



PANEL DISCUSSION  
THE INTERNET OF THINGS (IOT)  
SECURITY CHALLENGE: PROTECTING  
CRITICAL ASSETS AT MASSIVE SCALE

Craig Spiezle

Executive Director & President



<https://otalliance.org/IoT>

[liveworx.com](http://liveworx.com) | #LIVEWORX



FEB 17, 2016 @ 10:26 AM 6,150 VIEWS

## Samsung Fails To Secure Thousands Of SmartThings Homes From Thieves

**Thomas Fox-Brewster**, FORBES STAFF  
*I cover crime, privacy and security in digital and physical forms.*  
[FOLLOW ON FORBES \(168\)](#)    

[FULL BIO](#) ▾

When Samsung bought Internet of Things (IoT) startup SmartThings for \$200 million in 2014, it wanted to incorporate the latter's hub into its growing "smart home" business. That meant it inherited all the good and bad in the technology, including vulnerabilities

## Exec fears predators can reach kids through new Barbie

By **Kevin Dugan** January 16, 2016 | 1:36am



## ASUS Settles FTC Charges That Insecure Home Routers and "Cloud" Services Put Consumers' Privacy At Risk

**FOR RELEASE**

February 23, 2016

**TAGS:** [deceptive/misleading conduct](#) | [Technology](#) | [Bureau of Consumer Protection](#) | [Privacy and Security](#) | [Consumer Privacy](#) | [Data Security](#)

Taiwan-based computer hardware maker ASUSTeK Computer, Inc. [has agreed to charges](#) that critical security flaws in its routers put the home networks of hundreds of risk. The administrative complaint also charges that the routers' insecure "cloud" services expose thousands of consumers' connected storage devices, exposing their sensitive pers



**Consumer Electronics Mobility Security**

## Wearables, apps disclose user passwords and location: Symantec

Nector Arlano

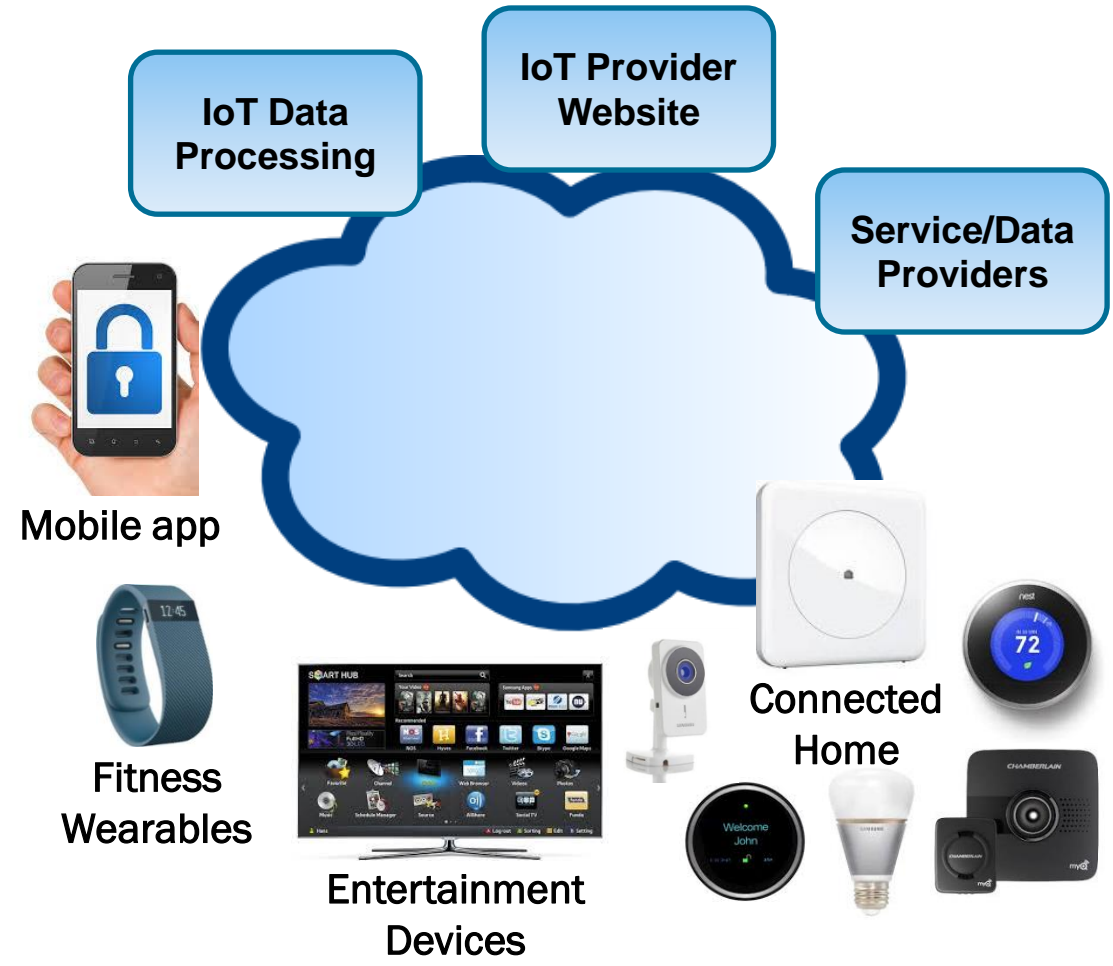
- 93% of adults say that being in control of who can get access to their information is important.
- 90% do not wish to be observed without their approval.
- 88% say it is important that they not have someone watch or listen to them without their permission. <sup>1</sup>
- **47% of respondents pointed to security and privacy as obstacles to adopting such technology.**
- **18% quit using IoT devices due to lack of service guarantees. <sup>2</sup>**

