KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 Eye Street, NW
Suite 1100
Washington, DC 20006

2013年6月1日

联邦贸易委员会
宾夕法尼亚大道西北600号房间H-
113（附件B）华盛顿特区20580

Re：2013年11月关于“物联网”研讨会的评论

民主与科技中心[1]很高兴在联邦贸易委员会（FTC）11月之前提交意见，以响应联邦贸易委员会（FTC）关于物联网隐私和安全方面的意见书[2] 21，2013年研讨会。 我们狭隘地将我们的意见集中在讨论我们建议FTC明确列入11月研讨会讨论的问题的类型以及FTC可能希望邀请参加研讨会的发言人的建议，以便进一步通知讨论。

I. 介绍

物联网（IoT）在联邦电信委员会提交的文件中提到，互联网连接越来越多地集成到家用电器，电表和医疗设备等消费类设备中。[3]此类设备的开发和部署将创建为消费者和公司创造和分析关于技术使用的数据提供了许多新的机会，特别是在高度本地化的私人环境中，例如工作和家庭。

随着公司和监管机构考虑互联网设备对消费者的影响，解决隐私和安全问题将至关重要。 由于家用电器，医疗设备和其他支持互联网的技术可以收集和传输的数据的敏感性，因此嵌入了强大，灵敏和灵活的隐私和安全范例，以及

[1] CDT是一个非盈利的互联网和技术倡导组织，致力于保持互联网和数字生活的开放，自由和创新。 CDT在数字时代推行公共政策，以保护隐私，促进创新并增强公民自由。

[2] “新闻稿：FTC就联邦贸易委员会隐私和安全影响寻求意见”（3013年4月27日），可在以下网址获得：http://www.ftc.gov/opa/2013/04/internetthings.shtm。

[3] 然而，请参阅第II.A部分，就FTC阐述的物联网定义发表意见。

P +1-202-637-9800 F +1-202-637-0968 E info@cdt.org

从产品研发一开始的机制至关重要。 基于公平信息原则，CDT在此之前曾就NIST关于智能电网技术发展的评论提倡强大的隐私和安全实践[4]。由于智能电网技术与互联网技术的可能性相似，我们认为智能电网讨论提出的类似问题将在物联网的背景下提出。 这些问题包括适当保护个人身份信息；对这些设备收集的数据的保留和使用限制；并开发强大的安全措施以防止不需要的第三方访问消费者数据。

尽管新技术带来了希望，使消费者能够创建和监控个人设备的使用情况，但CDT并不认为这些技术带来的问题是全新的。
虽然应用程序可能是新的，但如何保护消费者隐私和安全的根本问题是长期存在的问题。 为此，我们鼓励联邦贸易委员会通过认识到隐私和安全保护必须同时保护用户和鼓励这个有前途的领域的创新，从而采取均衡的方式来监管此类设备。

本评论的其余部分讨论了我们认为在11月的研讨会上有价值的会议类型，以及FTC可能希望邀请的潜在小组成员和发言人的一些想法。

II. 物联网中的突出问题

在本节中，我们将介绍三个具体领域，这些领域将成为11月份研讨会进一步讨论的富有成效的领域：消除物联网，重要的隐私问题和重要的安全问题。

A. 消除物联网的歧义

在FTC征集意见书中[5]，物联网被定义为“日常设备相互之间以及与人交流的能力”。 这是一个非常面向对象和面向对象的框架，涉及更广泛的问题，涉及人们如何与日益充满计算机化和网络化设备，传感器和其他对象的环境进行交互。 有许多重要的相关概念，如“普适计算”，“普适计算”和“环境智能”，每个概念都与物联网具有共同特征。 联邦贸易委员会可能会发现它在未来的调查中有所帮助并且有用，将重点放在这些与平衡隐私，安全和创新有关的领域。 在本节中，我们讨论这些不同观点的重叠。

[4] “对NIST机构间报告草案（NISTIR）7628，智能电网网络安全战略和要求的评论，”民主与技术中心“（2009年12月1日），可在以下网址获取：https：//www.cdt.org/files/pdfs/CDT评论NISTIR 7628草案12-02-09 FINAL - updated.pdf。

[5] FTC新闻稿，同上，fn。 2。

最近一篇旨在调查物联网定义的文章承认，该术语没有商定的定义，并且由于其广泛性和描述性，将以下定义确定为可用的最佳定义："物联网允许人们和需要连接的东西任何时间，任何地点，任何人和任何人，理想情况下使用任何路径/网络和任何服务。 "[6]当然，这与联邦贸易委员会在提交意见书中的表述明显不同。

