



# IoT Security Upgradability and Patching

# OTA Global Collaboration





# Challenges - IoT Ecosystem

- Highly personal, dynamic, persistent collection and transfer of data
- Combination of devices, apps, platforms & services
- Data flows, touch points & disclosures
- Lack of defined standards
- **Security**
- **Privacy**
- **Sustainability**
  - Lifecycle Supportability
  - Data retention / ownership



# IoT Trust Framework

---

- Multi-stakeholder working group
- 18 month, consensus driven process

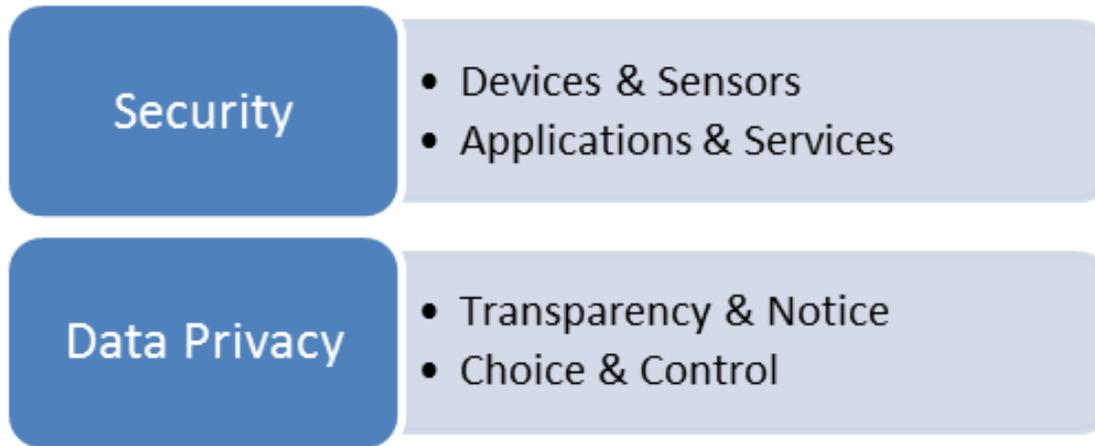
Security

- Devices & Sensors
- Applications & Services

# IoT Trust Framework

---

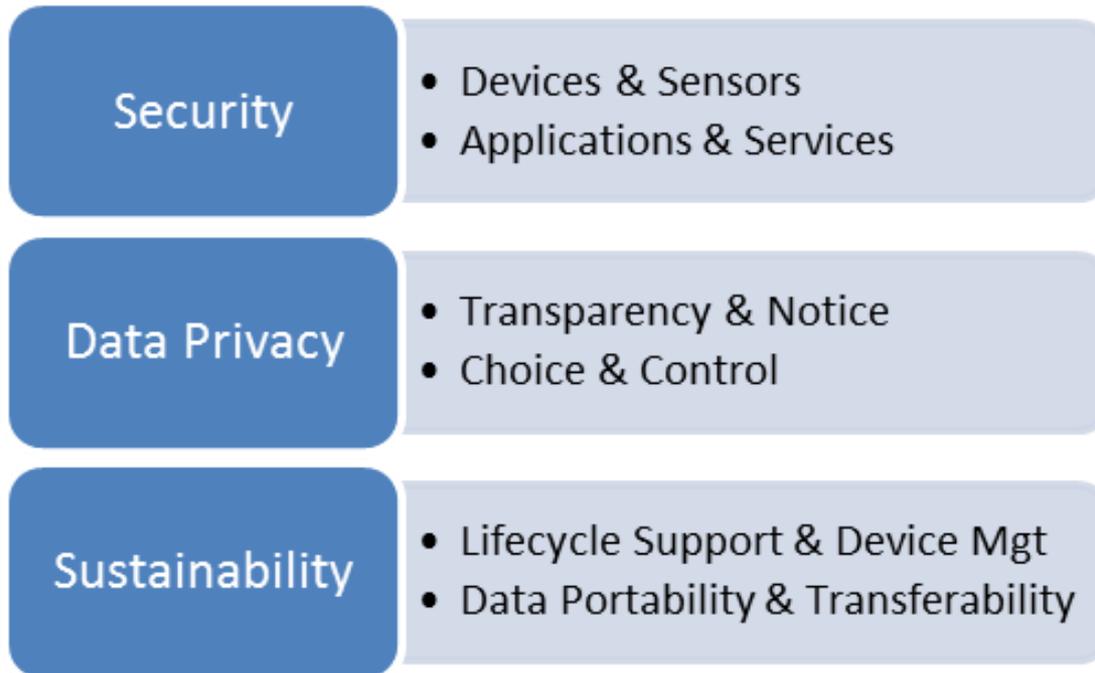
- Multi-stakeholder working group
- 18 month, consensus driven process



# IoT Trust Framework

---

- Multi-stakeholder working group
- 18 month, consensus driven process



# IoT Vision For The Future

“An ecosystem built on trust and innovation where benefits to society and commerce are realized by prioritizing security, privacy and safety.”

