中国消费类物联网设备白皮书

TIC 国际检验检测认证理事会上海代表处

数字化及智能制造工作组

（2023 年 3 月版）

目 录

摘要

TIC 国际检验检测认证理事会上海代表处（以下简称“TIC 理事会”）撰写《中国消费类物联网设备白皮书》（以下简称“白皮书”）。白皮书由 TIC 理事会“数字化及智能制造工作组”主笔，围绕消费类物联网设备，从市场规模、应用场景、市场驱动力、相关安全挑战、相关法规与标准等角度，梳理了中国消费类物联网设备发展概况及所面临的机遇与挑战，并从第三方认证机构的角度为提出规范性建议，以期充分发挥第三方认证在消费类物联网安全方面的积极促进作用，助力中国消费类物联网设备市场健康发展。

白皮书显示：随着中国消费类物联网市场规模不断增大，应用场景逐渐打破了线上与线下的界限，政策、科技、平台生态等亦助推着中国消费类物联网市场向全球化发展。但与此同时，也对设备的安全性提出了更高要求。消费类物联网产品因其面临的应用场景和用户群体的特性，其安全问题的产生和危害会影响到众多相关方，需要整合政府、制造商、第三方检测认证机构和用户个人等多方力量，从安全意识、安全法规、技术措施、应用操作等构建全方面的安全防护，才能真正保护个人隐私，避免因信息泄露和其它安全事件造成风险，从而促进消费类物联网行业健康有序的发展。其中，第三方认证机构，可凭其独立性及专业性，贯穿物联网标准与法规的设计、产品制造生产、市场监管等各个阶段或过程，成为消费类物联网设备全流程安全的守护者。

1. 简介

消费类物联网设备主要包括：1、个人购买使用的物联网产品，如可穿戴设备（wearable）、智能耳戴式设备（hearable）、智能手机，以及个人电脑外接设备如智能手表等；2、智能家居产品，如智能家电、智能电视、家庭监控等。特别指出，医疗类、车联网类设备不在本文讨论的范围内。

随着全球消费群体针对智能消费品需求的不断地增大，并伴随着相关智能科技日新月异的飞速发展，近年来智能科技从一开始简单的数据搜集，再到目前接近人工智能的用户数据分析并进行相关的用户习惯管控，所有的这些都通过不同的网络进行了跨时代的改革进步。

1.1. 中国消费类物联网设备展望

作为全球物联网消费品最大的国家之一，中国无疑在这方面具有相当大的市场潜力和客户使用群体，而各类与物联网消费品在中国的使用以及规模都达到了空前的情况。截止到 2022 年底，以智能家电为例，根据最新的中国工信部的统计，我国智能家电的市场规模从 2016 年的 2000 亿已经达到了现在的 5000 亿[1]，越来越多的年轻人加入了使用智能家居的行列并把这些科技带来的便利普及到更多身边的亲朋好友，而科技的不断发展融入了绿色低碳的元素，相信这类物联网消费品的市场占有率将会越来越大，普及率将会越来越广。

1.2. 全球消费类物联网应用的整体情况

放眼全球各国，消费科技领域也在大张旗鼓地发生着变化，从几年前全球倡导的万物互联飞速演变成了现在的万物智能互联，物联网消费品的全球格局更进一步地走向更为智能的新高度：各种可穿戴的设备、智能美妆仪器、人工语音助手、VR 的虚拟现实互联都进一步地展现了这一变化。根据全球电子消费品协会以及第三方机构 GfK 的统计，智能消费品市场在 2021 年，全球物联网市场价值已经超过 1 万亿美元，而亚太地区凭借 42%的销售份额继续维持技术消费品市场上的领先地位。此外，25%的销售额来自欧洲，20%左右来自北美，7%来自拉丁美洲，6%来自中东、土耳其和非洲。这一整体的数据并以每年 3%-4%的增长率飞速上涨。物联网市场的复合年增长率以两位数增长，预计 2028 年将达到 1.9 万亿美元。

这一切的美好确实充满着浓郁的科技感和便捷，展现了人类智慧的结晶，但是当人们开始关心由智能设备搜集的数据是否会被滥用泄露开始，相关的物联网消费品的安全便走入了各界的视野范围。

[1] 中新网 《工信部：我国智能家电市场规模增长到 5000 亿元》 https://www.chinanews.com.cn/cj/2022/09-14/9852212.shtml

2. 中国消费类物联网驱动力和市场态势

2.1. 消费类物联网场景

万物互联，让消费者无论在何处，都能使用连接到互联网的设备。借助物联网设备，用户的生活时时刻刻都在与互联网进行交互，线上与线下的界限逐渐被打破，由此，消费者的生活也能够更加便利，更加智能化。

2.1.1. 高度联网和智能化的产品带来无限便利

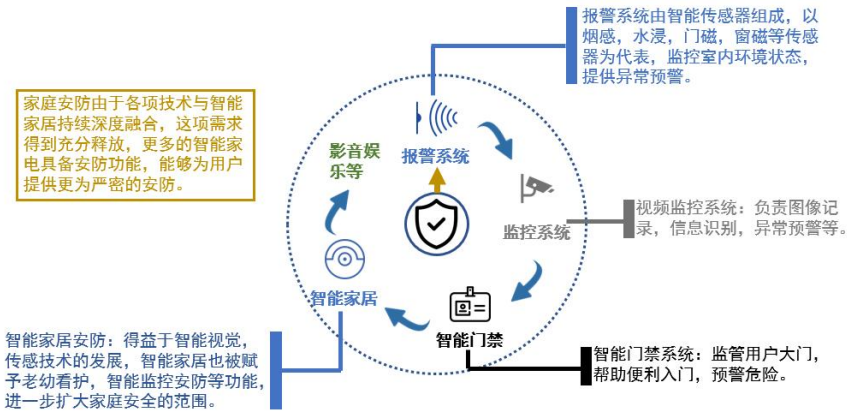
家庭智能安防

家庭安防的目的是为了保护用户及其财产的安全，近年来，物联网、AI 等技术融入到家庭安防让用户的生活变得安全、智能而又便利。目前家庭安防中起核心作用的当是以摄像头为中心而延展的一系列产品。

视频监控系统促进智能视觉技术的产生，智能视觉目前作为全屋智能联动生态核心能力之一，已经融入到各种全屋生态的智能家电中，例如智能猫眼，智能电视，智能扫地机器人等。这些智能家电能够提供家庭安全防范，老幼看护，娱乐交互等一系列深层次服务。未来 AI 技术，云计算等不断深入发展，还能够为视频监控系统提供更加智能化服务。

