LINKS Law Offices
通力律师事务所

上海
上海市银城中路 68 号
时代金融中心 16 楼和 19 楼
邮编：200120
电话：+86 21 3135 8666
传真：+86 21 3135 8600

SHANGHAI
16F/19F, ONE LUJIAZUI
68 Yin Cheng Road Middle
Shanghai 200120 P.R.China
T: +86 21 3135 8666
F: +86 21 3135 8600

北京
北京市建国门北大街 8 号
华润大厦 4 楼
邮编：100005
电话：+86 10 8519 2266
传真：+86 10 8519 2929

BEIJING
4F, China Resources Building
8 Jianguomenbei Avenue
Beijing 100005 P.R.China
T: +86 10 8519 2266
F: +86 10 8519 2929

香港
香港中环皇后大道中 5 号
衡怡大厦 27 楼
电话：+852 2969 5300
传真：+852 2997 3385

HONG KONG
27F, Henley Building
5 Queen's Road Central
Central, Hong Kong
T: +852 2969 5300
F: +852 2997 3385

伦敦
1F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

LONDON
1F, 3 More London Riverside
London SE1 2RE
United Kingdom
T: +44 (0)20 3283 4337
D: +44 (0)20 3283 4323

www.llinkslaw.com
master@llinkslaw.com

公司及并购法律评述
2018 年 11 月

简析物联网应用中的网安数据合规问题

作者：潘永建 | 邓梓珊

物联网，顾名思义，指物与物相连的互联网。物联网通过各种信息传感设备，按约定的协议，利用互联网把各种物品连接起来，进行信息自动交换和通信，实现对物品的智能化识别、定位、跟踪、监控和管理。[1]物联网有两种基本应用模式，对象的智能标签识别以及对象的智能控制。这两种基本应用模式与智能感应、自动化系统等多种技术结合，构成了应用于生活起居、工业控制、市政管理的综合性物联网管理系统。举例而言，智能穿戴设备、便携医疗设备、智能家居系统、无人驾驶卡车、物流跟踪标签、机器和基础设施维护、感应式库存管理等都属于物联网的具体应用。

根据 Gartner 公司预测，2018 年全球物联网设备约为 100 亿台，预计到 2019 年全球会有 132.7 亿台物联网设备联网。[2]随着物联网技术在社会生活中的广泛应用，由于物联网设备的数量、部署规模、系统的异构性(由多个厂家的产品所组成)以及各种新兴应用场景，物联网运营的安全与稳定事关社会经济安全与稳定。本文拟对物联网运营中涉及的网络与数据安全的重大问题进行简析，供相关企业参考。

如您需要了解我们的出版物，
请与下列人员联系：

郭建良: (86 21) 3135 8756
Publication@llinkslaw.com

通力律师事务所
www.llinkslaw.com

简析物联网应用中的网安数据合规问题

一、 物联网运营原理

要理解物联网应用中可能存在的合规问题，需要先对物联网的应用原理有所了解。物联网应用过程中主要通过三大逻辑层实现数据的收集、处理与传输。

1. 通过感知层实现全面感知，即通过传感网络，利用多种自动识别技术(如二维码、电子标签、语音识别等)或传感技术(如无线传感器、NFC 等)获取环境信息;

2. 通过网络层实现数据的可靠传输，即采用互联网协议、技术和服务或云计算等技术手段把各种物体接入互联网，实现基于互联网的物物连接与交互;

3. 通过应用层实现数据的智能处理，在应用层对感知层采集的数据进行计算、处理和数据挖掘，从而实现对物理世界的实时控制、精确管理和科学决策。

前述三个层面的内容，以地铁票的手机支付为例，体现为如下三个流程：用户手持移动设备经过验票区，验票装置通过移动设备的 NFC 电子标签识别用户身份；地铁公司、第三方

支付公司的服务器进行数据传输及订单验证；服务器上的应用程序进行数据处理实现购买地铁票的转账操作。

二、 网络安全

物联网应用系统具有操作简便，高度可视化的特点，但每一个具体应用都是极其复杂的生态系统，依赖于许多设备制造商、集成商、开发人员、部署人员和运营商。众多厂商各自都有不同种类和程度的安全风险，攻击可能发生在供应链的各个阶段。由于缺乏安全意识或者安全技术，企业很容易在开发过程中产生安全漏洞，在设备上线后也有可能发生网络攻击、勒索，以及敏感信息泄露等安全事件。除此之外，针对终端用户个人发起的安全攻击也屡见不鲜。攻击者通过攻击物联网设备可获取个人隐私信息或财务账户信息，并以勒索、盗窃等方式导致个人名誉或财产损失，或是通过所获取的大量个人隐私信息进行出售获利。