<sup>1</sup> Pew Research Center, 2015

<sup>2</sup> Accenture Research 1/2016, n = 28,0000

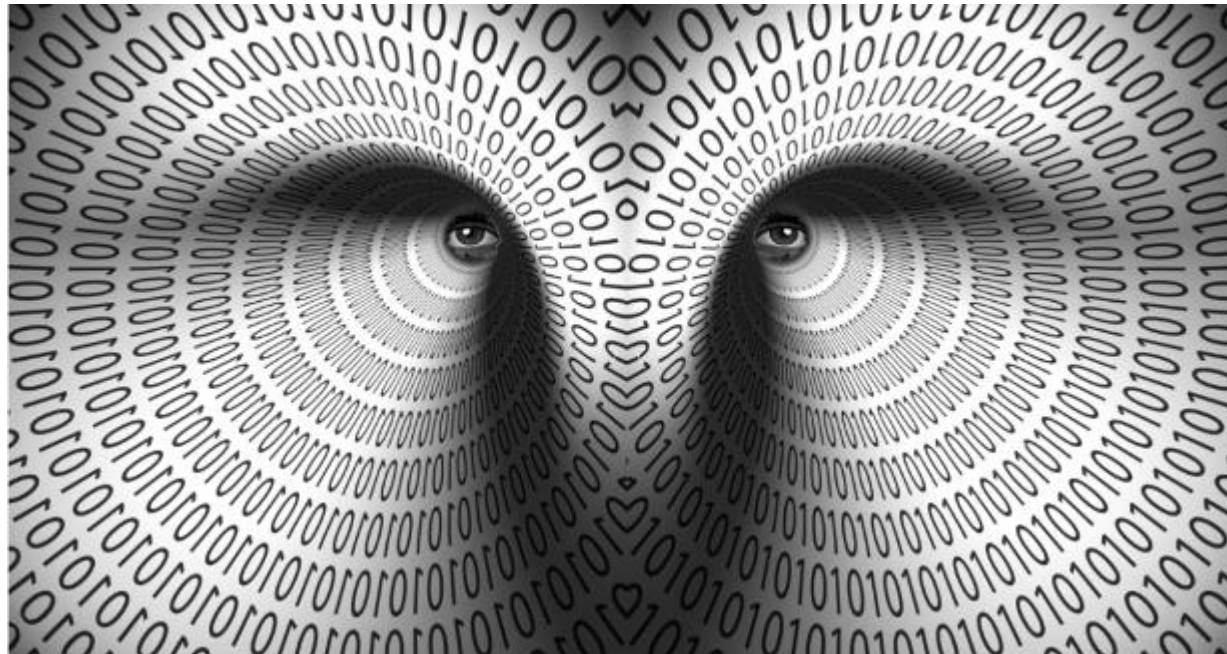
# CHALLENGES - ECOSYSTEM

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



# CHALLENGE - AMBIENT DATA COLLECTION

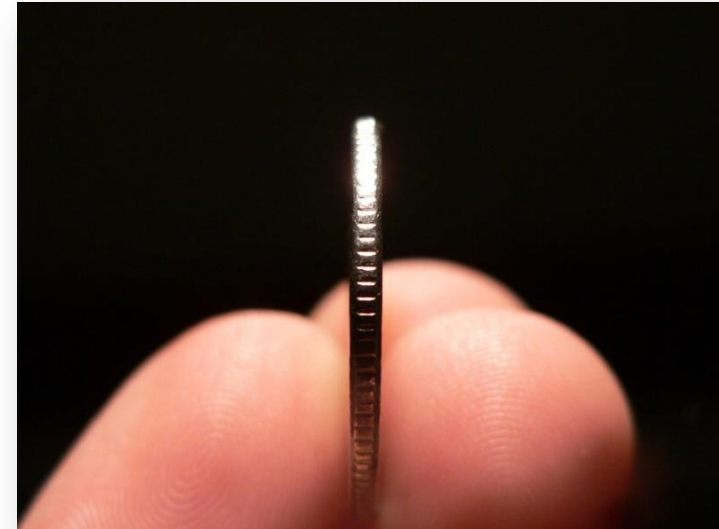
- Growing number of devices & sensors
- Sharing with unknown/undisclosed third parties
- May be “benign” today, but harmful tomorrow



# OVERVIEW – IOT TRUST FRAMEWORK



- Focused On:
  - Connected Home
  - Wearable Tech
- Developed a Code of Conduct
  - Foundation for certification
- 30 Principles Addressing Baseline:
  - Security
  - Privacy
  - Sustainability *from purchase to “end-of-life”*
- Info at <https://otalliance.org/loT>



# FRAMEWORK – 30 BASELINE CRITERIA



| IoT Trust Framework ● Required ○ Recommended N/A – Not Applicable   | Connected Home | Wearable Tech |
|---|----------------|---------------|
| <b>SECURITY</b>   |                |               |
| 1. Ensure devices 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. All authentication credentials, including but not limited to passwords shall be salted and hashed and/or encrypted.  | ●              | ●             |
| 3. All IoT support web sites must fully encrypt the user session. Current best practices include HTTPS or HTTP Strict Transport Security (HSTS) by default, also known as AOSSL or Always On 