部分共享充电宝竟被植入“木马”程序泄露隐私

警惕共享充电宝信息安全“陷阱”

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

一些黑色产业利用“木马”等恶意程序，控制用户的终端设备窃取数据，随后通过贩卖数据获取非法利益，或直接利用这些数据实施违法犯罪行为，已经形成一条黑色产业链

共享充电宝相关企业要确保产品合规、安全，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

生活中，出门在外遇到手机没电时，一款可租用的共享充电宝可谓“江湖救急”。近两年来，随着消费的变化，曾经被人称为“伪需求”的共享充电宝，如今似乎成了“刚需”。不过，共享充电宝最近陷入了泄露个人隐私的旋涡。

近日，公安部网安局微信公众号推送了一篇题为《警惕身边的共享充电宝陷阱》的文章。该文称，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。

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。

数据隐私问题突出 相关企业紧急发声

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。

在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，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。

当共享充电宝陷入泄露个人隐私旋涡后，2020年12月8日，小电公关负责人刘彬在微信朋友圈回应称：“特地剪了一个充电宝，小电的充电宝只有正负极线路，不涉及数据传输的线路，不会有木马和数据的泄露风险。”

随后，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。

企业自律确保合规 行业规范适时出台

大数据时代，如何保障网络安全、数据安全一直是各行各业普遍面临的问题。

据北京师范大学法学院教授刘德良介绍，一些黑色产业利用“木马”等恶意程序，控制用户的终端设备窃取数据，包括手机里面的一些数据信息，之后通过贩卖数据获取非法利益，或直接利用这些数据实施违法犯罪行为，已经形成一条黑色产业链。

值得注意的是，北京市盈科律师事务所高级合伙人韩英伟提出，目前还存在监管部门监管滞后、部分参与者和使用者个人素质待提高、国家法律法规不够完善、准入门槛、准入机制缺失等问题。

最近，共享充电宝行业暴露出来的隐私泄露风险再次将上述问题推上了风口浪尖。

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。同时，政府应对相关制度进行完善，加强对商家的监管和引导，成立相应的监管部门，加强对隐私保护的普及和推广等。

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、毁损、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。

吴启均建议，首先，建立共享充电宝行业标准，对共享充电宝设置特定的行业规范。例如，设置共享充电宝应当不具有数据传输功能等。其次，共享充电宝行业可以建立相应的行业运行规范。例如，在个人信息收集/使用过程中，建立完善的用户个人信息保护机制，通过用户协议或隐私保护政策等明示用户个人信息收集、使用的目的、方式和范围，查询、更正信息的渠道以及拒绝提供信息的后果等，在明确取得用户授权后在其授权范围内对用户个人信息进行采集和使用。

吴启均还建议，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、服务合同内容、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。

用户增强防范意识 如遇侵权及时止损

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？

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。

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。

如果消费者的隐私已经被泄露，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。

韩英伟提出，如果消费者在使用共享充电宝时遇到隐私泄露，可以通过以下途径进行维权：向互联网管理部门、行业管理部门和相关机构进行投诉举报；寻求公安机关的帮助，以减少或挽回损失；向侵犯隐私的违法充电宝公司进行索赔；通过法律手段维护自己的合法权益等。

“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。

（据新华网）

“要数据跟要饭一样”，智慧城市数据之渴何解？

观众在第十届中国智慧城市与智能经济博览会上体验5G技术应用的虚拟现实游戏 ■新华社发

数据是智慧城市的血液。没有数据，智慧城市就成了无本之木。

记者在江苏、浙江、广东、四川等地采访发现，部分地方在建设智慧城市时仍存在数据少、欠账多、成网难、平台重复建设等问题，其背后，则是数据返还难、共享难、积累难的沉疴。

数据少、欠账多、成网难

记者注意到，多数城市的数字城市建设仍在路上，特别是数字化程度低、数据无法互通、数据应用重管理轻服务等现象明显，离全面感知、泛在互联、智能服务的智慧城市还很远。

不少城市数字化程度低、历史欠账多。以广州市为例，该市与全国多数城市一样，城市治理长期受制于治理要素信息化和标准化不足、基础数据欠账较多。为赋予城市建筑和单位法人统一和唯一的“数字身份”，广州市开展大规模清理核准。期间发现，一个公共厕所居然落有10多户人。这种人户分离现象也是城市数字化的普遍难点。

部分地方重复建设，数字化投入巨大却难以成网。记者看到，为加强基层治理和服务质效，各地都在加强数字化治理平台建设。然而，同一个市不同区县，甚至同一区县的不同乡镇，都争相投入数十万甚至数百万元资金建设同样的平台，不仅导致碎片化、重复化，而且平台效能参差不齐。

一名负责区县智慧城市建设的基层干部对此也很无奈：基层不一定想重复建设，问题是上级部门缺少条件和统筹，比如一个市级治理平台给区县一个导流接口就能节省大量资金，但市级层面往往因为硬件不足、容量有限、软件系统与区县格式不统一等问题，无法支撑区县需求。

数据无法互通、甚至缺少数据也让智慧平台难有用武之地。浙江省金华市司法局相关负责人说，当地在推进“无证明城市”改革中发现，数据归集特别是历史数据归集难度大，不同部门不同系统对接难，同一部门不同历史时期使用不同系统也会导致数据不统一，造成平台数据源不充足、运行难。