对物联网用户而言，物联网技术在带来便利的同时，安全威胁具有侵入性和突发性，且难以从用户端进行直接阻断，事前防范尤为重要。因此，《网络安全法》要求物联网应用中各网络运营者应落实以下相关网络安全义务:

1. 落实网络安全等级保护义务，保障企业网路运行安全。《信息安全技术 网络安全等级保护定级指南(征求意见稿)》明确将物联网作为网络安全等级保护工作的作用对象，《GB/T 22239.4-XXXX 信息安全技术 网络安全等级保护基本要求 第 4 部分 物联网安全扩展要求》又在第 1 部分安全通用要求的基础上针对物联网提出更为细致的安全保护要求。对于物联网运营者来说，物联网应作为一个整体对象进行安保定级，主要包括感知层、网络传输层和处理应用层等要素。

2. 建设与网络安全等级保护以及物联网特点相适应的安全保护制度。针对不同逻辑层的特性，制定内部安全管理制度和操作流程，确定网络安全负责人。如针对感知层，应着重确保终端感知节点设备的物理和环境安全；针对网络传输层应关注通信安全及加密技术等；针对处理应用层，应落实访问控制，保证数据的完整性、可用性。

   企业在制定具体网络安全保护制度时，可以参考全国信息安全标准化技术委员起草的

《GB/T 22239.4-XXXX 信息安全技术 网络安全等级保护基本要求 第 4 部分 物联网安全扩展要求》。

3. 物联网应用中的网络产品、服务以及网络关键设备和网络安全专用产品应当符合国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

4. 落实网络实名制要求。为用户办理网络接入、域名注册服务，固定电话、移动电话等入网手续，或者提供信息发布、即时通讯等服务时，应当要求用户提供真实身份并核实，否则不得为其提供服务。

5. 制定应急预案。发现网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

   由于物联网经常与自动化系统结合使用，采用互联网协议交互与连接，一旦攻击者获得物联网中某台设备的远程控制权限，便可能引发连锁反应。例如，医院保存血浆的医用冰箱若采用统一联动管理的模式，攻击者只要篡改某单台设备的感应温度，其他所有设备都会受到影响。

   因此，应急预案的制定，应当将设备互联模式、各种形态的攻击方式、安全事件种类等因素考虑在内，并考虑如何介入并解决因此引发的连锁反应，将损失及影响降至最低。

6. 不得擅自发布网络公共安全信息。开展安全认证、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息应当遵守国家规定。

三、 关键信息基础设施的认定与义务

目前，法律对关键信息基础设施(“CII”)的范围仅作出了较为原则性的定义，缺乏明确的关键信息基础设施的认定标准，可以参照的法规及政策性文件有《网络安全法》《国家网络安全检查操作指南》(以下简称“《网络安检指南》”)《国家网络空间安全战略》以及《关键信息基础设施保护条例(征求意见稿)》。上述法规文件对 CII 运营者(“CIIO”)均采用“行业列举+后果概括”的复合定义。应当注意的是，并非一旦落入法规列举的行业的网络运营者，就必

然属于 CIIO；反之，未落入法规列举的行业的网络运营者，并非必然就不构成 CIIO。

《网络安检指南》在操作层面规定了确定 CII 的三个步骤，一是确定关键业务，二是确定支撑关键业务的信息系统或工业控制系统，三是根据关键业务对信息系统或工业控制系统的依赖程度，以及信息系统发生网络安全事件后可能造成的损失认定关键信息基础设施。具体到物联网企业，应当将应用环节中所涉及的网站、网络设施(硬件)、业务系统、数据存储(云)以及服务器等网络设施和信息系统作为一个整体综合考虑。只要整体上，或者有一个网络设施或者信息系统符合下列后果之一的，即构成 CII:

1. 日均访问量(超过 100 万人次)、注册用户数(1000 万人次)或者活跃用户数(100 万人次)、日均成交订单额或者交易额(1000 万元)、服务器或数据中心规模(1500 个标准机架);

2. 一旦发生安全事故，可能造成以下影响:
   (1)影响工作、生活的人口数(100 万);
   (2)泄露个人信息数(100 万);
   (3)大量个人或企业的敏感信息泄露。