智能门禁系统的代表产品包括智能门锁，智能猫眼，智能门，智能楼宇系统等，主要利用 AI，智能视觉技术，物联网技术，生物识别技术等为用户提供便利，安全生活。便利生活主要体现在人到门开，远程开门等生活场景；安全生活体现在门口监控，异常情况警报等生活场景。

家庭智能安防未来将会充当全屋智能生态保护者的角色，为用户提供安全便利生活。

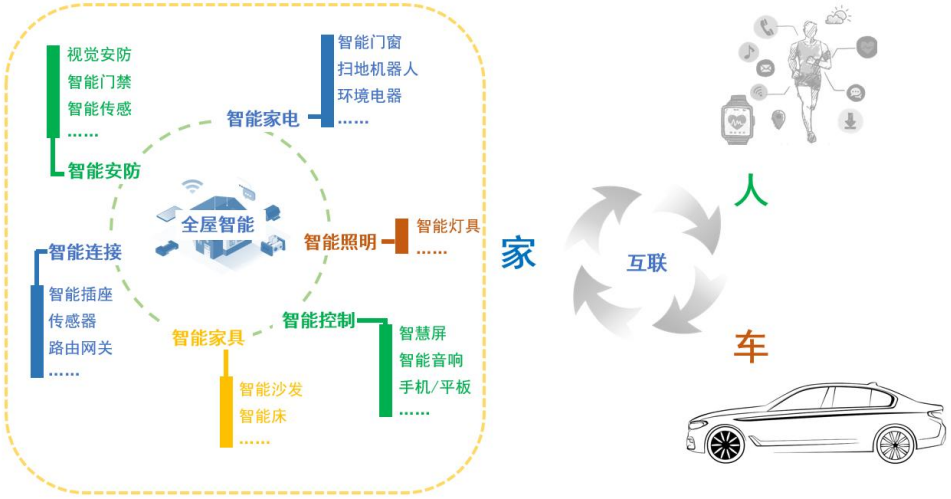


全屋智能

全屋智能生态综合了物联网，云计算，AI 等技术，可以对用户房屋内外的智能家居设备进行系统化的集中管理，并且能够与用户进行场景交互，场景联动，预测用户行为，成为用户的虚拟管家，为用户提供智能，便捷的生活。

用户在下班路上，就能通过汽车或者手机对全屋智能生态下达指令，通过智能环境电器，智能门窗，对室内的空气质量，温度，湿度进行调节，为用户提供舒适的环境；用户到家，智能安防系统，智能灯光系统进行协同作用，用户不进行任何操作的情况下就能安全入户；全屋智能系统会根据用户习惯，为用户入户后提供一系列场景服务，例如智能灯光与智能影音系统提供娱乐场景，智能卫浴系统提供洗浴场景，智能灯光与智能环境电器，智能床提供卧室入睡场景，为用户提供居家智能生活。

全屋智能生态还将与用户周边产品，例如手机，可穿戴设备，以及出行工具，例如汽车，形成“人-车-家”互联，互相协作生态，让用户的住与行便利化，智能化。



然而，物理世界与网络世界的边界趋于模糊，物联网为消费者带来便利的同时，也带来个人数据泄露的威胁。智能家居，可穿戴设备，资产追踪等物联网场景都会收集大量个人数据，通过个人数据能够对用户进行定位，生活行为分析，若被不法分子利用，将会对个人人身财产造成巨大损失。如何需要加强物联网设备的网络安全，保护消费者的个人数据，是厂商需要考虑的重点问题。

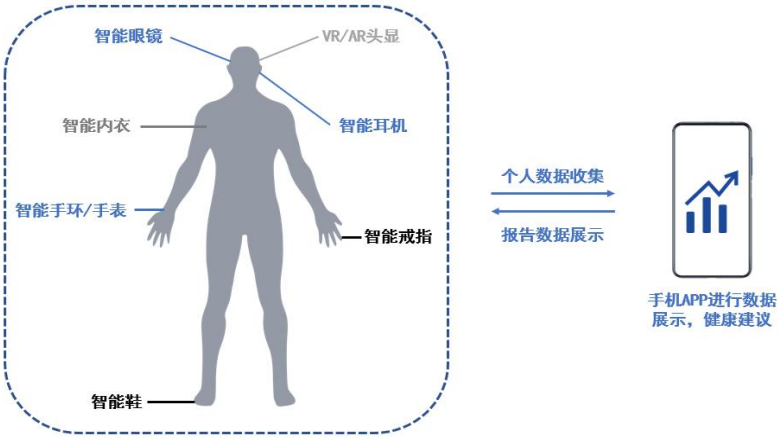
可穿戴设备

随着 AI、大数据、物联网等技术不断深化，智能可穿戴设备已经可以将用户的“一举一动”数字化，通过数据用户能够认识自己；可穿戴设备也能够将虚拟世界与现实世界相连，将虚拟与现实结合，提供便利。

目前主要的可穿戴电子设备，均围绕“健康”展开，可穿戴设备希望能够将身体中的一切状况利用可视化图表等方式展示出来，从心率，血氧，血压到用户的睡眠、饮食、运动，均可使用图像，文字等形式

为用户进行展示，甚至还能根据用户身体状况，为用户提供饮食，运动建议。以“睡眠监测”为例，使用智能腕带，运动手环等可穿戴设备就能掌握睡眠状况，用户可以在手机 APP 上阅读到自己详细的睡眠信息，包括深睡时间，浅睡时间等数据，从而知道自己睡得够不够好。除了监测睡眠，谷歌眼镜还能监测用户情绪健康，智能衣服、智能跑鞋能够监测身体健康数据，贴身监测用户的一举一动。

VR/AR 技术目前应用最广泛的领域当属娱乐和游戏，用户可以通过 VR/AR 进入虚拟世界，沉浸式体验游戏带来的刺激与快感。未来 VR/AR 也将广泛运用在商业，工业环境，例如进行外科手术培训，技术员工技能培训，沉浸式心理治疗等领域，提高员工工作效率，关注人员身心健康等。