物联网的所有定义都具有共同点，即它们专注于计算机，传感器和对象如何相互交互并处理数据。 环境智能和无处不在（或普及）计算[7]是与物联网有关的概念。但是，不要将物体相互作用作为参考点，环境智能和无处不在的计算描述人类与物联网的互动方式。 环境智能和无处不在的计算旨在描述用户体验的本质。

一旦物联网在非企业消费者中扎根，环境智能和无处不在的计算呈现了人类如何与其环境中的计算机和传感器进行交互和控制的替代愿景。 这两种参与机制可能并不相互排斥。 正如麦肯锡对IoT的分析所表明的那样，计算机和传感器的响应系统并未融入人类的个人生活中，因此可以不参考环境智能或普适计算来讨论物联网[8]。这是因为与物联网不同，环境智能无处不在的计算是个人用户体验的愿景。

CDT认为，FTC不应只是通过消费者购买的物品和物品来关注物联网，还必须考虑在数据收集和使用方面消费者周围环境无摩擦的力量。 例如，从隐私和安全角度来看，如果没有通知，反馈和技术可配置性，消费者可能对IoT饱和的环境感到不舒服。

---

[6] Charith Perera，Arkady Zaslavsky，Peter Christen和Dimitrios Georgakopoulos，"物联网的环境感知计算：一项调查"，IEEE通信调查与教程杂志，1-44（2013）（即将发表），预印本可在： http：/ / / / 1305.0982 ABS参考（最近访问时间为2013年5月30日）。

[7] 在这里，我们将无处不在的计算和普适计算结合在一起，称其无处不在的计算。 过去，"泛在计算"与我们今天所理解的更相关，因为"移动计算"和"普适计算"更多地是面对无关联网设备之间的互操作性和无缝功能的无摩擦用户体验。 有关有用的讨论，请参阅：Emile Aarts和Boris de Ruyter，"环境智能的新研究观点"，"环境智能与智能环境杂志"，1：5，5-7（2009），可在以下网址获得：
http://boris.borderit.com/docs/JAISE.pdf。

[8] 麦肯锡全球研究院，52-61（2013年），詹姆斯曼尼卡，迈克尔崔，雅克布金，理查德多布斯，彼得比森和亚历克斯马尔斯，"颠覆性技术：将改变生活，商业和全球经济的进步"，可在： http：/ / / / www.mckinsey.com洞察业务 科技/ 颠覆性技术（最后访问时间为2013年5月30日）。

在这方面，在11月的研讨会上举行初始会议可能会有所帮助，该研讨会会询问这个生态系统的哪些部分 – 物联网，无处不在的计算，环境情报 – 各种利益相关方认为FTC应该监测和/或积极参与。

B. 隐私问题

在许多方面，尽管消费者刚刚开始意识到互联网和万维网上的这些活动，IoT将促进密集的数据收集和使用。 熟悉和有争议的追踪和行为分析问题可能会嵌入物联网，可能与其他数据源（如在线行为数据）相结合。 简而言之，当消费者从现在开始购买一盒牛奶五年后，他们可能不会期望或以其他方式知道纸盒将向制造商（和/或分销商）报告信息，例如：使用频率信息（例如，每次消费者打开纸箱时，打开纸箱多久），使用方式信息（例如，如果消费者直接从纸箱中饮用;如果消费者将其用作门挡而不是食品），和/或环境数据（例如，消费者储存他们的牛奶的温度;关于消费者冰箱中的其他种类产品的细节）。 正如“不跟踪”和网页浏览一样，CDT认为，公众的隐私和创新利益之间的适当平衡在于消费者控制的有效机制，以及消费者认为隐私侵入的数据收集和使用的通知。

围绕物联网，无处不在的计算和环境智能的许多讨论考虑将可联网的计算组件和传感器直接插入家庭和工作场所，这些环境享受对隐私的高度期望以及根据4日修正案加强对政府搜索和扣押的访问障碍（以及其他州和普通法保护）。

消费者可以通过配置这些技术解决这些跨界问题，以控制敏感位置的物联网能力传感器和设备传输的数据量和性质。 例如，可以设计家庭或企业的成员可以配置的“中间件”网络设备[9]以选择性地允许或禁止在家庭网络外部进行通信的联网对象。 理想情况下，这样的隐私设备可以轻松识别家庭网络中具有物联网功能的产品所发出的数据，但这依赖于制造商将正确的标签插入其设备可以读取的网络通信中。 这可能需要大量的标准工作和制造商的支持（或立法或监管任务）来支持这种功能。 另一种选择可能是为物联网对象的可联网组件设计标准元素 – 比如拉式标签或屏蔽元素 – 消费者可以激活以切换或禁用网络功能。 鉴于这一点

