Internet of Things
A Vision for the Future

Online Trust Alliance
an Internet Society initiative

The rapid rise in the Internet of Things (IoT) has brought forth a new generation of devices and services representing the most significant era of innovation and growth since the launch of the Internet. IoT solutions are game-changers offering consumers, businesses and governments across the globe countless benefits. From fitness trackers to "smart" thermostats and connected toys to connected cities and healthcare services, society is on the cusp of a new technological era. Leading analysts forecast that 6.4 billion connected devices will be in use worldwide in 2016 and will reach 20.8 billion by 2020. This year alone over 5 million new devices are being connected every day.[1]

"An ecosystem built on trust and innovation, where benefits to society and commerce are realized by prioritizing security and privacy"

As is true with most emerging technologies, challenges remain before these benefits can be fully realized. Nine in ten Americans state that controlling the information that is collected about them is important. At the same time, users' confidence that their data is secure and private is at an all-time low.[2] When it comes to IoT, consumers' fears about security and privacy are cited as the two biggest barriers to IoT adoption.[3]

In many cases, these fears may be justified. Researchers and malicious actors continue to demonstrate ways an insecure IoT device can drive collective harm. While shipping devices "secure-by-default" is a goal, all too many devices have vulnerabilities which could have been prevented.[4] Left unaddressed, IoT devices risk becoming proxies for abuse with a capacity for causing significant disruption.

In order to realize the economic and social benefits IoT can provide, we must address these security, privacy, and governance issues holistically. This will require innovation, leadership, and collaboration. If all stakeholders can come together and achieve consensus, the benefits will be fourfold: not only will they realize economic growth, but they will also keep regulation at bay, increase the resiliency of critical infrastructure and help bring IoT to scale.

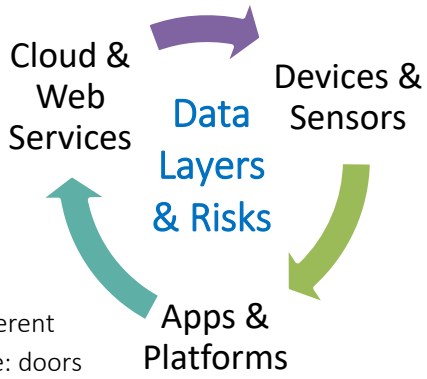
The Online Trust Alliance (OTA) believes that by fostering a public-private dialog we can overcome these challenges and create a safer and more trustworthy connected world. OTA has been a convener bringing together developers, vendors and policymakers to proactively address these challenges, developing best practices, standards and benchmark research.

Working with all stakeholders, OTA is committed to promoting innovation and the vitality of online services, while enhancing online trust and empowering users. With over a decade of public policy, internet governance, standards and deep technology expertise, OTA helps stakeholders anticipate and address potential risks, while helping make security and privacy core to their value proposition.

UNIQUE CHALLENGES

IoT security requires a nuanced understanding of its unique characteristics. First, the IoT ecosystem is made up of three dimensions: the device or sensor, the supporting applications, and the backend / cloud services.[5] Combined with the supply chain of each, every facet and data layer is a potential risk.[6]

Each IoT dimension needs to be secured across multiple layers. As they communicate with, and rely on each other, each data flow must be secured. As more and more cases of data breaches, identity theft, and state sponsored espionage come to light, consumers and businesses alike are becoming increasingly reticent about sharing their personal and business data. Companies will need to demonstrate that they are prioritizing privacy through responsible practices. By embracing transparent data collection, use, sharing and ownership principles, collectively we can bring IoT to scale.



Understanding complex relationships and knowing who is responsible for their protection is key to securing almost all systems. What makes IoT different is that actions are executed in the physical—as opposed to digital—sphere: doors are unlocked, temperatures are lowered, insulin is delivered, and fire suppression systems activated. If the integrity of the data or device is compromised, connectivity interrupted, or the functionality remotely controlled by a malicious actor, the consequences can be catastrophic.

IoT SUSTAINABILITY

Incorporating security and privacy protections in the earliest stages of design and development is the most effective way to bring secure IoT devices to market and help ensure their safety tomorrow. The processes, technologies, and policies that protect users require ongoing support throughout the device's—and the data's—life cycle. Supportability post-warranty (including usability, patch management, data ownership and portability) must be addressed. Defined as "sustainability", it is the risk and implications of devices left unpatched, orphaned, or bricked which is critical to realizing the promise of IoT. Sustainability also includes the policy, governance and regulatory issues related to the ownership and transferability of the device and user data. Since devices may outlive an owner or be transferred to new home buyers, consumers and businesses need the assurance that companies will continue to address these needs after the expiration of their traditional warranty. At the same time, it is important to recognize first, there is no perfect security and privacy; and second, that technology has a lifespan, and there will be a sunset, an end-of-life for support for all devices.

Continuing use of out-of-date devices abandoned by their manufacturer will render them insecure and at risk of being targeted and exploited. Case in point is Windows XP. In spite of Microsoft's providing Windows XP users no-charge support for over a decade, today millions of these devices remain in use and at risk.[7] Not unlike driving a Model T automobile on a highway today, such devices limited by their hardware architecture can no longer be secure on today's digital highway. Unfortunately, while such solutions may ship secure, no degree of patching can address design limitations against unforeseen threats decades later.

To help insure sustainability, companies are increasingly considering a service or subscription model to provide long-term support, security and functional updates over the life of a product, after an initial period of no-charge support. Offering ongoing support will allow companies to take the lead on incorporating sustainability into their business models and demonstrate a long-term commitment to users' security and privacy, while offering added functionally, services and compatibility.