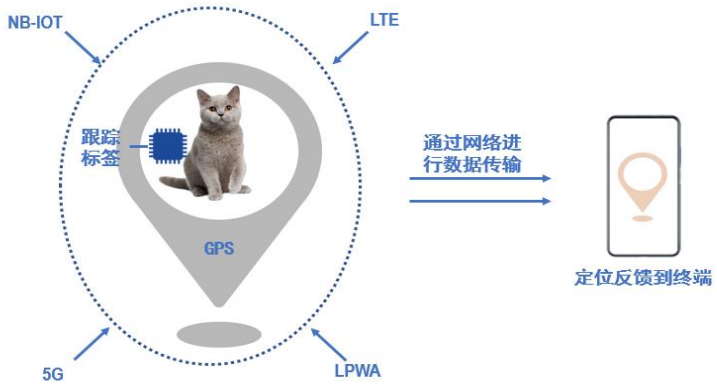


资产跟踪

物联网资产跟踪是一种用于跟踪项目物理位置和状态的方法，能够帮助个人和企业准确跟踪世界上任何地方的实物。物联网资产跟踪依赖于被跟踪装置的网络连接，因此它可以传达其位置和其他受监测信息。这种方式主要通过跟踪标签或装置固定到资产上来实现的，该资产使用定位技术（如北斗、GPS）进行定位，以及大覆盖范围的 5G、NB-IoT、LTE 或 LPWA 网络进行通信。

对于 C 端消费者资产追踪运用最广泛的场景莫过于儿童追踪，老年人或弱势群体跟踪，宠物跟踪等。用户可以在以上人群或宠物上进行跟踪标签的佩戴，若其走失，用户可以在电脑或者手机上快速定位失踪物，并快速找回。

资产跟踪也广泛运用于商业与工业，从货物运输到车辆跟踪，从森林到沙漠，物联网资产跟踪技术为企业降低了大量财产损失。

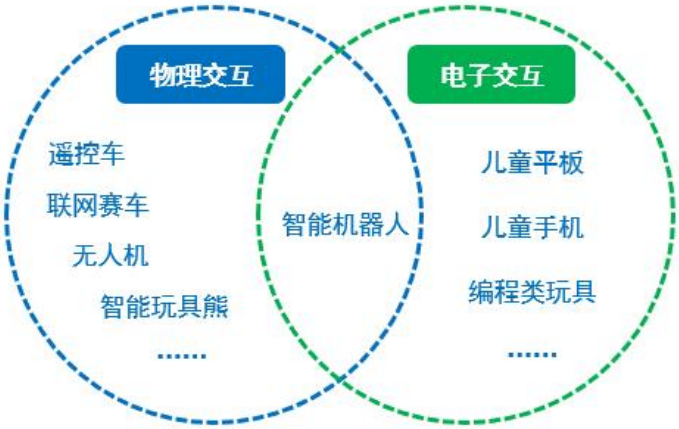


智能玩具

智能玩具是玩具产品的一个细分市场，主要是将物联网技术，AI 等技术与传统的玩具整合，让儿童能够进行网络交互，物理交互等。

目前主流的智能玩具有智能机器人，能够与儿童进行语音交流，同时融入 AI 教育，能够为儿童提供基础教育等；也包含儿童编程类产品，可以让儿童通过简易的编程技术，让儿童自己去构建机器人；还有传统玩具智能化，例如联网赛车，无人机，遥控车，智能洋娃娃等。

除了传统的玩具智能化，手机，平板电脑等电子屏幕交互式产品对于儿童而言也是智能玩具之一，电子屏类产品能够为儿童提供线上游戏，线上教育等功能，能够帮助儿童拓展眼界。



2.1.2. 消费物联网发展的核心

与其他诸如工业物联网设备不同，消费类物联网更直接地与终端用户交互，更直接地服务于终端用户，更广泛地嵌入到终端用户的日常生活场景，因此发展消费类物联网的核心其实就是消费类物联网设备如何可以更好地服务于终端用户。

首先，消费类物联网设备应当努力提升用户体验。可以看到，目前就国内而言，消费类物联网设备在提升用户体验上还有很大的发展空间。当前，大多数厂商对于提升用户体验的认知和实现还停留在如何做一个更加友好的用户操作界面，或者如何简化用户对于设备的操作流程等。诚然，这些也是提升用户体验的方法，不过这样的方法过于碎片化，也无法做到标准化。事实上，用户体验是一个系统性的课题，是渗入到整个产品设计的完整生命周期中的，事实上已经有如 ISO 9241 这样的系列标准来规范和指导实施。这些标准提供了整套可用性设计的框架和流程，包括评估和测试标准。将类似 ISO 9241 这样的用户体验相关的标准应用到消费类物联网设备的设计之中，是消费类物联网的发展方向之一。

再者，消费类物联网设备应当充分利用收集到的用户使用数据回馈用户，为用户提供更好的使用习惯和体验。消费类物联网设备往往掌握大量用户的使用数据，这些数据可以很好的勾勒出用户画像，从而反过来为用户提供更符合他们使用习惯的服务。但是同样需要注意，这样的交互过程需要充分考虑用户在厂商使用其个人数据上的顾虑，任何的改变或者新的服务都需要提前征得用户的同意，而不能自以为是地做出自认为对用户有利的改变或服务。

最后，改变传统的商业模型，也许也是消费类物联网的发展方向之一。传统场景中，用户需要一次性购买多个设备来实现某一个或某几个生活场景的消费类物联网设备覆盖，对于用户来说这样的一次性消费阈值很高，很可能会降低用户的使用意愿。例如，可以采用类似 Equipment as a Service（EaaS）这样的商业模型，用户只需要按需要租用消费类物联网设备，这样可以降低用户的一次性消费阈值，从而提升用户使用消费类物联网设备的覆盖场景和意愿。事实上，类似这样的模式，已经在其他行业应用很久，比如我们所使用的家庭宽带，我们只是租用宽带设备而不是购买宽带设备。

2.2. 消费类物联市场态势分析

2.2.1. 政策利好促进行业发展

近年来，中国物联网行业受到各级政府的高度重视和国家产业政策的重点支持。国家陆续出台了多项政策，鼓励物联网行业发展与创新，《关于印发“十四五”冷链物流发展规划的通知》《关于开展营商环境创新试点工作的意见》《关于印发物联网基础安全标准体系建设指南（2021 版）的通知》等产业政策为物联网行业的发展提供了明确、广阔的市场前景，为企业提供了良好的生产经营环境。

工信部等八部门联合印发《物联网新型基础设施建设三年行动计划(2021-2023 年)》。目标到 2023 年底，在国内主要城市初步建成物联网新型基础设施，社会现代化治理、产业数字化转型和民生消费升级的基础更加稳固。强调在行业标准体系、网络数据安全、知识产权等方面不断完善提高，支持物联网健康发展。

