭到各种质疑，但谁也无法阻挡“共享经济”的扩张步伐。上周，摩拜单车宣布完成 6 亿美元 E 轮融资，创下共享单车行业诞生以来的单笔股权融资最高纪录，再度印证资本市场对共享出行模式的狂热追捧。

值得关注的是，这股本钱追捧潮，也迅速蔓延至电动汽车共享出行领域。业内人士表示，随着共享单车被更多用户接受，资本市场开始关注并着手布局电动汽车分时租赁服务，产业链上的消费支付、停车充电等环节，即将引来一波投资热潮。

究其原因，一是电动汽车分时租赁等共享出行模式具有广阔的发展前景，如果说共享单车模式解决的是用户 3 公里之内的出行“痛点”，电动汽车分时租赁则解决用户 50 公里之内的出行问题，引发新的蓝海市场；二是电动汽车共享出行领域尚在发展初期，无论是充电桩布局，还是电动汽车投放经营均有巨大发展空间，谁能最早完成业务布局，就能分享产业发展最大红利。

总部位于深圳前海的云杉智慧新能源技术有限公司，大概是这一波“风口”的首位受益者。其近日透露，公司即将启动新一轮股权融资，融资额约在 10 亿元左右。资料显示，云杉智慧 2015 年成立于深圳前海，主营业务为打造融合充电网、车联网、互联网和停车位，提供大数据挖掘和以大数据为基础做增值服务的智能运营平台，为用户提供电动汽车分时租赁消费支付、停车充电、绿色出行等服务。截至目前，由该公司投资建设的充电网络已进入全国数十个城市，累计建设 5000 多个充电桩并投入运营，总功率超过 10000 千瓦；在新能源汽车运营方面，公司在上海、广州、深圳等地投放数千辆电动汽车提供分时租赁等共享出行服务。

资本之所以青睐电动汽车共享出行模式，不仅仅在于其广阔发展前景与政策扶持力度，更在于市场已经看到其盈利空间——在国内，部分电动车分时租赁平台通过引入大数据分析、区块链等技术优化管理效率，已经在一些城市实现业务盈利。比如云杉智慧新能源是广州最大的电动汽车分时租赁运营公司，在广州市的周均出租率从初期的 11% 提升至 25%，峰值达到 69%，单车租赁时长达到 9 小时，迈过了盈亏平衡点。如此，只需要这套先进管理模式在其他城市复制，便能带来规模扩张与利润增加的双丰收。

“不过，电动汽车共享出行产业发展看似广阔，实际操作层面面临的挑战依然不小。”多位业内人士指出，目前电动汽车分时租赁产业链面临的最大的运营瓶颈就是充电难。据了解，国内大部分已建成的充电桩的使用率相当低，有些设备平均利用率不足 5%。

而对那些跃跃欲试的电动汽车分时租赁运营平台而言，在打通充电难这一最大瓶颈之后，能否在提供电动汽车共享出行服务的同时，提供周边充电桩（站）位置、最优路线引导指示、路况信息、充电预约、充电情况等提示、让充电与支付结算变得更加方便快捷，是一个更大的考验。

在云杉智慧总经理徐征鹏的心目中，未来的电动汽车分时租赁平台，应该是一个整合了城市新能源出行各个场景的智能服务体系，其服务不仅仅只是电动汽车的租赁、充电，还可以将诸如网约车、物流配送、零售、在线社交等融合进来，形成一个全新的分享出行业态。在这一思路之下，云杉智慧近期发布了国内首个综合平台型充电服务场景品牌——易云社，让用户在享受充电服务的有限时间里，享受多元化消费服务。易云社将单一的充电桩升级为集充电、购物、休闲于一体的综合场站，并引入中小商家及新能源车企，打造一个以绿色环保为核心的全新盈利业态，为用户提供消费与支付服务、停车充电服务、绿色出行服务等多样化选择。未来甚至还会将充电服务完全链接到线上，在云端平台实现下单、上门服务、点评、社区等多个场景的“一键解决”方案。“我希望最终能将它打造综合的新能源汽车广场，成为城市新的标志性充电建筑物，不仅满足智能充电服务，同时提供如咖啡厅、便利店、电影院等生活服务。”徐征鹏表示。