While realizing there is no one-size-fits-all solution, the scope and commitment to sustainability is a decision every company must evaluate. Anticipating these needs and costs is critical to a company's financial model and ability to support customers in the future. Accurately communicating this commitment to consumers prior to purchase is good business, setting realistic expectations and helping protect one's brand and reputation. These security and privacy challenges are faced by all stakeholders, but can easily be addressed. By working together and taking the lead on transparency, security and privacy, we can build the trust that's needed for IoT to reach its true potential.

THE IoT TRUST FRAMEWORK

Users' confidence in entities' ability to keep data secure and private is declining, making it increasingly difficult to convince users to share their information. Ironically, in many cases it is this very data that provides the value for IoT solutions. Fair and open exchanges between companies and consumers will help both understand where the benefits and obligations for IoT lie.

If individuals and businesses cannot trust that their personal and proprietary data will be kept secure and private, large-scale adoption of IoT will not be realized, and calls for regulatory legislation will increase. Already, European Union lawmakers are considering rules that may require companies to go through a certification process to meet new security standards and guarantee user's privacy.[8]

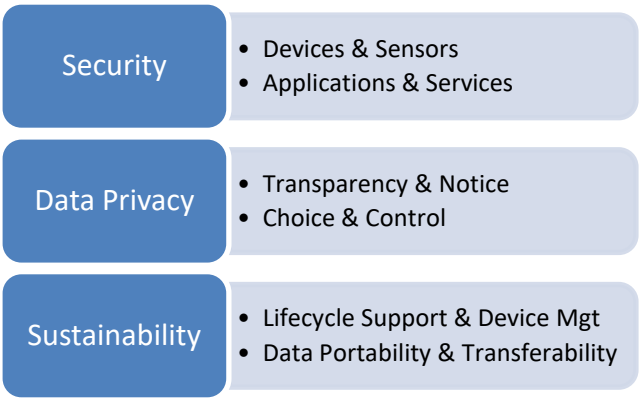
To address these combined issues, OTA convened a cross industry working group with the vision to create an IoT Trust Framework, a voluntary self-regulatory model.[9] Through an 18-month, consensus driven process with over 100 stakeholders, OTA identified 31 criteria initially focused on the connected home, office and wearable technologies. Serving as a voluntary code of conduct, today the Framework is serving as the foundation for several IoT certification and risk assessment programs which are envisioned to provide the basis for future "safe harbor" initiatives.[10]

These measurable criteria empower companies to help assess their risk and address security and privacy head-on, becoming stewards and champions of the critical IoT elements users value. By leveraging this Framework and other OTA resources, companies can demonstrate they are committed to a safe and trusted IoT future.

The Framework provides a path to meaningful self-regulation. If the private sector can demonstrate its commitment to security and privacy, government will be less compelled to regulate and innovation will flourish. Externally imposed regulations, rather than best practice and standards generated through stakeholder consensus, can lead to a culture of compliance—which is inefficient and insufficient for everyone.

WORKING TOGETHER - DRIVING TRUST & INNOVATION

The future of IoT is bright, but it cannot be realized without concurrently addressing security and privacy. Over the next decade, they will become key criteria that consumers, businesses, industry and government will require. Securing and protecting the things that matter most—our systems, our data, and our privacy—is a shared responsibility.



While the industry will evolve and embrace interoperability and platform standards, it also needs to integrate core trust principles. These cannot be bolted on mid-flight, and instead must be designed in from the onset. Creating a culture of security, privacy and sustainability with transparency will yield long-term benefits to society.

OTA provides a forum for stakeholders to confidently discuss ideas, policies, technologies and practices so that, together, we can create consensus by which the industry can—and should—operate. Through OTA's consensus-driven process, we help our members develop best practices and advance balanced public policy. Through working groups and strategic relationships with subject matter experts in interactive marketing and advertising, technology, privacy and public policy, OTA provides strategic insights helping members prosper and innovate as thought leaders while avoiding potholes and roadblocks.

OTA is an initiative within the Internet Society (ISOC), a 501c3 charitable non-profit with the mission to promote the open development, evolution, and use of the Internet for the benefit of all people throughout the world. OTA's mission is to enhance online trust, user empowerment and innovation through convening multi-stakeholder initiatives, developing and promoting best practices, responsible privacy practices and data stewardship. To learn more visit https://otalliance.org and https://www.internetsociety.org/.

© 2017 Online Trust Alliance. All rights reserved.

[1] Gartner IoT Forecast http://www.gartner.com/newsroom/id/3165317

[2] Pew Research Center. (2015). Americans' attitudes about privacy, security and surveillance http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

[3] Accenture 2016 Consumer Survey https://www.accenture.com/us-en/insight-ignite-growth-consumer-technology

[4] OTA Research September 8, 2016 https://otalliance.org/IoTvulnerabilities

[5] National Institute for Standards & Technology "Networks of "Things." http://doi.org/doi:10.6028/NIST.SP.800-183

[6] Symantec Internet Security Threat Report, April 2016. https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

[7] Windows XP Support https://support.microsoft.com/en-us/help/14223/windows-xp-end-of-support

[8] EU Commission https://www.euractiv.com/section/innovation-industry/news/commission-plans-cybersecurity-rules-for-internet-connected-machines/

[9] OTA announced IoT Working Group May 2015 https://otalliance.org/oTWGannounce

[10] RSA Conference Framework Release March 2, 2016 https://otalliance.org/IoTFW-release

r10-25