2.2.2. 科技的突破带动行业赛道跨界合作与竞争

物联网行业发展的内生动力正在不断增强。连接技术不断突破，NB-Iot、eMTC、Lora 等低功耗广域网全球商用化进程不断加速;物联网平台迅速增长，服务支撑能力迅速提升;区块链、边缘计算、人工智能等新技术题材不断注入物联网，为物联网带来新的创新活力。受技术和产业成熟度的综合驱动，物联网呈现“边缘的智能化、连接的泛在化、服务的平台化、数据的延伸化”等特点。各项技术不断突破带动行业不断发展。

随着物联网的快速发展,物联网在生活中的应用越来越广。物联网遍及智能交通、环境保护、政府工作、公共安全、工业监测、个人健康等多个领域。物联网应用领域丰富，市场需求逐渐被释放，市场前景广阔。

在竞争的同时，也伴随着一些风险，某些设备存在收集个人隐私以及处理个人隐私数据的情况。这些数据被用来进行大数据分析，向用户提供定制化的服务以及专有信息推送。虽然方便了用户更快捷地获取自己所关心的信息，但是暴露了个人隐私数据。

2.2.3. 平台生态的发展，进一步丰富应用领域

在智能家居领域，最新推出的 Matter 1.0 协议，使得软硬件解耦，促进智能家居业务模式的变革。因为 Matter 互联标准的到来，使得智能家居的控制软件（APP）和智能家居硬件设备之间，可以实现各自独

立开发。同样，即便是独立开发，在满足用户对智能家居功能以及场景需要的同时，又能够轻松构成一个完整的控制系统。

2.2.4. 技术和产业成熟度的综合驱动，消费类物联网进一步全球化发展

消费物联网的现阶段：以增加设备连接量为主

随着智能硬件品类和 IoT 应用的丰富，物联网向多元的消费场景渗透，所谓智慧生活概念在消费者中的认知度不断提升，消费物联网市场空间巨大。

据 GSMA（全球移动通信系统协会）公布的数据，自 2010 年至 2019 年，全球物联网设备数量的年复合增长率达 22%，2019 年设备连接数量达 120 亿，其中直接面向消费者的设备连接量为 44 亿（智慧家庭 20 亿，消费类电子产品 12 亿，可穿戴设备 3 亿，智能汽车 3 亿，其他消费类产品 6 亿）。综合分析业内参与者的布局，智能家居、可穿戴设备是消费物联网目前的发展重点。[2]

由智能硬件销售向数据服务升级

面向消费者的物联网业务主要包括终端设备销售、平台及设备连接服务、应用与解决方案服务等方面。

具备硬件开发和生产实力的企业具备较好的发展路径，发展初期，企业聚焦重点领域发展自有品牌的核心产品，以智能硬件销售获得用户和营收。随着智能硬件品类的丰富，销量的提升，连接的设备数量增多，设备之间的连接与交互需求也在提升，建设提供设备连接与管理功能的平台是支撑消费物联网业务持续扩展的基础。

为了增强用户粘性，企业进一步发展消费者服务，构建开发平台，为开发者提供开发工具及服务，进而拓展面向消费者的应用及内容服务。智能硬件与应用服务形成合力，汇聚流量，积累用户数据，最终实现数据价值的挖掘。

全球化发展

物联网的发展受到基础设施建设、基础性行业转型和消费升级三大周期性发展动能的驱动。物联网概念兴起至今，庞大市场中各类应用长时间并存，处于不同发展水平的各领域和行业分波次地动态推进物联网发展。当前全球物联网进入了由基础性行业推动的新一轮发展浪潮。

一是利用物联网技术重建工业/制造业竞争优势成为主要推动力量。工业/制造业作为国家的战略性基础行业，具有规模巨大、带动性强的特点，历来是世界各国发展竞争的焦点。通过以物联网为代表的新一代信息技术持续创新并与工业/制造业融合，推动传统产品、设备、流程、服务向数字化、网络化、智能化发展，加速重构发展新体系。

[2] https://www.ydisp.cn/developer/123515.html

另一个巨大的发展动力是市场化的内在增长机制推动物联网行业逐步向规模化消费市场聚焦。对于物联网而言，消费升级带来的物联网智能单品销售持续爆发。物联网能够有效解决行业痛点，催生新的发展热点。物联的趋势使得门锁迫切需要网络化、智能化，安防向预警及主动监测发展。目前以智能门锁、智能单品设备为代表的家居成为这类应用的代表。

3. 与消费类物联网设备相关的安全性挑战

3.1. 与消费类物联网设备相关的安全性挑战

物联网以其广泛的连接性以及智能、自动、便利的交互体验，使其在过去的五年间得以蓬勃发展，然而物联网设备包含大量传感器，收集并传输有关个人生理、周边环境和设备运行的数据，结合云计算、大数据、人工智能、5G 等新兴技术，在为人们提供个人和家庭助理、健康、娱乐、工业控制和其他新用途的同时，也面临着更为复杂和严峻的安全性挑战。

据 SecuringSAM 研究数据，在 2021 年发生的 10 亿次与网络安全相关的攻击中，物联网设备就占据了超过九成。作为互联网的延伸和扩展，针对互联网的攻击手段几乎可以完全应用于物联网设备，物联网新的特征使得安全问题更加突出，主要表现在以下几个方面：

更广泛的安全威胁

“万物互联”的特性使得物联网设备相比于传统 IT 互联网存在更广泛的网络安全攻击面和攻击窗口，如设备电子电气、传输网络及与云端服务的接口，大量数据收集及处理使得数据安全、个人信息及隐私保护问题变成重灾区。物联网打破了对产品安全规则的传统理解，从传统的功能安全向网络安全、数据安全、隐私保护领域漫延，从单一的产品安全对个人的影响，扩散至潜在对社会和国家的数据安全、网络安全影响。2019 年黑客通过定向攻击某运营商的家庭用户设备（家庭物联网控制中心）并植入恶意程序 Pink，使其成为僵尸网络节点，最终造成超过百万台设备被入侵并控制。

