联网玩具：
打造安全的现代世界

玩具制造商和零售商电子指南

UL Solutions

Safety. Science. Transformation.™

概述

返回概述

快速安全指南：联网玩具和儿童产品

联网玩具和儿童产品可为各年龄段的儿童带来无尽欢乐，同时激发儿童智力。由于对益智互动联网玩具的需求增长，互联网和物联网 (IoT) 连接可为玩具制造业创造出的潜在优势，可谓前所未有。但用于学习和游戏的电子与无线设备联网也为玩具制造商带来新的挑战。

要为孩子提供学习机会的家长可利用促进 STEM（科学、技术、工程和数学）教育的玩具。某些玩具机器人可让孩子自行设定机器人的动作，教孩子编程基础知识。健身追踪器和智能牙刷等 IoT 设备有助于保持孩子身体健康。

这些数字玩具和设备可为儿童带来诸多优势。

为保护年轻消费者的安全与健康，玩具和儿童产品行业监管格外严格。玩具和儿童产品存在非常特定的安全隐患，因为预期用户可能在按照非预期但可预见的方式来玩用这些产品。可以理解的是，家长也担心孩子的健康与安全。

此外，联网玩具还有更大的潜在风险，包括隐私和安全问题。现在，包含摄像头、麦克风和 GPS 定位器的玩具和儿童产品可对儿童构成前所未有的威胁，而如果玩具最先进的功能只是在外壳上装了可调的手柄，这种威胁根本无法想象。

信息来源：Connected Toys Market – Growth, trends, COVID-19 impact and forecasts (2022–2027) – Mondor Intelligence

联网玩具主要风险

根据投放产品的目标市场，玩具制造商充分了解玩具一贯存在的安全风险（例如窒息危险和锐利边缘），也熟知关键产品的安全要求（包括化学和物理/机械安全）。他们也了解电池安全风险和射频 (RF) 暴露固有风险。然而，联网玩具和儿童产品现在有新的危险隐患（例如数据隐私风险），可能对儿童及其家人同样有害。

为避免 RF 暴露风险，制造商测量自己的联网玩具以及暴露于 RF 源的其他玩具的比吸收率 (SAR)。SAR 是在人体暴露于 RF 电磁场时，每单位质量吸收能量的比率。

在电子玩具由电池或墙插电源供电时，需要评估特定风险才能保持电池安全。例如，在电路板、电机或电池盒导致外露表面温度升至高水平时，就可能在儿童触碰时造成烫伤危险。

现在，让我们关注数据隐私风险，这是一种新型风险，相关法规有时并不明确。

首先要强调的是，黑客可利用此类设备收集有关儿童的以下各种信息：

- 生日、姓名和性别
- 个人资料照片
- 儿童发送的语音消息、聊天消息和图片
- 帐户密码
- 实际位置
- 历史聊天记录
- 互联网浏览历史记录[1]

黑客还可收集有关家长的个人信息：

- 电子邮件地址和邮寄地址
- 性别
- 个人资料照片
- 家长发送的语音消息、聊天消息和图片
- 帐户密码和密码找回问题
- 信用卡信息
- 电话号码
- Wi-Fi 密码和 IP 地址[2]

[1]Nelson, Bill 1942–. 2016. “Children’s Connected Toys: Data Security and Privacy Concerns.” Homeland Security Digital Library. Retrieved April 13, 2017 (https://www.hsdl.org/?abstract&did=797394).

[2]Nelson, Bill 1942–. 2016. “Children’s Connected Toys: Data Security and Privacy Concerns.” Homeland Security Digital Library. Retrieved April 13, 2017 (https://www.hsdl.org/?abstract&did=797394).

UL Solutions

黑客可在产品注册和使用过程中，或通过入侵玩具和儿童产品连接到的家庭 Wi-Fi 系统收集信息。此外，即使消费者的家庭网络安全，在服务器上存储相关数据的联网产品制造商和零售商也可能遭到网络攻击和发生数据泄露。这种情况下，除了制造商和零售商因数据泄露而受刑事和民事处罚之外，消费者对其品牌忠诚度也可能受到致命打击。

消费者还应了解制造商是否以及在多大程度上共享联网玩具收集的数据。即使这种数据共享的目标是改善语音识别等功能，制造商也必须向消费者披露在保留和共享非匿名化数据时存在的固有风险。

