RSA®Conference2019

San Francisco | March 4 – 8 | Moscone Center

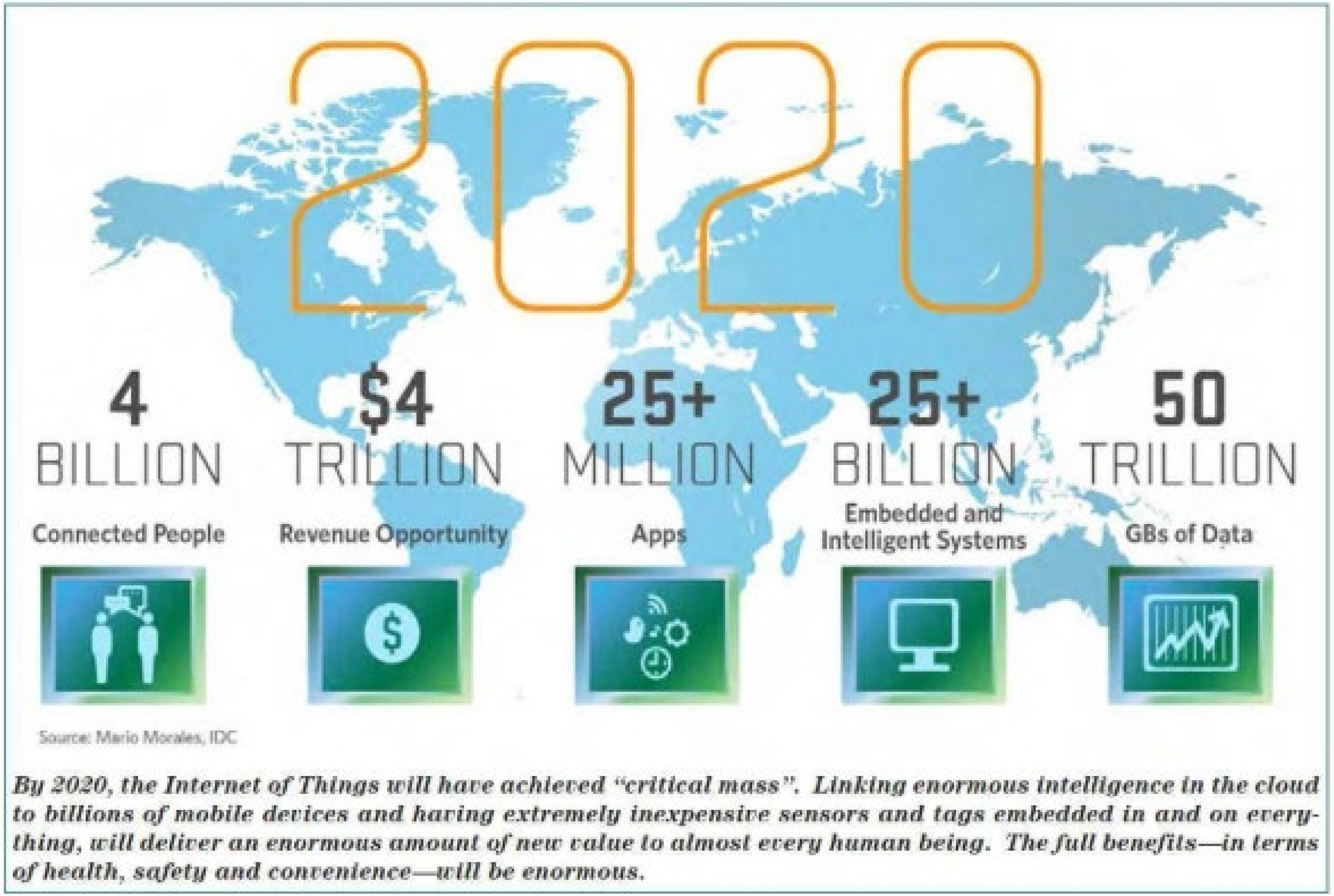
BETTER.