安全防护能力与机制缺失

作为新兴的技术领域，技术标准及产品准入准则的缺失，使得产品及服务在开发过程中缺乏对网络安全防护技术的同步规划与防护，未设计和开发应有的安全机制或与设备性质及功能相适应的安全性能，物联网设备自身及关键业务形态（如网络传输、数据采集及处理、隐私）安全隐患突出。物联网设备对互联网及云平台的依赖，拉长了产品的关联边界，产品在销售后直至退役的生命周期阶段也可能面临未知的网络安全威胁。2020 年，研究人员发现某家庭自动化系统智能语言交互控制设备漏洞，漏洞能够让攻击者激活并劫持音箱，攻击者可利用此缺陷获取用户的隐私个人信息，进一步可造成更加严重的财产损失、人身安全。

个人信息及隐私保护泛滥成灾

物联网产品及服务对数字化的增强和不断“更新”的能力，使得在使用过程中个人信息和隐私信息易发生未经授权的访问、破坏、使用、修改或披露等风险。物联网产品及服务的长链条特性，使得在发生安全问题或侵权事件时，个人权益的保护及维权变得困难。2021 年，某汽车销售公司门店在未经过消费者同意的情况下，通过摄像头对进入门店的客流进行统计和分析，包括进店人数、男女比例、年龄分析等个人信息。 2022 年“315 晚会”爆出“儿童电话手表并不安全”，作为家长意图提升孩子生活安全而购买使用的儿童手表也面临着安全风险，通过二维码，后台能在用户无感知的条件下获取到手表的位置、录音、摄像头等隐私信息，甚至能够远程打开摄像头实时观察用户情况。

3.2. 来自消费者（物联网设备用户）意识的挑战

IT 网络和物联网的网络安全意识差异

多年来，互联网用户已经学会了对电脑和手机安全的保护，扫描病毒木马并对可疑短信、邮件保持警惕，在某些行业中工作的用户也会定期接受培训，以应对大多数公司现在面临的网络攻击。 但由于物联网是一项相对新兴的技术，且消费类物联网设备的用户不是技术人员，通常他们并不会意识到自己的物联网设备会引致安全问题，也并不知道他们的设备何时受到损害，因为大部分设备在受到攻击后仍然会正常运行。 因此，设备终端用户成为了安全性中薄弱的一环。事实上，大多数用户在使用个人电脑，平板电脑甚至智能手机时通常具有安全意识，但当使用其联网的健身手环、智能手表、智能汽车、网络摄像头、智能家电时，许多人就会忽略安全问题，他们并不会意识到这些设备上的智能传感器和钓鱼邮件、短信一样，都可能存在潜在的安全风险。

无物联网产品网络安全识别能力

安全风险意识的缺乏让用户在购买、部署和使用物联网设备时均不会考虑太多的安全因素，其中就包括购买缺乏安全认证的设备、使用弱强度的密码、不进行必要的网络安全设置等。

缺失物联网络的安全配置的能力

对任何物联网设备而言，一旦进入了家庭或商业的网络中，它就不再是一个独立的设备，而成为了网络攻击的潜在切入点。但多数用户并不会单独为物联网设备设置防火墙和过滤器，也并不并将其与网络中的其他设备分开，也不会正确地配置安全参数，通常使用默认配置选项，这一系列操作为物联网安全带来了巨大的风险与挑战。

4. 消费类物联网设备相关的法规与标准

4.1. 中国物联网设备相关法规与标准

4.1.1. 中国基础法规和标准

自 2016 年以来，中国网络安全监管体系快速发展，并先后推出一系列法规和标准：

《网络安全法》：[3]我国第一部全面规范网络空间安全管理方面问题的基础性法律，确立了网络安全法规的基本原则，明确了各主体的职责权限、监管体制、义务和责任。

《数据安全法》：规范数据处理活动，保障数据安全，促进数据开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益。在中华人民共和国境内，任何涉及数据处理活动的产品和服务，都需要遵循该法规。

《个人信息保护法》：个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。物联网设备中存储、处理的个人信息均需要满足该法规要求，以进一步加强对数据和个人信息的保护要求。

《数据出境安全评估办法》：在全球化与数字经济的发展背景下，数据作为生产要素在国际间的流动越来越频繁且呈逐年增长趋势。《数据出境安全评估办法》旨在防范数据跨境的无序流动带来的数据主体、数据安全，维护国家安全和社会公共利益。法规明确了数据处理者向境外提供在中华人民共和国境内运营中收集和产生的重要数据和个人信息时的安全评估目的、原则、范围、程序和监督机制等内容。

另外，《信息安全技术-网络安全等级保护基本要求》即“等保 2.0”，对云计算、移动互联网、物联网、工业控制系统等新技术的安全提出了更高的要求，消费类物联网相关的产品和服务也需要遵守此合规要求。

伴随着法规的制定，相关部门推进并编制了物联网领域一系列相关的技术标准。

2018 年，国家市场监督管理总局、中国国家标准化管理委员会发布《GB/T 37025-2018 信息安全技术 物联网数据传输安全技术要求》，提出了物联网数据安全传输模型，明确了基础级和增强级的传输安全技术要求，并给出了数据安全传输安全能力要求和自查表。

2020 年，工业和信息化部批准行业标准《物联网信息系统安全运维通用要求第 1 部分：总体要求》：该标准针对物联网信息系统的安全要求，提出了物联网信息系统安全运维服务能力模型，规定了安全运维服务组织在人员、资源、技术和过程方面应具备的条件和能力，同时从感知层、网络层、应用层三个层面明确了物联网信息系统各分层运维要求。

2021 年，工业和信息化部发布《物联网基础安全标准体系建设指南（2021 版）》，提出到 2022 年初步建立物联网基础安全标准体系，研制重点行业标准 10 项以上，明确物联网终端、网关、平台等关键基础环节安全要求，满足物联网基础安全保障需要，促进物联网基础安全能力提升。到 2025 年，推动形成较为完善的物联网基础安全标准体系，研制行业标准 30 项以上，提升标准在细分行业及领域的覆盖程度，提高跨

[3] http://www.gov.cn/xinwen/2016-11/07/content_5129723.htm

行业物联网应用安全水平，保障消费者安全使用。

同年，由全国信息技术标准化技术委员会归口，由物联网分技术委员会组织制定，发布了 5 项与物联网相关的推荐性技术标准：

GB/T 40684-2021《物联网 信息共享和交换平台通用要求》：规定了物联网信息共享与交换平台的概念和功能要求，功能要求包括数据管理、目录管理、服务支撑、平台管理和安全机制，适用于物联网信息共享和交换平台的设计、开发和实现。

GB/T 40778.1-2021《物联网 面向 Web 开放服务的系统实现 第 1 部分：参考架构》：规定了面向 Web 开放服务的物联网系统的参考架构和功能组件，并对协议适配、物体描述、物体发现、物体共享和安全保障等功能组件进行了描述，适用于面向 Web 开放服务的物联网系统的顶层设计。