美国 1998 年儿童在线隐私保护法案 (COPPA) 针对服务于 13 岁以下儿童的网站或在线服务运营商或将从 13 岁以下儿童收集个人信息的其他网站或在线服务运营商提出了要求。[3] 联网玩具包括在此项法规的适用范围之内。

[3]https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

返回概述

最大限度降低联网玩具和儿童产品风险

包含无线、人工智能 (AI) 和计算组件的玩具和儿童产品存在制造商可能并不熟悉的风险和法规要求。

除了联网玩具和儿童产品安全风险测试之外，制造商还可采取措施降低消费者和品牌面临的其他风险。例如，玩具只应收集运行玩具功能和实现玩具用途必不可少的数据。不得出于任何原因共享或出售此数据。

作为制造流程的一部分，隐私和安全需要纳入玩具设计之内，就像确保人身安全一样。需要增强互通性和安全连接功能，控制玩具配对方式以防未经授权擅自访问玩具和家庭网络。

联网玩具或儿童产品上市前评估测试

无线组件和连接引擎：

包含无线组件或连接引擎的联网产品须满足一整套全新的法规要求，具体取决于所在地区。例如，欧盟无线电设备指令 (RED) 要求多种测试以验证无线设备安全。美国联邦通信委员会 (FCC) 也有类似的监管标准。

要在这些市场中销售无线玩具，公司必须证明自身符合地区要求。了解在每个市场中适用的相关法规是全球市场准入过程中非常艰难而又至关重要的一步。

在此领域内，一些关键的测试包括：

- 电磁兼容性 (EMC) 测试——评估电子设备的能力以确保其在靠近其他电子设备或暴露于电磁辐射的情况下能按预期正常工作。
- RF 测试——有助于确保无线电广播高效利用频谱空间。RF 测试涵盖大多数广播类型，包括 Bluetooth®、Wi-Fi 和蜂窝设备等。
- SAR 测试——测量无线设备附近人体吸收的电磁能量，有助于评估设备是否超过国家规定的 RF 暴露极限。
- Bluetooth® Special Interest Group (SIG) 合格测试——满足要求以使用 Bluetooth® 技术及其知识产权和相关徽标。
- 无线 (OTA) 测试——许多标准组织和无线运营商都要求准确预测实际的无线设备性能。
- 互通性 (IOP) 测试——有助于确保产品正常连接和工作。

返回概述

与任何联网产品都一样，数据隐私和网络安全风险是公司面临的艰巨挑战。消费者最担心的是，网络安全漏洞可能危及最弱势的群体之一，也就是儿童。公司可以采取的明智之举是树立健康的网络安全文化，包括开展充分的网络安全测试和监控，以确定并消除潜在漏洞。在此领域内，一些关键的测试包括：

- 法规要求和标志——根据产品所用技术，必须证明产品符合法规要求才能投放市场，这是赢得品牌信任的关键元素。
- 设计安全——将安全考量纳入组织治理流程，让网络安全上升到产品核心地位，而不是将其轻视为亡羊补牢之举。
- 渗透测试漏洞分析——应用所需标准和最佳方法原则，以确保产品及其辅助服务（例如移动应用程序和 Web 界面）不会成为易受恶意攻击的目标。
- 后端保护——任何云基础结构或后端都需要保护，以解决安全隐患和数据传输隐私问题。

除了设计和制造尽可能安全的玩具和儿童产品这一目标之外，制造商还要应对纷繁复杂、不断变化的全球法规。最重要的是了解全球范围内合规要求对产品有何影响，消除市场准入壁垒并克服国家和地区特定法规的关键挑战，这样才能让联网玩具和儿童产品成功上市。

返回概述

UL Solutions 如何提供帮助

作为全球安全科学专家，UL Solutions 是在安全和性能测试以及第三方认证领域内备受信赖的公司。我们有丰富的经验、遍及全球的设施和深厚的专业知识，可帮助玩具公司应对智能玩具和儿童产品投放市场的复杂性。我们的玩具安全测试可评估您的产品是否符合适用的美国、欧盟及其他国际标准消费者安全规范，以及对 IoT 联网适用的所有安全标准。

我们丰富齐全的测试和认证服务包括 EMC、SAR、产品安全、Bluetooth® 合格、网络安全和无线电测试。如果制造商可证明产品真正采取了“安全第一”方法，那么他们将与家长和孩子建立更牢固的关系。

返回概述

要了解详细信息，请访问 ul.com/smart-toys-solutions

UL Solutions

UL.com/Solutions

Safety. Science. Transformation.™