SESSION ID: **SEM-M04F**

# IoT State of Security

**Julie Fitton**

VP, Digital Product Security
Stanley Black & Decker



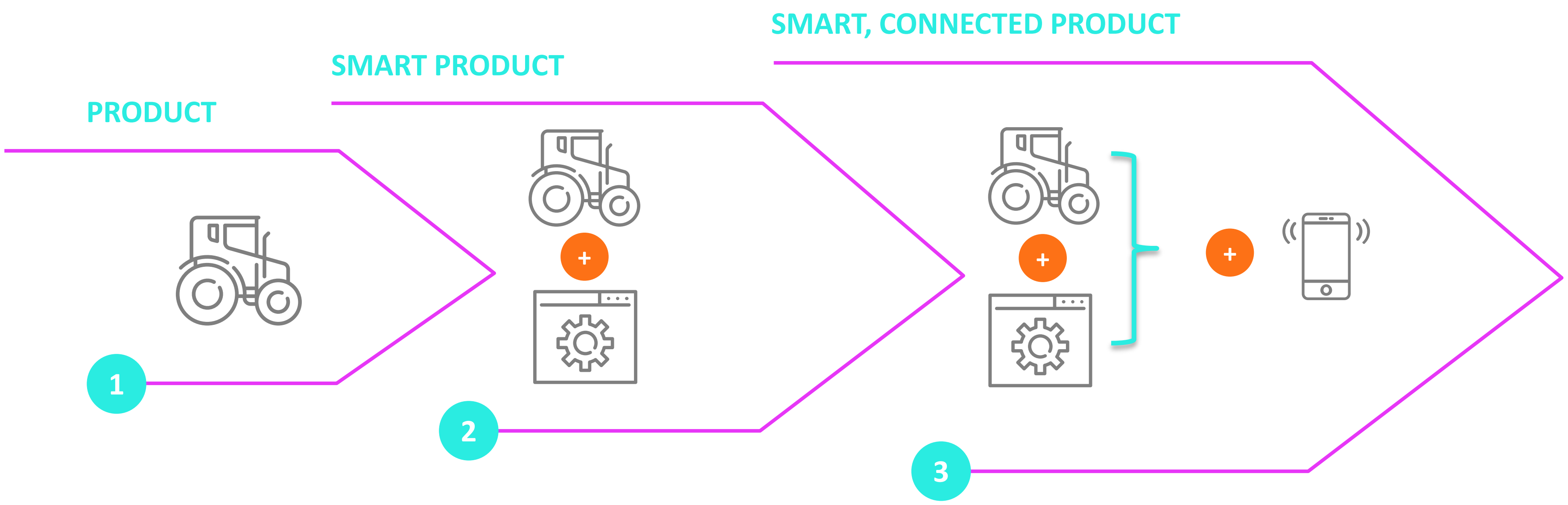
Source: Mario Morales, IDC

*By 2020, the Internet of Things will have achieved "critical mass". Linking enormous intelligence in the cloud to billions of mobile devices and having extremely inexpensive sensors and tags embedded in and on everything, will deliver an enormous amount of new value to almost every human being. The full benefits—in terms of health, safety and convenience—will be enormous.*

https://www.spindox.it/en/innovation/internet-of-things

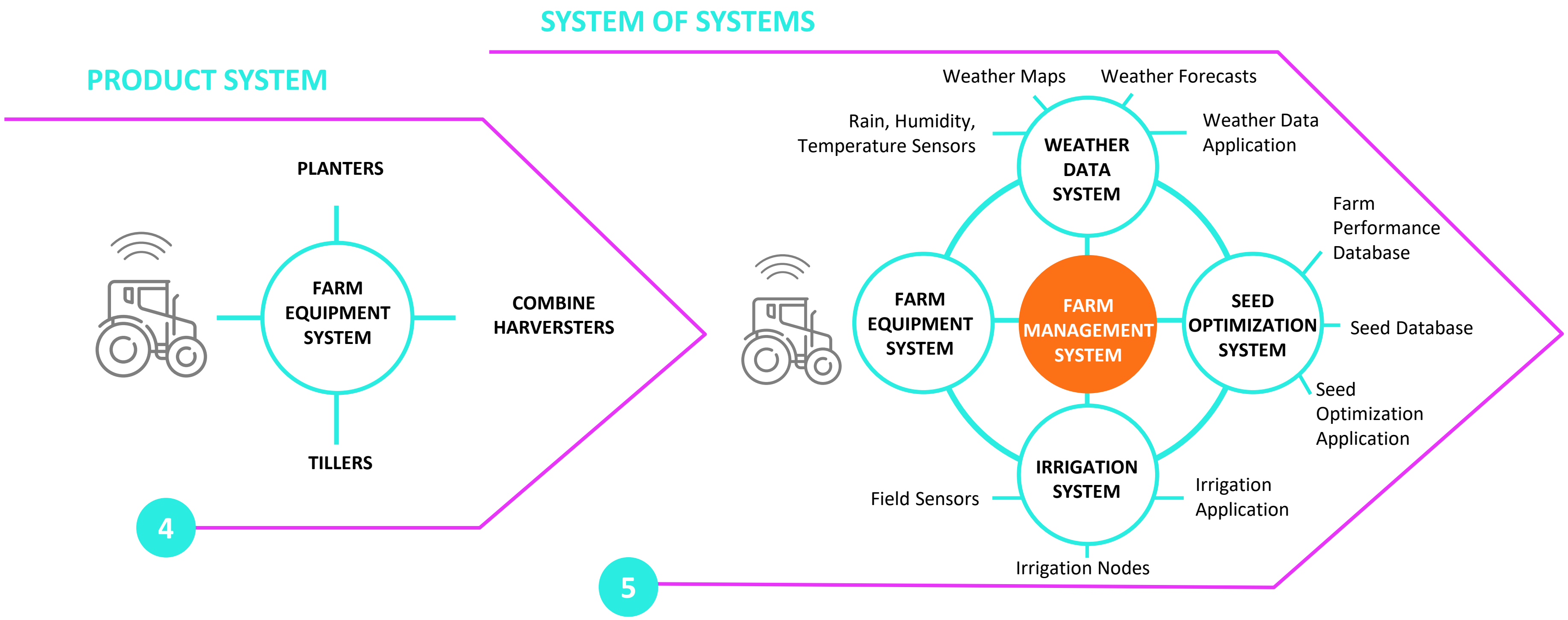
# What Makes a Piece of Hardware IoT

- Increasing capabilities and visibility
- Reshape competition within industries
- Expand industry boundaries