GB/T 40687-2021《物联网 生命体征感知设备通用规范》规定了生命体征感知设备外观和结构、功能和性能要求、安全要求、环境适应性、电磁兼容性、可靠性、限用物质限量等要求和试验方法，适用于生命体征感知设备的设计、研发和产品的选型。

GB/T 40688-2021《物联网 生命体征感知设备数据接口》规定了生命体征感知设备数据接口总则、通用接口要求以及通用接口和业务接口的基本功能和参数，适用于生命体征感知设备的设计和研发和产品选型。

4.1.2. 中国相关行业及企业在标准方面的实践

消费品物联网在一些消费细分领域正在快速发展。家具、小家电行业，许多厂商结合第三方物联网解决方案提供商的技术能力，将传统的产品/生产线迅速改造为智能产品和智能产品/生产线，纷纷推出可联网的设备并投入市场，以抢夺行业内的高利润市场。在白家电行业，价格竞争下的成熟市场早已形成，各类家电功用也早已固定，物联网、人工智能等技术的诞生，使得传统白家电厂商发现市场中的新机遇。各大厂商纷纷投入到“白家电互联网+”的研发中。结合传统制造业的能力，白家电厂商正在纷纷推出自身产品的“物联网生态圈”。

基于行业和市场的发展，许多行业/协会也在法规/标准方面进行了一些探索，衍生出了较多的行业标准，如：

中国标准化协会推出了一系列与物联网相关的标准，如《搭载物联网操作系统的智能家用电器技术要求》（T/CAS 520~527—2021）、T/CAS 499-2021《智能家用电器网络安全技术要求和测评方法》等，其中包含家用燃气快速热水器、除湿机、电饭锅、吸油烟机、豆浆机等 8 大类家电产品。

佛山市顺德区智能家居产业联合会推出了一系列智能家居产品的标准（T/SHIF 0001~0004—2022），规定了智能窗帘、智能开关、智能插座以及智能家居产品通用技术要求。

上海市电子电器技术协会在 2019 年就推出了《智能家居产品安全智能门锁安全技术要求》（T/SETEA 000001—2019），随后陆续推出了 T/SETEA 00002~00009 8 项与智能家居、智能户门相关的技术规范和安全

要求。

随着物联网技术在消费品领域的深入，各类行业协会与团体也正在逐步完善对应的行业法规和要求。部分企业也在积极探索消费物联网产品和服务的安全防护，建立内部标准，提升自身产品以及整个产业链的安全能力。

4.2. 国外物联网法规与标准概览

随着消费物联网的技术及产业发展，信息安全、隐私保护等安全问题引起了全球广泛的关注，各国已经开始探索物联网方面的网络安全法规：

欧盟

GDPR《通用数据保护条例》：该法规将数据持有者定义为数据控制者或数据处理者。任何收集欧盟公民数据的人都将被视为控制者，明确了数据控制者和处理者新的义务，以保护欧盟公民的个人数据。物联网设备收集和存储的信息显然属于 GDPR 的管辖范围。

EU Cybersecurity Act《2019 欧盟网络安全法》：《[4]网络安全法案》针对对象主要包括欧盟机构、机关、办公室和办事处等机构（下文统称："欧盟机构"），规制内容主要为上述欧盟机构在处理个人用户、组织和企业网络安全问题的过程中加强网络安全结构、增强对数字技术的掌控、确保网络安全应当遵守的法律规制，旨在促进卫生、能源、金融和运输等关键部门的经济，特别是促进内部市场的运作。

Cyber Resilience Act《网络弹性法案》：[5]法案要求所有连接设备的基线网络安全标准和更严格的关键产品符合性评估程序。具有数字元素的产品（任何软件或硬件产品），其预期或合理可预见的用途是包括有与设备或网络的直接或间接逻辑或物理数据连接的产品都需要满足法规要求，企业将必须证明它们满足网络安全的基本要求，从而将攻击风险降至最低。

英国

Secure by Design：该法规是为物联网（IOT）设备制造商出台的自愿行为准则，旨在保护消费类物联网。确保家用集线器、智能家居设备、安全摄像头、可穿戴设备和连网玩具等设备免受外部攻击和数据泄露。除了在选择过程中对供应商进行更严格的审查之外，内置的、设计安全（secure-by-design）的方法还要求在整个系统或产品的整个生命周期中采用安全的安装和维护措施。

---

[4]EU Cybersecurity Act《2019 欧盟网络安全法》https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.151.01.0015.01.ENG&toc=OJ:L:2019:151:TOC

[5] Cyber Resilience Act《网络弹性法案》，https://digital-strategy.ec.europa.eu/en/library/cyber-resilience-act

美国

CCPA《加州消费者隐私法案》:《加州消费者隐私法案》(CCPA)是继欧盟《通用数据保护条例》(GDPR)颁布后又一部数据隐私领域的重要法律。CCPA 是美国首部关于数据隐私的全面立法(美国之前并没有 GDPR 一类的通用数据保护法律,只在一些特殊行业或领域立法里,有关于隐私保护的内容散落在其中)。根据 CCPA 的规定,消费者主要拥有知情权、访问权、删除权、选择权、公平交易权、个人诉讼权六大权利。CCPA 的出台弥补了美国在数据隐私专门立法方面的空白,它旨在加强加州消费者隐私权和数据安全保护,被认为是美国当前最严格的消费者数据隐私保护立法。

加拿大

PIPEDA《个人信息保护及电子文档法案》:PIPEDA 是一项加拿大联邦法案,适用于加拿大各省份中所有商业活动过程中对个人信息的收集、使用和披露,艾伯塔、不列颠哥伦比亚和魁北克省中的类似省级隐私法案对此法案进行了充分补充。PIPEDA 还适用于个人信息在国际以及省之间的传递。

从目前的国际贸易市场环境观察,各国家/地区对于 IOT 设备的市场准入要求如下:

准入法规要求	地区/国家	适用范围与大致要求
CCC	CHINA	220v 供电产品、家具、玩具等(IOT 设备常见品类);产品基础安全强制性认证
网络安全弹性法案(暂未实施)	EU	具有数字元素的产品(任何软件或硬件产品),其预期或合理可预见的用途是包括有与设备或网络的直接或间接逻辑或物理数据连接的;要求产品具备安全的架构且要求制造商提供安全措施与方案
GDPR	EU	欧盟境内个人的个人数据(覆盖绝大多数 IOT 设备的服务对象);用户个人数据安全性保护
ETSI / EN 303645	EU	详细介绍了广泛接受的有关物联网消费设备安全性的"最佳实践"。 ETSI / EN 303 645 没有采用规定的方式满足其要求,而是以结果为中心,在实施特定于给定产品的安全解决方案时提供很大程度的灵活性
EMC	EU	电子产品;产品电磁兼容性测试
CE-RED	EU	无线电设备及通讯终端;产品无线控制安全指令认证
LVD	EU	低电压产品;产品所有安全规则
UL 62368	US	各种高科技产品(计算器和网络产品,消费性电子产品等);安全规范标准
FCC	US	使用无线电频率装置;产品电磁兼容性认证
ICID	CA	在线上销售(尤其在亚马逊上销售的)的无线电组件产品;产品电磁兼容性认证/测试
MIC	JP	针对信息通讯设备和 ITE 产品及电脑周边办公设备,以及各种无线射频产品;强制性认证
PSE	JP	电气产品;强制性市场准入安全认证
RCM	AUS	电气产品;产品安全规定和电磁兼容要求

物联网的发展以及技术的在整个物联网生态中的不断应用，物联网安全漏洞及问题频发，警示我们应加强物联网产品和服务网络安全的重视，在整个产品生命周期中使用正确的安全设计、验证，加强立法和标准约束并进行必要的合规性测试和产品符合性认证。网络安全风险所带来的法规和技术挑战是深远且全球性的，加强信息安全技术、法规和国际社会紧密合作共同制定网络安全战略，以及统一的合作框架有助于遏制网络安全问题的增加与蔓延。

法规多样化使得企业往往需要遵守不同国家/地区/领域的法规要求。不同法规要求之间的差异，使得企业在生产、销售、售后等环节都面临繁杂的合规挑战。从落地实施层面，企业可能面临法规理解不到位、质量建设过程中资源重复、低效投入等问题。TIC 机构可以针对这些问题向企业提供专业化服务，以帮助企业更准确、更高效地理解法规之间的共性和差异，系统性建立覆盖产品全生命周期的消费物联网产品安全体系。

5. 总结

中国消费类物联网的蓬勃发展，为消费者带来了无限便利，但消费类物联网产品因其面临的应用场景和用户群体的特性，面临着更多的安全挑战，需要政府、制造商、第三方机构和用户个人从安全意识、安全法规、技术措施、应用操作等构建全方面的安全防护才能真正保护个人隐私，避免因信息泄露和其它安全事件造成风险，从而促进消费类物联网健康有序的发展。

5.1. 综述

从政策方面看，国家鼓励物联网行业创新，多项宏观政策利好促进行业发展；从应用场景看，消费类物联网普及率越来越广，几乎覆盖了大部分的生活与工作场景。从技术发展看，行业发展的内生动力不断增强，连接技术不断突破，物联网平台迅速增长，应用领域不断丰富。但与此同时，消费类物联网产品也面临着诸多安全挑战:

消费类物联网涉及到各行各业，是多种力量的整合，其安全问题的产生和危害会影响到众多相关方。需要国家在立法上要走在前面，要制定出适合这个行业发展的安全法规，保证行业的正常发展。虽然以《数据安全法》为代表的相关法规、标准、规范等陆续出台，但深入程度、整体协调性和全面覆盖度仍需进一步加强。

二、消费类物联网产品的连接数量多和易联接特性，使得物联网设备面临广泛的网络安全攻击面和攻击窗口；产品及服务具有长链条特性，人工智能和机器学习等技术使得网络攻击越来越隐蔽，使得安全问题或侵权事件发生时，消费者极易暴露在网络安全风险、财产风险乃至人身安全风险中，个人维权也愈加困难。

三、消费类物联网产品消费者关注点在易用性和便利性上，缺乏对物联网设备面临的网络安全攻击面、攻击路径与攻击手段的认知，亟需简单易用的安全标志指导消费者规避风险。

5.2. 发展的机遇和方向

5.2.1. 消费者的安全期望

（终端）消费者和制造商的信任的基础是哪些？

在购买物联网产品的时候，面对市场上琳琅满目的商品、参差不齐的品质与漫天盖地的宣传，消费者追求品质的前提必然是实现功能、保证安全。在现实中，消费者会以对某个品牌的信任作为选择的基础；而在网络中，身份的信任就成为端与端之间作出交互行为响应的重要依据。

设备的身份是消费者和制造商的信任基础，每个设备都应该有唯一的可识别身份标识，以便于外部设备在建立通信过程中验证各自身份信息，识别非法访问，并对设备行为记录进行管理。因此，身份的保护在网络安全中至关重要。这不仅关乎个人信息与隐私的保护，而且能够应对在缺乏足够的身份验证机制下，智能家居中所面临的多种威胁，例如设备信息被越权访问，联网设备失控，数据被篡改，敏感数据丢失，中间人攻击等等。基于上述原因，为物联网构建信任的架构是相当必要的。

5.2.2. 制造商和供应商应采取的措施

对于物联网企业和供应商，如何应对网络安全风险，处理网络安全事件，既是对技术的重要挑战，也对体系管理提出了诸多要求。行业通用的准则包含以下几点：

一、企业需要从顶层设计信息安全相关政策与战略，明确网络安全管理的必要性与职责。

二、对自身产品进行安全分析，建立威胁模型，明确安全需求及执行计划。

三、根据网络安全需求与计划进行产品设计，执行网络安全活动。

四、对于设计完成产品的网络安全性进行测试与验证。

五、根据测试与验证结果对产品网络安全相关设计进行更改及调整，直至产品通过网络安全的测试及验证。

六、持续跟踪，监控产品在市场上是否存在已知网络安全漏洞或信息泄露风险。

七、对物联网产品网络安全漏洞及信息泄露风险进行分析，修复，并且及时更新系统。

5.2.3. 市场对监管机构的诉求

为确保安全连接的设备以及相关服务和系统，建议监管机构加强的方面

当前，网络安全已成为全球城市治理的热门话题，随着技术的飞速发展，城市的数字化进程在不断加快，居民的衣食住行均享受到了数字化服务所带来的便捷。与此同时，网络安全的威胁也渗透到方方面面，威胁无处不在，针对物联网消费品，其网络安全威胁所带来的危害影响范围已超出产品物理功能本身，且