数据不充足也会限制地方数字化治理的思维和作为。记者发现，不少地方数字化治理平台只是简单接入公安、交通运输、城管等部门的信号，让平台具备可视化功能以辅助管理和决策，但并没有积极开发便民服务功能，有些平台有数字无智慧、有管理无治理。

在南京市溧水区，当地的智慧城市系统已开发出40多个服务应用。其中，仅一个智慧殡葬应用，就让原来一两天才能完成的证明申报和报销流程变成不到一小时就能办完。溧水区智慧办主任章丽坤说，数据多少决定服务多少，他们也曾想打通医院和社保数据，让市民不带医保卡也能看病，却因缺少数据难以实现。

“要数据跟要饭一样”

显然，数据是城市数字化建设的核心，数据无法有效共享已成为智慧城市建设的最大掣肘。

部分负责智慧城市建设的基层干部表示，许多部门在拒绝数据共享时的口头禅是：“不给你们顶多挨领导一顿骂，给了你们我天天担惊受怕。”

记者采访发现，部分地方建设数字治理平台准入门槛较低、参与建设运营的企业和机构资质参差不齐，相关部门缺乏监管机制、监管技术，的确可能存在重要敏感数据泄露的隐患。

这种地方平台无法有效保障数据安全的现实，加重了“数据大户”部门的免责心态。而没有更高层面的统筹，许多掌握核心数据的部门因为担心数据出问题需要担责，就会变着法儿躲闪，更不会主动研究信息共享机制。

记者还发现，长期以来，国家和省市各部门直通基层的信息采集系统平台（专网）较多，不少采集项目交叉重复，信息一旦采集上去又缺乏整合、难以返还共享，也给地方城市数字化建设带来难题。

成都市政务服务管理和网络理政办公室相关负责人说，国家和省级层面与地方数据共享机制尚不完善，“纵强横弱”现象突出，特别是受行业管理限制、数据管理权限上收等因素影响，部分数据未进行属地返还，造成地方部分数据使用困难。目前仅成都一地，就有37个部门的326项数据管理权限不在市本级，其中，132项在国家部委、194项在省级部门。

多地地方干部反映，专网权限限制了地方数据获取及业务开展。比如，因公安、卫健等部门数据管理权限上收，地方能接触到的人口库中身份、常住人口等信息不再更新，影响了地方人口信息管理、不动产登记等工作的开展和基于人口数据的大数据分析。又如，虽然民政部通过国家共享平台提供了婚姻登记查询核验接口，但像四川这样的省份，每日数据调用频次被限制在1万次，实际上影响了地方购房资格核验、公积金办理等相关业务办理。

“平时要数据跟要饭一样，能不能要到全凭运气。”一名负责智慧城市建设的基层干部感慨说，各地展示成果时只能强调平台归集了多少条、多大量的数据，而不是归集了多少部门、涉及多少权限，这是因为：第一，几乎没有一个部门的数据毫无保留、全口径与智慧城市建设共享；第二，还没有归集到的数据才是最重要、最核心的数据。

疫情期间，通过与公安等部门及腾讯、阿里等第三方公司协作，不少城市的智慧平台归集了本地人口、企业信息等数据。负责数字城市建设的地方干部直观感受到，只有直接服务居民群众才能实现数据积累，归集到更广泛而准确的数据，但疫情防控毕竟是特殊情况，常态化开展服务、实现数据沉淀是各地的迫切需要。

“不能等到智慧城市建好再去考虑如何服务群众。我们亟须转变观念，深化对智慧城市建设的认识。”章丽坤认为，部分地方城市数字化与政务服务网络化等未能有效互通，影响数据汇集，阻碍智慧城市建设进展，最终将制约当地数字化治理和服务群众的水平。

促进数据规范有效流通

没有数据的自由流通，智慧城市就无法生长。

各方认为，当前，迫切需要以智慧城市建设为契机形成以服务为导向的数据结构和应用体系。推动数据有序公开、有效流动，供社会各部门共享，降低社会信息成本，做大行政改革和数字化的红利。

有专家建议，国家层面应加快健全完善数据流通应用相关的法律法规。立法保障数据资源权益、个人信息（隐私）保护等，以推动数据流通和市场化应用，真正发挥数据要素对社会治理和经济发展的作用。

部分基层干部表示，国家层面需完善制度，将相应数据管理权限按需下放基层。加快推动垂直管理信息系统数据资源的属地返还，尤其是支撑地方政府城市数字化治理所需数据返还。

同时，还应推进从中央到地方的纵向数据共享和省市地区间横向数据共享，推动行政审批改革、综合执法改革、营商环境建设和市民服务创新等改革成果数字化，把改革和建设统一起来，实现数字化治理效能的全面有效提升。

也有专家建议合理安排数字城市数据节点。比如，南京财经大学红山学院副院长王晓庆建议长三角地区在土地相对充裕、新能源比较丰富的江苏北部等地区建立智慧城市大数据中心，而就全国来说则可实施“东数西算”，或是部分省区实施“南数北算”，以解决区域供应不匹配、地方发展不均衡、数字化系统建维成本高等问题。

（据新华网）