

共享充电宝可能在『共享』你的隐私

随着科技进步，个人信息泄露途径不断增多，我们该如何守好自己的隐私

共享充电宝最近陷入了泄露个人隐私的旋涡。部分共享充电宝不仅可能存在质量隐患，还可能被不法分子植入“木马”程序，导致手机里的通讯录、文本信息甚至照片、视频等隐私数据被泄露。App、SDK、二手交易平台……随着科技进步，个人信息尤其是隐私的泄露途径不断增多。由中国消费者协会发布的《App个人信息泄露情况》提到，个人信息被泄露后，约86.5%的受访者曾收到推销电话或短信的骚扰，约75.0%的受访者接到诈骗电话，约63.4%的受访者收到垃圾邮件。作为消费者的我们，如何守好自己的个人信息？相关监管部门，又该如何加强监管？

数亿人在用的共享充电宝有陷阱

艾媒咨询发布的《2020上半年中国共享充电宝行业发展专题研究报告》显示，2020年中国共享充电宝用户已达2.29亿人。消费者使用共享充电宝致使个人隐私数据泄露现象时有发生。

近日，公安部网安局微信公众号推送的《警惕身边的共享充电宝陷阱》一文中称，部分共享充电宝不仅可能存在质量隐患，还可能被不法分子植入“木马”程序，导致手机里的通讯录、文本信息甚至照片、视频等隐私数据被泄露。这些充电宝主要来源于三个地方：一是商场里的可租赁移动电源；二是火车站里叫卖的满电充电宝；三是扫码免费送的充电宝。

警方提示：不要随意购买和扫描来历不明的充电宝，如有需要，请选择正规产品或扫描正规公司的可租赁移动电源。当手

机连接充电电源时，提示是否“信任”时，请提高警惕。

目前，我国共享充电宝行业已形成“三电一兽”——街电、来电、小电、怪兽充电的垄断式格局。

小电发布官方声明称，小电共享充电宝在设计上充分注重对用户隐私数据的保护。在硬件层面，小电充电宝内部线路不含有数据传输线，仅以电源线提供充电功能。在软件层面，小电始终严格遵守《隐私政策》条款，通过多重数据保护技术和管理措施杜绝非法收集用户信息的情况发生。

怪兽充电的工作人员也表示，“我们的数据线是没有数据传输能力的，只能用来充电”“用户的充电订单都会享受隐私保护”，并强调其充电宝查询不到用户手机上的数据、无法读取用户的数据。



如果隐私已经泄露，怎么办？

对此，吴启均提到，如果消费者在使用共享充电宝时遭遇隐私泄露，首先应该厘清可能的泄露途径，如确定是在使用共享充电宝时泄露的个人信息，那么应当及时采取有效措施固定证据，如手机使用痕迹、可能存在的“木马”等程序、已经泄露的个人隐私信息以及泄露平

台。然后立即通知相关平台要求对个人信息予以删除，以降低对个人的不利影响。若因隐私泄露对个人名誉、财产等造成损失，可以要求侵权人予以赔偿。最后，及时向人民法院提起诉讼，要求侵权人停止侵权、赔礼道歉并赔偿损失。若侵权情节严重，构成犯罪的，也可向公安机关检举控告。

企业如何加强自律？

韩英伟建议，共享充电宝相关企业要确保产品合规、安全，始终严格遵守《隐私政策》条款等，杜绝非法收集用户信息的情况发生，设立可疑充电宝检举部门，并设线下检举点，对被检举的充电宝进行检测。在企业内部培养用户隐私绝对至上的企业文化，同时成立监管合规部门，充分了解法律法规。

吴启均则认为，从技术保护层面来讲，共享充电宝企业可以采取更多的信息安全防护措施来保障用户的个

人信息安全，如制定共享充电宝检测和维护机制，对可能已被拆封/改装或植入恶意程序的共享充电宝及时进行回收并维护等。从企业合规经营层面来讲，共享充电宝运营企业应建立个人信息泄露救济预案机制。若发现保管的用户个人信息发生或者可能发生泄露、损毁、丢失的，应当立即采取补救措施；造成或者可能造成严重后果的，应当立即向准予企业许可或者备案的电信管理机构报告，并积极配合相关部门进行调查处理。

部门如何加强监管？

吴启均说，随着科技进步，个人信息尤其是隐私的泄露途径不断增多，而法律法规中针对具体社会生活的规定往往与新技术之间存在一定的时间差。因此，首先要求立法机关、司法机关以及行政机关关注科技动态，在处理相关问题时，灵活掌握，参照法律原则进行处理，并不断完善立法及监管措施；其次要求消费者在使用新生事物时，增强防范意识，确认安全后再使用；再次，供应商应注意保护消费者的隐私不被泄露。

吴启均建议，政府可以设立企业运营的最基本条件，包括实名制注册使用、服务内容、使用费用和押金监管、鼓励为使用者购买责任保险并在事故中先行赔付、明确运营维护内容和从业人员准入要求、对使用者违法违规行为的约束和处

