SESSION ID: AST3-W02

THE PROMISE OF IOT
BEST PRACTICES, TESTING & THE
HAZARDS OF INACTION

MODERATOR: **Craig Spiezle**
Managing Director, Agelight Risk Advisory Group
Founder & Chairman, Online Trust Alliance
@craigspi

PANELISTS:

**Patricia Adair**
Director of Risk Management Group
Consumer Product Safety Commission
@USCPSC

**Justin Brookman**
Director, Privacy & Technology Policy
Consumers Union
@JustinBrookman

**Terrell McSweeny**
Commissioner
Federal Trade Commission
@TMcSweenyFTC
Danger Will Robinson IoT Devices Ahead!
Challenge of The IoT Ecosystem

Devices

Cloud

Apps
Shift from Online to Risks to Hazardization

- Amplified Impact to Critical Infrastructure & Communities
IoT Incident of the Week

Hackers exploit casino's smart thermometer to steal database info
Testing Models – Can They Apply To IoT?
Kidde Recalls Dual Sensor Smoke Alarms Due to Risk of Failure to Alert Consumers to a Fire

A yellow cap left on during the manufacturing process can cover one of the two smoke sensors and compromise the smoke alarm’s ability to detect smoke.

Fitbit Recalls Force Activity-Tracking Wristband Due to Risk of Skin Irritation

Note: On February 20, 2014, Fitbit Inc. announced a refund program for the Fitbit Force. This press release serves as the official recall announcement. For more information, visit www.fitbit.com/warranty/how-to-report-a-defect or call 1-844-937-4449. Effective 1/11/16.

- Name of product: Wireless activity-tracking wristband
- Hazard: Users can develop allergic reactions to the stainless steel strap, or adhesives used to assemble the product, where the skin has been in contact with the tracker
- Remedy: Refund
- Recall date: March 12, 2014
- Units: About 1,000,000 in the U.S. and about 20,000 in CA
Samsung and Roku Smart TVs Vulnerable to Hacking, Consumer Reports Finds

Security and privacy testing of several brands also reveals broad-based data collection. How to limit your exposure.
Harmonizing Risk Assessment Models

Guiding Directives
• Address the root causes of risks at-scale
• Promote security and privacy practices which are feasible to adopt
• Reduce consumer risk & support burdens
• Drive supply chain continuous improvement
• Incentivize adoption & differentiation
• Ability to evaluate & select secure products
• Be applicable globally

Scoring Criteria
• User benefit & completion
• Impact to ecosystem (internal and externally)
• Financial and performance impact
• Physical safety risks if not addressed
• Effort to support over a product’s life
• Regulatory and product liability risks
<table>
<thead>
<tr>
<th>Disclosure of Security Updates and Support Duration</th>
<th>GDPR / Article 29 WG</th>
<th>NIST Framework</th>
<th>ENISA</th>
<th>UK Secure by Design</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disclosure of security updates and the duration of support</td>
<td>Yes</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Notes** — All devices should receive security updates and patches throughout their expected life. In some cases companies may offer extended support for a fee as a managed service. In addition existing protocols and standards may have to be updated due to newly discovered vulnerabilities such as KRACK compromising devices which support WPA2. See #22 for related requirements and context.

**Updates and patches should not modify user-configured preferences, security, and/or privacy settings without user notification.** In cases where an update must overwrite device settings, the user must be prompted to review and select settings prior to install.

**Notes** — User device configurations ranging from security, privacy to battery power settings have been inadvertently "written over" from updates which have placed devices back to their default or “factory shipped” status. If overwriting preferences and settings cannot be prevented, prior to updates being installed users should be prompted to review and record their settings to facilitate the ability to reset them. On "first use" the user should be prompted and walked through re-setting such settings.
### Disclose if device security updates and patches are provided and the duration of support

**Notes** — All devices should receive security updates and patches throughout their expected life. In some cases companies may offer extended support for a fee as a managed service. In addition existing protocols and standards may have to be updated due to newly discovered vulnerabilities such as KRACK compromising devices which support WPA2. See #22 for related requirements and context.

### Updates and patches should not modify user-configured preferences, security, and/or privacy settings without user notification. In cases where an update must overwrite device settings, the user must be prompted to review and select settings prior to install.

**Notes** — User device configurations ranging from security, privacy to battery power settings have been inadvertently “written over” from updates which have placed devices back to their default or “factory shipped” status. If overwriting preferences and settings cannot be prevented, prior to updates being installed users should be prompted to review and record their settings to facilitate the ability to reset them. On “first use” the user should be prompted and walked through re-setting such settings.
Apply What You Have Learned Today

Within 30 days:

- **Organizations / Users**
  - Inventory devices and review privacy and security settings
  - Be thoughtful of the benefits / risks before you buy

- **Device Vendors**
  - Embrace established IoT trust principles and standards
  - Review FTC guidance and EU General Data Protection Regulations (GDPR)
  - Review your marketing claims and privacy policies

Within 180 days:

- **Organizations / Users**
  - Establish and implement device configurations based on your “risk appetite”
  - Move all devices to an isolated network / Disable insecure products/functions

- **Device Vendors**
  - Develop a life-cycle / sustainability support plan
  - Tune your practices and policies - Shift from compliance to stewardship
Looking Ahead- Q & A
Resources https://agelight.com/IoTResources.html

- Internet Society https://internetsociety.org/IoT
- Department of Commerce, NTIA – Coordinated Vulnerability Disclosures https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities
- FTC & The NIST Cybersecurity Framework https://go.usa.gov/xQqgA
- FTC Building Security into IoT https://ftc.gov/carefulconnections
- AgeLight https://agelight.com/iot.html
- Consumer Reports / Digital Standard https://www.thedigitalstandard.org/