本版插图：视觉中国

空中上网，真的成了一门大生意

预计国内空中 WiFi 市场规模将达百亿元

■张斌

根据中国民航网调查，在我国，超过 73% 旅客的旅游行为第一意愿就是上网，而当飞行时间超过 4 小时，这一意愿接近 100%；超过 70% 的旅客愿意付费享受空中 WiFi 服务，当飞行时间超过 4 小时，这一意愿更是高达 88.8%。

随着乘客对空中 WiFi 的需求量大大增加，各航空公司布局此项业务的步伐也在加快。4 月 12 日，我国首颗高通量通信卫星“实践十三号”成功发射，为航空公司的空中 WiFi 布局加速提供了良好助力。中国联通也加入到空中 WiFi 建设布局的版图中来。4 月下旬，联通旗下的全资子公司联通宽带在线与航美在线、海特凯融联合宣布组建“联通航美”公司，主要任务是为中国联通提供航空 WiFi 集成服务、产品开发、客户服务等。空中 WiFi 在我国起步虽晚，发展却非常快。2013 年，国航在国内首次实现全球卫星通信互联网航班飞行，在万米高空为旅客提供定制互联网服务。2014 年 4 月 16 日，国航在北京飞往成都的 CA4116 航班上实现了 ATG（地面基站）模式下的空地宽带无线通信上网。

加装热点 开销不是一笔小数目

提供空中 WiFi 服务，让枯燥的旅程变得有趣起来。这个想法很不错，但要普及空中 WiFi，在政策和技术上还有一段路要走。

通信资源稀缺是空中 WiFi 普及中需要面对的首要问题，这主要牵扯到卫星资源和大型通信基站资源。例如，南航和东航等航空公司需利用 KU 波段卫星

通信系统，为乘客提供空中 WiFi，覆盖面可达世界绝大部分区域，稳定性高，并且不受天气和地形限制。但是价格非常昂贵，波段资源非常稀缺。另一种是国航采用地面基站发送信号的通信方式，受

链接
海南航空 据介绍，海南航空目前具有空中 WiFi 功能的航班并不多，机型主要是波音 737-800 客机。
东方航空 为上海到纽约、旧金山、洛杉矶、芝加哥、多伦多和温哥华的所有航班

到云层和基站切换的因素影响较大，信号不稳定。

此外，航电系统的改造是空中 WiFi 的技术瓶颈。目前已有的客机，在出厂时都没有加载空中 WiFi 系统，航空公司要拓展空中 WiFi 业务，就需要对现有飞机进行改造。改造项目包括在机身顶部加装卫星接收天线，飞机内部还要安装相应的控制器、文件服务器以及多部无线网络热点设备。我国法律规定，搭乘民航客机需要关闭手机，就是因为存在手机信号干扰航班航电系统的危险，空中 WiFi 的使用也有干扰信号的风险存在，

如何更好地升级改造航电系统，也是航空公司需要探索的问题。

另外，成本也是重要的考量。据专家介绍，改装一架飞机，仅硬件产品就大约需要 40 万美元，在不包括后期运维的情况下，改装一架飞机，大约需要 350 万元人民币。

规模化商用 将催生空中网络购物

除了技术瓶颈，空中 WiFi 的规模化商用也需要航空公司探索，如果说乘客掏出真金白银使用昂贵的空中上网服务，航空公司至今没有多少好办法。

美国空中 WiFi 供应商 GoGo 公布的数据显示，传输数据到飞机上，每传输 1M 字节成本大约是 20 美分，传输 1G