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 generally accepted 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 the research community. Remediate post product release design vulnerabilities and threats in a publically responsible manner either through remote updates and/or through actionable consumer notifications, or other effective mechanism(s). | ●              | ●             |

## Major Sections Include:

- Security
- User Access & Credentials
- Privacy Transparency & Disclosures



The image features several colorful geometric shapes, primarily triangles and lines, scattered across the white background. A large, multi-colored triangular shape is prominent on the right side, composed of various shades of blue, green, yellow, orange, pink, and purple. Several thin, colored lines (blue, pink, green, orange) radiate from the center towards the edges. The text 'LIVE WORX 16' is centered, with 'LIVE' in a thin, spaced-out font and 'WORX 16' in a bold, black font. A black rectangular box containing the tagline 'TAKE A FRESH LOOK AT THINGS' is positioned below the main text. The website address 'liveworx.com' is located at the bottom left.

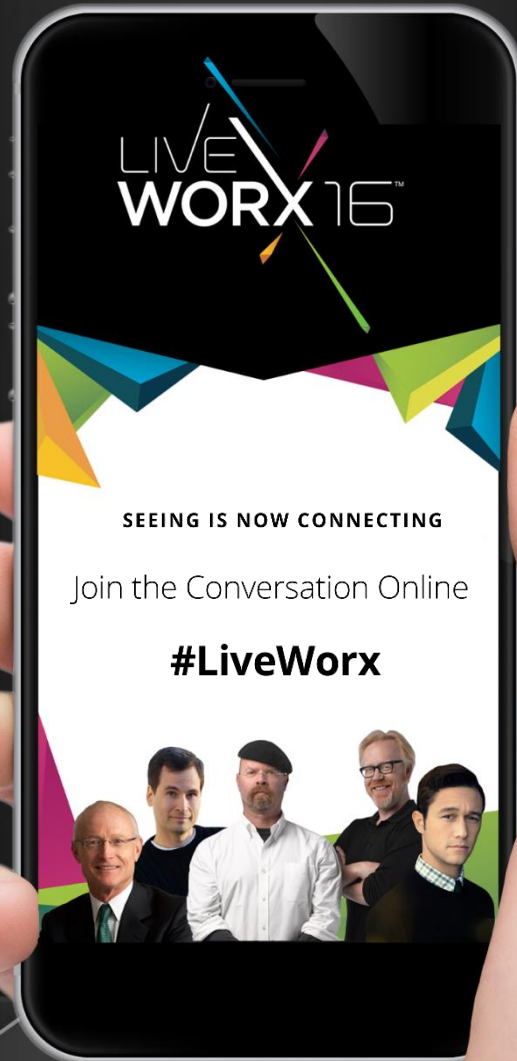
LIVE  
WORX 16™

TAKE A FRESH LOOK AT THINGS

liveworx.com



LIVE  
WORX 16™



Please use the  
mobile app to rate  
this session  
Access the latest schedule and join  
the conversation on social media  
**#LIVEWORX #IoT.**