理、投诉处理、使用者隐私保护等内容。另外，可以协调政府部门加大对充电宝使用违法违规的执法力度，推动将违规使用、故意损毁、破坏和私自改装等行为纳入信用体系，促进充电宝良好使用“软”环境的建设。

“日常生活中，消费者在使用共享充电宝时，如果没有意识到相关安全问题，那往往在使用某些共享充电宝时很难发现其隐私数据被窃取，一方面因为“木马”程序都比较隐蔽，另一方面大多数消费者缺乏网络安全技术相关知识，一旦其隐私被泄露，除非遭遇敲诈勒索等，否则很难主动发现自己的隐私被泄露。”刘德良说。

因此，刘德良建议由政府相关部门出面，对提供共享充电宝的企业进行不定时安全检测，如果发现问题，则立即追究责任。

信息泄露的隐患还有哪些？

App、SDK、二手交易平台……生活中，还存在哪些信息泄露的隐患？日前，工业和信息化部网站公布关于侵害用户权益行为的App通报（2020年第七批）。截至通报发出时，尚有63款App涉及“违规收集个人信息”尚未完成整改。

上述通报所指App违法违规收集个人信息，主要表现为存在强制授权、过度索权、超范围收集个人信息等。以超范围收集个人信息为例，不少用户可能会遇到这样的情况，即在无十分必要的情况下，天气类App要求访问通讯录，健身软件要求授权手机相册……若用户拒绝接受授权，将无法下载或正常使用App。

事实上，不仅是部分App，对用户个人信息安全造成威胁的还有SDK。这种在手机软

件中提供某种功能或服务的插件可谓是隐形“窃贼”。据业内人士介绍，第三方SDK除了收集用户手机号码、设备信息之外，还会收集用户手机通讯录、短信信息、传感器信息等隐私信息，在采集之后还会发送至指定服务器进行存储。

除了上述隐蔽手段，还有不少明目张胆的威胁，将个人信息堂而皇之地摆上交易桌。

在一些知名的二手交易平台，个人户籍、名下房产、出行记录等20多项个人隐私信息被公开售卖，根据信息的查询等待时间及难度不同，费用也在几百元到上千元浮动。

此外，随着人脸识别技术被广泛应用后，面部特征等生物特征信息收集使用不规范等问题也逐渐暴露，加剧了“人脸”信息泄露的风险。

个人如何防范？

面对部分共享充电宝带来的隐私泄露风险，消费者该如何辨别和防范？

北京市盈科律师事务所高级合伙人韩英伟给出了三点建议：第一，注意商家的虚假标识，不要使用可疑或假冒伪劣产品；第二，查看充电宝的安全标志；第三，使用共享充电宝时，当出现“是否信任此电脑”的弹窗，或出现要求信任等提示时，需要提高

警惕。先点击“否”或“拒绝”等，并归还可疑充电宝。

重庆市律师协会民事专业委员会主任、重庆中世律师事务所创始合伙人吴启均也建议：消费者在使用共享充电宝前，须仔细阅读用户协议及隐私保护政策，尤其应注意相应责任划分约定及个人信息收集和共享条款，以免后续产生争议。若用户对相应企业的用户协议或隐私政策条款约定存有异议，则需谨慎对个人信息作出授权或使用相关产品。

保护公民隐私有哪些招？

《刑法》规定侵犯公民个人信息罪

根据我国《刑法》规定，违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，构成侵犯公民个人信息罪。根据相关司法解释，非法获取、出售通信信息、财产信息等50条以上，或者非法获取、出售或提供通信信息、交易信息等公民个人信息500条以上的，或违法所得5000元以上，均属于情节严重的情形。

《民法典》对隐私权保护范围作出规定

《民法典》在第四编第六章对隐私权的概念和保护范围作出明确具体的规定，提到“信息处理者在进行个人信息的收集、存储、使用、加工、传输等行为时，必须征得权利人同意，并明示处理信息的目的、方式和范围，不违反法律、行政法规的规定和双方的约定。”作为首部专门规定个人信息保护的律

治理App违法违规收集使用个人信息

为保护个人信息权益，2020年7月，中央网信办、工信部、公安部、国家市场监督管理总局四部门启动2020年App违法违规收集使用个人信息治理工作，重点打击App后台私自上传个人信息等群众反映强烈的问题。2020年10月至12月，市场监管总局等14部门联合开展2020网络市场监管专项行动，重点任务之一是加强二手物品网络交易平台监管。

规范App个人信息收集行为

为落实《中华人民共和国网络安全法》关于个人信息收集合法、正当、必要的原则，规范App个人信息收集行为，2020年12月1日，国家互联网信息办公室印发关于《常见类型移动互联网应用程序（App）必要个人信息范围（征求意见稿）》的通知，提出网络直播类、在线影音类、短视频类等App无须个人信息，即可用基本功能。此外，《征求意见稿》还规定了地图导航、网络约车、即时通信等38类常见类型App必要个人信息范围。