不能轻易被人感知，因此对政府的治理带来了新的挑战与诉求。当今全球，欧盟对于物联网消费品的网络安全立法与思考走在世界前列；从政府职能上，于 2004 成立的欧盟网络安全局 ENISA 为欧盟网络政策做出贡献，通过网络安全认证计划提高 ICT 产品、服务和流程的可信度，与成员国和欧盟机构合作，并帮助欧洲做好准备应对未来的网络挑战。通过知识共享、能力建设和意识提高，该机构与其主要利益相关者合作，加强对互联经济的信任，增强欧盟基础设施的弹性，并最终确保欧洲社会和公民的数字安全。其职责包括：1. 制订跨部门，包容各方的合作框架；2. 制订网络安全政策；3. 协助企业和政府建设网络安全防御能力，培养相关人才；4. 为企业和政府的网络安全建设提供咨询及解决方案；5. 组织评测机构对于企业和政府网络安全风险进行评估；6. 推动信息交流和知识传播，增强消费者网络安全意识及隐私保护意识。

在具体法规层面，全球政府正在为物联网产品提供切实可行的标准和指南，在标准及指南的制订上，主要体现于以下几个大类文件：网络安全基线要求；隐私保护要求；评估方法；最佳实践指南；企业网络安全架构建设几个方面。在法律法规方面，欧美如 EN 303 645, NIST 8259, GDPR，以及在欧盟具有强制影响力并将于 2024 年对联网设备网络安全评估执行的 RED 指令，目前都受到了全球的关注，并且作为各国网络安全标准及准则的广泛参考。未来，欧盟还将对人工智能相关的网络安全风险制订法律法规，加强执法与监督。在执行方面，全球因触犯 GDPR 及网络安全而面临罚款及通报的企业已屡见不鲜，已引起了物联网消费品制造商的重视，产品的网络安全合规刻不容缓。今后随之法规的陆续出台及案例的明晰，其监管力度可以预见将愈发加强。

5.2.4. TIC 机构的积极作用

在消费者物联网价值链中，TIC 机构（即检验检测认证机构）在各阶段的附加值是什么?

TIC 机构作为产品安全的守护者，在市场中一直发挥着重要作用。

在物联网标准与法规的设计阶段，TIC 机构作为网络安全检测的执行者，具有中立性及权威性，将协助法规制订机构针对具体网络安全风险及威胁给出专业意见，反映市场客观情况。

在产品制造生产阶段，TIC 机构将为企业的网络安全体系建设进行审核，及对产品网络安全风险进行评估。弥合产品与标准差距，提升产品质量，助力产品顺利推向市场。

在市场监管过程中，TIC 机构将协助市场监督管理机构对市场物联网消费品进行抽查及评测，发现市场中具有潜在网络安全风险的产品和行为，在保护消费者权益、促进行业健康快速的发展方面发挥重要作用。

5.3. 中国消费物联网的思考

我国有着全球最大的消费市场，消费升级使得消费类物联网产品出现巨大的需求缺口，消费类物联网产业正处于快速发展时期，而消费类物联网产品的应用对数据隐私与安全性的要求更高，如何保证消费类物联网的用户数据安全性，俨然已成为物联网发展的重要命题，也是用户应用消费类物联网产品的必然要求。

如何遏制威胁、降低风险，不仅是摆在产品制造商、网络方案提供商、云平台服务商面前的问题，更是需要政府监管方面高度重视，第三方 TIC 机构的积极参与。因为在一系列物联网新技术诞生初期，业界的兴奋、激进与政策和监管的滞后往往会形成鲜明的对比。行业的技术力量几乎都在专注于创新。而一旦这种创新与应用开始普及时，新技术所带来的各种风险也就突显出来。消费类物联网产品兼具“物”和“网”两种的属性，在其安全要求上，传统的消费类产品（物）的电气、机械、材料之类属性有着数十年比较成熟的法律法规标准和方案可以沿用，但在信息安全、网络安全和数据安全等新的安全观上，涵盖消费类物联网的全面安全的法律框架近两年才开始构建，新的治理措施越来越受到相关各方的关注。

随着联接的消费类产品的数量显著增加，海量设备里可能暗藏的代码漏洞造成各种网络、实体攻击的潜在点。数据采集、存储、使用、转移、销毁，应用软件的访问控制，多余功能权限，协议安全，OS 安全，代码安全，攻击防护等，这些原本属于互联网安全风险上的专有名词，正逐步显现在消费类物联网产品上，再加上其与人身财产直接相关的属性，情况就变得更加复杂。产业链众多的薄弱环节，必备的传感器带来的数据上云和隐私保护的挑战，既需要规避技术创新带来的潜在危害，又要为技术发展预留出足够的空间，还要保证技术商业化不被政策牵制，包括中国在内的一些产业先发国家的物联网立法也开始构筑，但在落地和实现成效之间还存在一系列待解决的问题。

结合国内物联网安全相关政策、法规、指南等的要求，提出六个方面的思考。一、产业链上下游各相关方共同参与，从设计环节开始就将安全性考虑进来，共同构建消费类物联网可信生态系统，并建立含有物联网安全评估机制的采购政策。二、转“被动防护”为“主动防御”，提升实时监测、分析、应对安全威胁的能力。三、加强供应链风险管理。组织利益相关者沟通物联网安全要求，明确相关责任界面，建立和加强基于风险等级的验证、评估工作。四、加强对消费类物联网设备的安全认证。开展对消费类物联网产品的测评及可信认证工作，发挥独立第三方机构的技术和公信力优势，通过合格评定方式持续提升对物联网平台供应商的安全资质管理，提升对消费类物联网产品性能的专业化确认能力，强化民众对消费类物联网产品的信心。五、加强物联网漏洞信息的披露和处置。政府或行业应建立漏洞信息共享和分析平台，上报解决网络安全漏洞问题的补丁和更新信息，同时鼓励社会力量发现、披露漏洞隐患。六、着眼未来和面向全球构建全球消费物联网的安全体系，以包容协同精神吸纳现有的国际标准并引领新的国际标准的开发，通过全球性消费物联网络，提高国际货物贸易的规模和效率，促进全球经济复苏。

在全球消费类物联网的发展格局中，中国处于增速领先地位，已经基本形成覆盖智能感知、信息传输处理、应用服务的完整产业链，随着政策利好、科技突破和平台生态的发展，共享经济蓬勃发展，"双创"新活力持续迸发，未来几年将迎来巨大的发展。充分发挥第三方认证在消费类物联网安全方面的积极促进作用，消费类物联网市场潜力将加速释放。