## Internet of Things A Vision for the Future



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.<sup>1</sup>

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

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.<sup>2</sup> When it comes to IoT, consumers’ fears about security and privacy are cited as the two biggest barriers to IoT adoption.<sup>3</sup>

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.<sup>4</sup> 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.



# Usability & Functionality

## English man spends 11 hours trying to make cup of tea with Wi-Fi kettle

Data specialist Mark Rittman spent an entire day attempting to set up his new appliance so that it would boil on command



Mark Rittman set about trying to make a cup of tea at 9am but night had fallen by the time his new Wi-Fi enabled kettle could complete the task. Photograph: Alamy

All [Mark Rittman](#) wanted was a cup of tea. Little did he know he would have to spend 11 hours waiting for his new [hi-tech kettle](#) to boil the water.

Rittman, a data specialist who lives in Hove, England, set about trying to make a cup of tea around 9am. But thanks to his [Wi-Fi](#) enabled kettle it wasn't long before he ran into trouble.



**Mark Rittman**  
@markrittman

[Follow](#)

My work is done. And now onto everything else I meant to do today, after that first cup of tea.

4:11 PM - 11 Oct 2016

← ↻ 62 ❤️ 163

Although some people following Rittman's progress - justifiably - was wrong with the old technology.



**ready 4 december**  
@onekade

[Follow](#)

@markrittman why don't you just get normal  kettle

6:46 AM - 11 Oct 2016

← ↻ 61 ❤️ 218



**Michael Laccetti**  
@mlaccetti

[Follow](#)

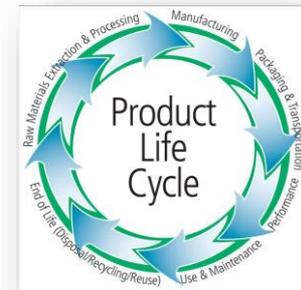
@markrittman At this point, I'm desperate to avoid this future at all costs.

11:15 AM - 11 Oct 2016

← ↻ 34 ❤️ 159

# IoT Trust Framework - Addressing

- Security
- Privacy
- Sustainability / Lifecycle Issues



**IoT Trust Framework ● Required ○ Recommended N/A – Not Applicable**

1. Ensure devices and associated applications support current generally accepted security transmission protocols. All personally identifiable data in transit and in storage must be encrypted using current generally accepted security standards. This is including but not limited to wired, WI-FI, and Bluetooth connections.	●
2. Authentication credentials including but not limited to user passwords shall be salted, hashed and/or encrypted.	●
3. All IoT support web sites must fully encrypt the user session, from the device to the backend services. Current best practices include HTTPS or HTTP Strict Transport Security ( <u>HSTS</u> ) by default, also known as AOSSL or Always <u>On</u> SSL.	●
4. IoT support sites must implement regular monitoring and continual improvement of site security and server configurations to acceptably reduce the impact of vulnerabilities. Perform penetration tests at least annually.	●
5. Establish and maintain processes and systems to receive, track and promptly respond to external vulnerabilities reports from third parties including but not limited to customers, consumers, academia and the research community. Remediate post product release design vulnerabilities and threats in a publicly responsible manner either through remote updates and/or through actionable consumer notifications, or other effective mechanism(s).	●
6. All software and/or firmware updates, patches and revisions must either be signed and/or otherwise verified as coming from a trusted source. Updates and patches should not modify user-configured preferences, security, and/or privacy settings without user notification.	●
7. Ensure all IoT devices and associated software, have been subjected to a rigorous, standardized software development lifecycle process including unit, system, acceptance, regression testing and threat modeling, along with maintaining an inventory of the source for any third party/open source code and/or components utilized. Employ generally accepted code and system hardening techniques.	●
8. End-user communications including but not limited to email and SMS, must adopt authentication protocols to help prevent spear phishing and spoofing. Domains should implement SPF, DKIM and DMARC, for all security and privacy related communications and notices as well as for parked domains and those that never send email.	●
9. For email communications within 180 days of publishing a DMARC policy, implement a reject policy, helping ISPs and receiving networks to reject email which fail email authentication verification checks.	○
10. IoT vendors using email communication must adopt transport-level confidentiality including generally accepted security techniques to aid in securing communications and enhancing the privacy and integrity of the message.	○
11. For user access, provide unique, system-generated or single use passwords; or alternatively use secure certificate credentials. As necessary, require use of unique passwords for administrative access, delineating between devices and services and the respective impact of factory resets.	●