[9]例如，网络设备 – 一种小型的联网专用计算机 – 连接到从内部网络到网络交换机，有线/ DSL调制解调器等的网络电缆。

家中的活动和区域对任意数据收集（卧室，浴室，儿童区域）特别敏感 – 可能存在一定程度的跟踪和数据使用情况，超过此级别对于这些产品或该行业承诺进行连接和断开连接版本。

在11月的研讨会上，我们建议FTC从学术和行业角度讨论如何在物联网和无处不在计算等领域的隐私控制和响应能力发展以及不久的将来展望。

C. 安全问题

对于包含更复杂可编程组件的物联网对象来说，毫无疑问，它们的设计和实施中存在安全缺陷。 也就是说，计算机科学还没有想出编写没有缺陷的软件的方法，并且需要有更新，冻结，隔离或禁用这些组件的机制。 理想情况下，制造商将支持和更新产品的保质期，但对于一些更耐用或不易腐烂的产品，这将是困难的（Android移动操作系统安全更新的拼凑是有启发性的[10]）。 因此，CDT建议联邦贸易委员会讨论以下替代方案的可行性（前两项不相互排斥）：

- 冻结：也许物联网对象可能会被冻结，导致进一步的软件更新无法进行。 这将允许继续与对象进行网络交互，但不会允许任何可能稍后将功能修改为不期望状态的恶意软件更新。

- 隔离：也许物联网对象可以与外部网络隔离。 这将允许在家庭/企业网络上进行持续的网络交互，但不允许与更大的外部互联网连接或从其连接。

- 禁用：最后，如果给定设备的软件和网络功能不是该设备的功能或操作的基础，则该功能可能完全被消费者禁用。 这意味着使得给定设备成为物联网参与者的软件和网络能力将完全失效；实质上是将互联网从物联网中分离出来。

最后，联邦贸易委员会可能希望在11月份的研讨会中讨论并解决的一个技术性问题是可组合安全问题。 也就是说，当独立设计的设备被集中在一起并用于组合或合成系统时，原始安全保证通常不会

[10] Craig Timberg，“'碎片'让Android手机容易受到黑客，骗子的攻击”，华盛顿邮报，（2013年2月6日），可在：http：//02/2013 articles.washingtonpost.com 06 /商业/ 36942653_1_android的手机，Android的生态系统，Android的设备。

适用于较大的系统[11]由于物联网的精确目的是将大量传感器和设备组装成组合系统，因此很难想象得到的系统与各个组件一样安全。 这在计算机科学中是一个特别困难的问题，并且在过去三十年中一直是一个积极的研究领域。 除此之外，CDT并没有特别的建议，除了鼓励联邦贸易委员会在11月的研讨会上讨论这个问题作为安全讨论的一部分。

III. 一些建议的专家/演讲者

我们对可能的发言人和小组成员提出了几点建议，即FTC可能希望邀请他们参加11月的研讨会。 下面，我们列出了一些在物联网，隐私和安全方面涉及或拥有重要专业知识的人员的名字。

物联网和无处不在计算领域的专家：

- Marco Castillo（Responsys）；
- 亚当格林菲尔德（Urbanscale）；
- Usman Haque（Haque Design + Research）；
- Trevor Harwood（Postscapes.com）；
- Laura James（开放知识基金会，Makespace）与物联网相

关的隐私问题专家：

- 贾斯汀布鲁克曼（CDT）；
- L Jean Camp（印第安纳大学）；
- 约翰·坎尼（加州大学伯克利分校）；
- 彼得太古（佐治亚理工）

与物联网相关的安全问题专家：

- William Arbaugh（马里兰大学）；
- Urs Hengartner（滑铁卢大学）；
- 彼得G.诺伊曼（SRI国际）；

[11] “可以连接两个系统，这两个系统都被认为是安全的，这样复合系统就不安全了。"Daryl McCullough，“无干扰和安全特性的可组合性”，1988年IEEE研讨会论文集关于安全和隐私，（1988），177-186，可在以下网址获得：http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8110&isnumber=427。

感谢您提交意见的机会，请随时与我们联系并提出进一步的问题。

此致

/s/

约瑟夫洛伦佐霍尔
高级技术人员； CDT

/s/

GS Hans
Plesser研究员； CDT

/s/

劳伦亨利
实习生； CDT