Online Trust Alliance
an Internet Society initiative

IOT TRUST BY DESIGN

The OTA IoT Trust Framework

The advent of connected things in our day-to-day lives brings the promise of convenience, efficiency and insight, but also creates a platform for shared risk. Gartner projects that more than 20 billion devices will be connected by 2020. Ranging from fitness trackers to smart thermostats, locks and appliances, this Internet of Things (IoT) represents a massive market and will ultimately redefine how people interact with the world around them.

Consumer confidence is critical for IoT to thrive and grow, yet many of today's products and services are rushed to market at the lowest possible cost with little consideration for basic security and privacy protections. This introduces various levels of risk to both users and the Internet itself – from unwitting surveillance and data compromise to physical risk (e.g., smart locks) to security cameras used as part of a botnet to attack the Internet. By default, many collect vast amounts of personal and sensitive information which may be shared and traded on the open market. The majority of these devices do not have the functionality (or an easily discoverable method) to easily remove one's personal data.

In the absence of adoption of security norms and responsible privacy practices we are reaching a crossroads where regulation may be required. Yet in reality legislation by itself will not be effective. Passing regulation will take too long and will never keep pace with the evolving threat landscape.

In response, more than a hundred stakeholders representing industry, government and consumer advocates contributed to a recommended set of core actions as part of the Online Trust Alliance (OTA), which is now an initiative of the Internet Society. Adoption of this IoT Trust Framework raises the level of security for IoT devices and related services to better protect consumers and the privacy of their data. The Framework serves multiple purposes since it:

- Guides manufacturer and service provider design and business policy choices from initial design through the entire product lifecycle,
- Provides purchasers and distribution channels with the appropriate filters to assess privacy and safety, and
- Gives policymakers the necessary security principles for informed advocacy and economic policy.

Though there are other IoT-related frameworks, this IoT Trust Framework is unique in two significant ways:

- **It covers security, privacy and long-term sustainability (lifecycle) issues.** Many others focus just on security or interoperability or privacy, and few take into account the lifecycle issues associated with these products and services, such as how to transition data and accounts associated with a smart home or what to do when software upgrades are no longer available for a long-lived device such as a garage door opener.
- **It holistically addresses the entire ecosystem**. This includes devices/sensors, mobile apps and backend services. Most frameworks focus on just the devices, but a system is only as strong as its weakest link.

Online Trust Alliance
an Internet Society initiative

The Framework includes a list of actionable principles in eight categories. If followed, these principles can reduce security and privacy risk, increase trust and enable the IoT ecosystem to thrive:

- **Authentication –** authenticate devices and users to prevent malicious access.
- **Encryption –** comprehensively encrypt data to prevent eavesdropping or access to sensitive data.
- **Security –** security must be incorporated in all areas – devices, apps and backend services, whether offered directly or through third parties. Regular testing and updates should be performed to minimize vulnerabilities.
- **Updates –** inform purchasers about device updatability and deliver those updates securely with minimal user intervention or impact (e.g., requiring reconfiguration).
- **Privacy –** clearly disclose privacy-related policies such as data collection and sharing, and limit collection to that required to support functionality.
- **Disclosures –** thorough, easily discoverable disclosures covering privacy policies, data collection, functionality with or without connectivity and duration of support/patching enable informed consumer decisions.
- **Control –** consumers have choices and control regarding the data collected by the device/service and the ability to transfer or wipe the data upon loss or sale.
- **Communications –** consumer communications after purchase (e.g., update/support information) need to be proactively established and secured using best practices to limit social engineering attacks.

Ensuring proper levels of security and privacy for IoT products and services is a collective responsibility. The Framework principles can be used by a wide range of stakeholders to fulfill their role in protecting users and the Internet:

- **IoT vendors and their supply chain** – by following these principles, vendors can increase market confidence in IoT solutions. To raise awareness and highlight leaders prioritizing consumer security and privacy, the Internet Society is asking vendors to publicly commit to the Framework principles.
- **Distribution channels (bundled offerings, retailers) –** the Framework principles can be used as a filter to determine which products to carry, ensuring better security and privacy for purchasers. The Internet Society is also asking for public commitment by these stakeholders to only offer products that support Framework principles.
- **Policymakers and government agencies –** the Internet Society is asking that Framework principles be used to guide policies, laws and regulation associated with consumer-grade IoT products and services to reduce security and privacy risk for consumers and enterprises. Governments, as large procurers of IoT solutions, can also use the Framework as a foundation for purchasing requirements.
- **Consumer testing and product review organizations –** the Internet Society is asking that the Framework principles be incorporated into the testing and review processes. This will raise consumer awareness of their security and privacy choices and promote better buying decisions.
- **Consumers and enterprises –** consumers and enterprises can use the Framework principles as a guide for making informed choices. To facilitate this, the Internet Society has provided consumer and enterprise checklists that summarize key principles.

In summary, the promised convenience, efficiency and insight of a connected Internet of Things is threatened by unnecessary risks introduced via insufficient security and privacy in most of today's IoT products and services. The Internet Society's IoT Trust Framework identifies the core requirements manufacturers, service providers, distributors/purchasers and policymakers need to understand, assess and embrace for effective security and privacy as part of the Internet of Things.