**IoT Trust Framework** ● Required ○ Recommended N/A – Not Applicable

12. Provide generally accepted recovery mechanisms for IoT application(s) and support passwords and/or mechanisms for credential re-set using multi-factor verification and authentication (email and phone, etc.) where no user password exists.	●
13. Take steps to protect against 'brute force' and/or other abusive login attempts (such as automated login bots, etc.) by locking or disabling user and device support account(s) after a reasonable number of invalid log in attempts.	●
14. Provide users notification of password reset or change utilizing secure authentication and /or out-of-band notice(s).	●
15. Enact a breach response and consumer notification plan to be reevaluated, tested and updated at least annually and/or after significant internal system, technical and / or operational changes.	●
16. Ensure privacy, security, and support policies are easily discoverable, clear and readily available for review <u>prior</u> to purchase, activation, download, or enrollment. In addition to prominent placement on their website, it is recommended companies utilize <u>QR</u> Codes, user friendly short URLs and other similar methods.	●
17. Disclose the duration of security and patch support, (beyond product warranty). Such disclosures should be aligned the expected lifespan of the device.	●
18. Conspicuously disclose what personally identifiable and sensitive data types and attributes are collected and how they are used, limiting collection to data which is reasonably useful for the functionality and purpose for which it is being collected. Disclose and provide consumer opt-in for any other purposes.	●
19. Disclose what features will fail to function if connectivity becomes disabled or stopped including but not limited to the potential impact to physical security.	●
20. Disclose the data retention policy and duration of personally identifiable information stored.	●
21. IoT devices must provide notice and/or request a user confirmation when initially pairing, onboarding, and/or connecting with other devices, platforms or services.	●
22. Publically disclose if and how IoT device/product/service ownership and the data may be transferred (e.g., a connected home being sold to a new owner or sale of a fitness tracker).	●
23. Only share consumers' personal data with third parties with consumers' affirmative consent, unless required and limited for the use of product features or service operation. Require third party service providers are held to the same polices including holding such data in confidence and notification requirements of any data loss/breach incident and/or unauthorized access	●
24. Provide controls and/or documentation enabling the consumer to review and edit privacy preferences of the IoT device including the ability to reset to the "factory default."	●
25. Commit to not selling or <u>transferring</u> any identifiable consumer data unless it is a dependent part of the sale or liquidation of the core business which originally collected the data, providing the acquiring party's privacy policy does not materially change the terms. Otherwise notice and consent must be obtained.	●
26. Provide the ability for a consumer to return a product without charge after reviewing the privacy practices that are presented prior to operation, provided that such terms are not conspicuously disclosed prior to purchase. The term (number of days) for product returns shall be consistent with current exchange policies of the retailer, or specified in advance.	●

IoT Trust Framework ● Required ○ Recommended N/A – Not Applicable	
27. Whenever the opportunity is presented to decline or opt out of any policy, the consequences must be clearly and objectively explained, including any impact to product features or functionality. It is recommended the end-user value of opting in and/or sharing data be communicated to the end-user.	●
28. Comply with applicable international privacy, security and data transfer regulatory requirements. <sup>1</sup>	●
29. Publicly post the history of material privacy notice changes for a minimum of two years, including date stamping, redlines, and summary of the impacts of the changes.	○
30. Provide the ability for the user or proxy to delete, or make anonymous personal or sensitive data stored on company servers (other than purchase transaction history) upon discontinuing, loss, or sale of device.	○
31. Provide device or service data erasure and zeroization in the event of transfer, loss or sale.	○

Updates to the Framework, and supporting resources are posted at <https://otalliance.org/IoT>

**Terminology, Definitions & Clarifications**

1. Unless specified otherwise, the terms device manufacturers, vendors, application developers, service providers and platform operators are all indicated by the term “Companies.” The inclusion of platforms is paramount as the IoT may be headed to a future where platform and OS providers and their respective connected ecosystems communicating on a seamless network may pose security and privacy risks.
2. It is expected companies disclose of sharing data with law enforcement and reference any applicable transparency reports as legally permitted.
3. Smart devices refer to devices (and sensors) which are networked and may only have one-way communications.
4. Smart Cars including autonomous, self-driving vehicles as well as medical devices and HIPPA data<sup>2</sup> are beyond the scope of the Framework, yet the majority of the criteria are deemed to be applicable. Respectively they fall under regulatory oversight of the National Highway Traffic Safety Administration (NHTSA) and the Food and Drug Administration, (FDA).<sup>3</sup>

- Examples: EU-US Privacy Shield Framework [www.commerce.gov/privacyshield](http://www.commerce.gov/privacyshield)
- EU General Data Protection Regulation (GDPR) [www.eugdpr.org](http://www.eugdpr.org).



# #6 Updates & Lifecycle Patching

---

- All software and/or firmware updates, patches and revisions must either be signed and/or otherwise verified as coming from a trusted source.
- Updates and patches should not modify user-configured preferences, security and/or privacy settings without user notification.
- Examples: Nest, Vizio



# Related Key Principles

---

#8 – Secure customer communications

How can you inform customers an upgrade is required?

#16 – Ensure support policies are easily discoverable up front  
What statement is made about support? Warranty ≠ Support

#17 – Disclose duration of security and patch support  
Should align with expected lifetime of the device

#22, #30 – Provide ability to delete or transfer data upon EOL/transfer  
Likely require ability to patch/upgrade when device transferred.

- All of this must be done in a manner reasonably achievable by average consumers