因此，若物联网企业运营管理的联网设备数量众多，达到日均访问量、注册用户数、活跃用户数或数据中心规模的标准；或运营过程中收集存储的个人信息数达到 100 万条以上；或涉及的业务量大，达到订单额或交易额的标准；或涉及关系民生的重要信息系统、控制系统的，该企业就有可能构成关键信息基础设施运营者，具体还需要采用上文所述的三步骤进行判断。物联网企业一旦构成 CIIO，则需要遵守《网络安全法》对 CIIO 专门提出的要求。属于跨国运营的物联网企业，需要格外注意 CIIO 的个人信息及重要数据本地存储义务以及数据出境安全评估义务，并考虑调整与此相关的网络架构及业务模式设计。对于服务器部署在国外或因组织架构等原因必须将个人信息或重要数据传输出境的，应注意以下两方面内容:

1. 确保在隐私政策或类似性质的文本中就数据出境情况向个人信息主体进行明示;

2. 尽快就数据本地化存储及安全评估流程展开相应准备工作，以免被认定为 CIIO 后，无法在规定的时限内完全做到合法合规。

四、 个人信息与重要数据

使用物联网传感设备收集个人信息与重要数据，受《网络安全法》规制。对于物联网而言，数据合规更具有挑战性，因为收集数据的传感设备数量众多，分布在各个地区甚至是以动态方式配备在运输设备上或直接由用户随身携带。企业需要清楚明确数据是如何收集的，在哪里收集的，收集了何种数据，数据是如何受保护的，以及如果出现了问题该如何应对。

(一)获取用户知情同意

根据与个人信息保护相关的法律法规要求，物联网企业收集、使用个人信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。不得违反法律、法规的规定和双方的约定收集、使用信息。

物联网应用普遍具有高效、便捷的特点，在物联网网络中处理个人数据的知情同意可能难以获得。一般情况下，个人信息收集者可以通过隐私政策、书面同意声明、用户注册协议的方式获取知情同意。但如果个人信息主体并非物联网平台或服务的注册用户，则个人信息收集者与个人信息主体之间唯一的互动可能就是设备之间的信息交互。企业应在发生信息交互时，采集用户个人信息之前，及时以合法合规的方式获取用户的知情同意。在与被收集主体无互动连接点的情况下，如果难以获得用户的知情同意，则应避免直接采集用户的“个人信息”，在商业目的允许的范围内，考虑配合其他技术手段直接采集去标识化的非个人信息。

(二)避免过度收集信息

实践中，有物联网 APP 存在“一键”收集与所提供的服务并无必然联系的个人信息的情况。《网络安全法》第四十一条提出，网络运营者收集、使用个人信息，应当遵循合法、正当、**必要**的原则，不得收集与其提供服务无关的个人信息。具体而言:

1. 收集的个人信息的类型应与实现产品或服务的业务功能有直接关联。直接关联是指没有该信息的参与，产品或服务的功能无法实现;

2. 自动采集个人信息的频率应是实现产品或服务的业务功能所必需的最低频率;

3. 间接获取个人信息的数量应是实现产品或服务的业务功能所必需的最少数量。

另外，物联网企业应注意，感知设备采集的指纹、人脸识别信息等生物特征信息属于个人敏感信息。收集用户个人敏感信息前，还应:

1. 向个人信息主体告知所提供产品或服务的核心业务功能及所必需收集的个人敏感信息，并明确告知拒绝提供或拒绝同意将带来的影响。应允许个人信息主体选择是否提供或同意自动采集;

2. 产品或服务如提供其他附加功能，需要收集个人敏感信息时，收集前应向个人信息主体逐一说明个人敏感信息为完成何种附加功能所必需，并允许个人信息主体逐项选择是否提供或同意自动采集个人敏感信息。当个人信息主体拒绝时，可不提供相应的附加功能，但不应以此为理由停止提供核心业务功能，并应保障相应的服务质量。

过度收集个人信息可能导致行政处罚[3]，甚至可能构成刑事犯罪[4]。为避免过度收集个人信息，物联网企业应根据个人信息与实现各项功能之间的因果关系；区分产品或服务的核心功能与附加功能；并确保用户拒绝提供个人敏感信息时能够继续使用核心功能。

(三)重要数据识别

构成CIIO的物联网企业，负有个人信息及重要数据本地存储义务以及数据出境安全评估义务。因此，除了判定是否属于 CIIO 外，企业还应根据其所处的行业(领域)，业务所涉猎的行业(领域)，业务规模，所收集的数据类型、体量、性质，综合判断其运营过程中收集、产生的数据是否属于重要数据。在需要的情况下，可以通过与行业主管部门积极沟通，有效地识别重要数据，以更好地履行重要数据的合规义务。例如，曾有某矿石粉碎机制造商向我们咨询，其用设备端传感器收集的“采矿设备数据”是否构成重要数据。该等采矿设备数据中包含碎石颗粒大小、设备的运行温度、钻头转速、处理吨数等。简言之，在判断该等“采矿设备数据”是否构成重要数据，首先应当考虑该客户矿

石粉碎机所销往的矿场矿石种类，才能判断相关数据涉及的所有行业；其次应明确客户所收集的数据的具体种类，以进一步判断客户所收集的数据是否落入有关行业的重要数据的范畴；最后还需考虑相关矿场的规模、市场份额等因素，以进行汇聚数据后果判断。

五、 其他合规要点

除上述合规问题外，物联网从业企业应注意以下其他问题:

1. 物联网应用涉及的行业众多，企业在制定相关合规政策时应注意是否存在特殊的行业规定。必要时，可积极与行业主管部门进行沟通。例如，《征信业管理条例》《金融消费者权益保护实施办法》《人口健康信息管理办法》《地图管理条例》等单行行政法规均设置了“数据出境”和“数据本地化存储”的限制。
2. 由于感知设备遍布位置分散，特别是从事跨国运营的物联网企业，应注意从各地收集到的数据在适用法律上可能有所不同，且该等法律对网安数据的合规要求亦可能有所不同。
3. 物联网应用涉及的系统、平台、参与方众多，物联网企业应注意与第三方之间的网络安全、数据存储移转安全责任的明确界定与划分。

简析物联网应用中的网安数据合规问题

如需进一步信息，请联系:

作　者	
潘永建 电话:+86 21 3135 8701 david.pan@llinkslaw.com	

上　海	
俞卫锋 电话: +86 21 3135 8686 david.yu@llinkslaw.com	**刘贇春** 电话: +86 21 3135 8678 bernie.liu@llinkslaw.com
佘　铭 电话: +86 21 3135 8770 selena.she@llinkslaw.com	**娄斐弘** 电话: +86 21 3135 8783 nicholas.lou@llinkslaw.com
钱大立 电话: +86 21 3135 8676 dali.qian@llinkslaw.com	**孔焕志** 电话: +86 21 3135 8777 kenneth.kong@llinkslaw.com
吴　炜 电话: +86 21 6043 3711 david.wu@llinkslaw.com	**潘永建** 电话: +86 21 3135 8701 david.pan@llinkslaw.com
姜　琳 电话: +86 21 6043 3710 elyn.jiang@llinkslaw.com	
北　京	
俞卫锋 电话: +86 10 8519 2266 david.yu@llinkslaw.com	**刘贇春** 电话: +86 10 8519 2266 bernie.liu@llinkslaw.com
杨玉华 电话: +86 10 8519 1606 yuhua.yang@llinkslaw.com	
香　港(与张慧雯律师事务所有限法律责任合伙联营)	
俞卫锋 电话: +86 21 3135 8686 david.yu@llinkslaw.com	**吕　红** 电话: +86 21 3135 8776 sandra.lu@llinkslaw.com
伦　敦	
杨玉华 电话: +44 (0)20 3283 4337 yuhua.yang@llinkslaw.com	

简析物联网应用中的网安数据合规问题

[1] 韩毅刚，冯飞，杨仁宇等编著(2017). 物联网概论. 北京：机械工业出版社.
[2] Christy Petty (2018). The Emergence of the IoT Architect. https://www.gartner.com/smarterwithgartner/the-emergence-of-the-iot-architect/.
[3] 2018 年 3 月，支付宝(中国)网络技术有限公司因在“年度账单”中过度要求收集、使用用户个人信息，被中国人民银行杭州支行以“个人金融信息收集不符合最少、必要原则”及“个人金融信息使用不当”为由处以罚款。
[4] 《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》规定，“违反国家有关规定，通过购买、收受、交换等方式获取公民个人信息，或者在履行职责、提供服务过程中收集公民个人信息的，属于刑法第二百五十三条之一第三款规定的‘以其他方法非法获取公民个人信息’。”