# Redefining Industry Boundaries

- Interoperability within Systems of Systems



PRODUCT SYSTEM

PLANTERS

FARM EQUIPMENT SYSTEM

COMBINE HARVESTERS

TILLERS

4

SYSTEM OF SYSTEMS

Weather Maps

Weather Forecasts

Rain, Humidity, Temperature Sensors

WEATHER DATA SYSTEM

Weather Data Application

Farm Performance Database

FARM EQUIPMENT SYSTEM

FARM MANAGEMENT SYSTEM

SEED OPTIMIZATION SYSTEM

Seed Database

Seed Optimization Application

Field Sensors

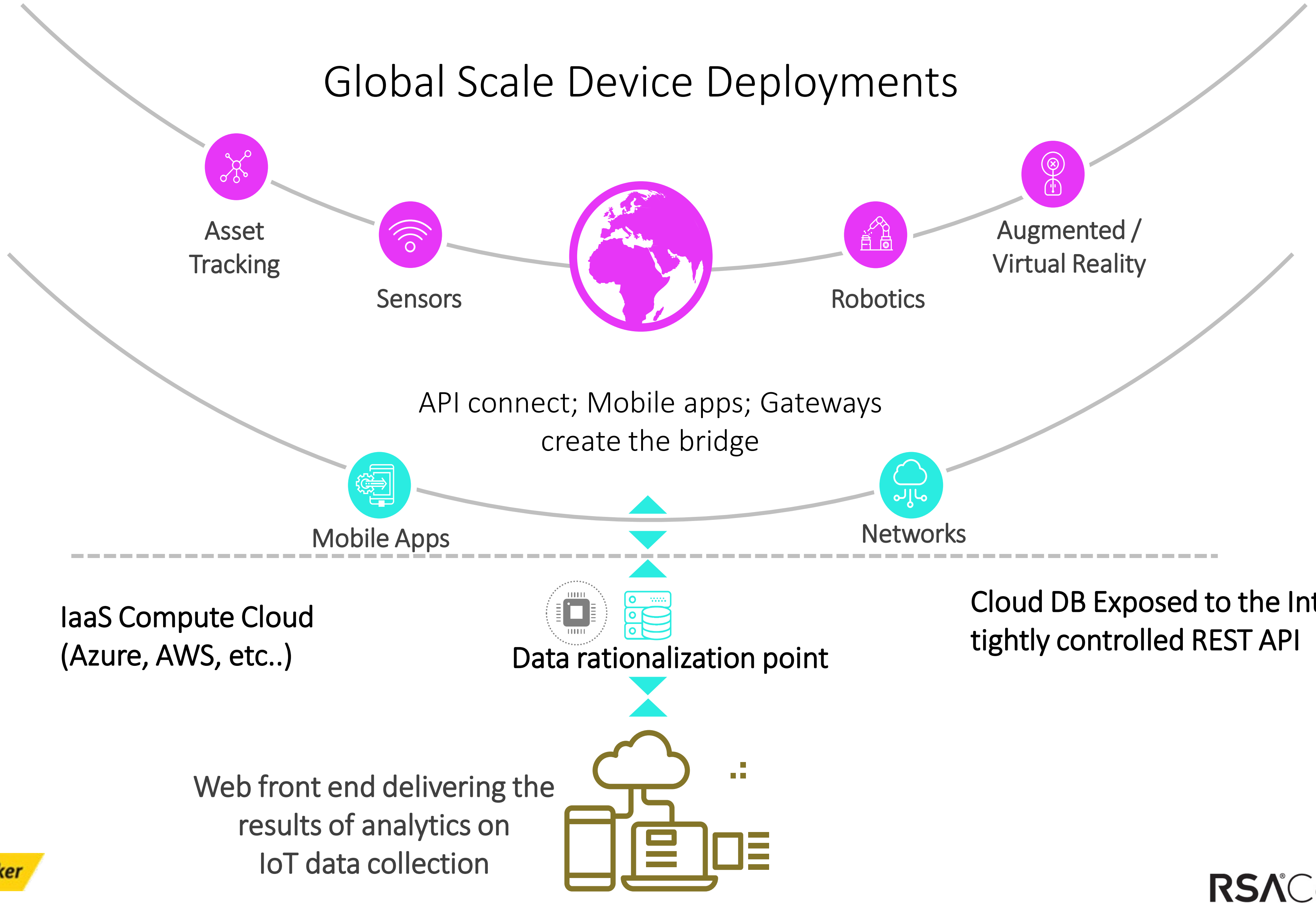
IRRIGATION SYSTEM

Irrigation Application

Irrigation Nodes

5

# Technology Layers of Connected Products



Global Scale Device Deployments

Asset Tracking

Sensors

Robotics

Augmented / Virtual Reality

API connect; Mobile apps; Gateways create the bridge

Mobile Apps

Networks

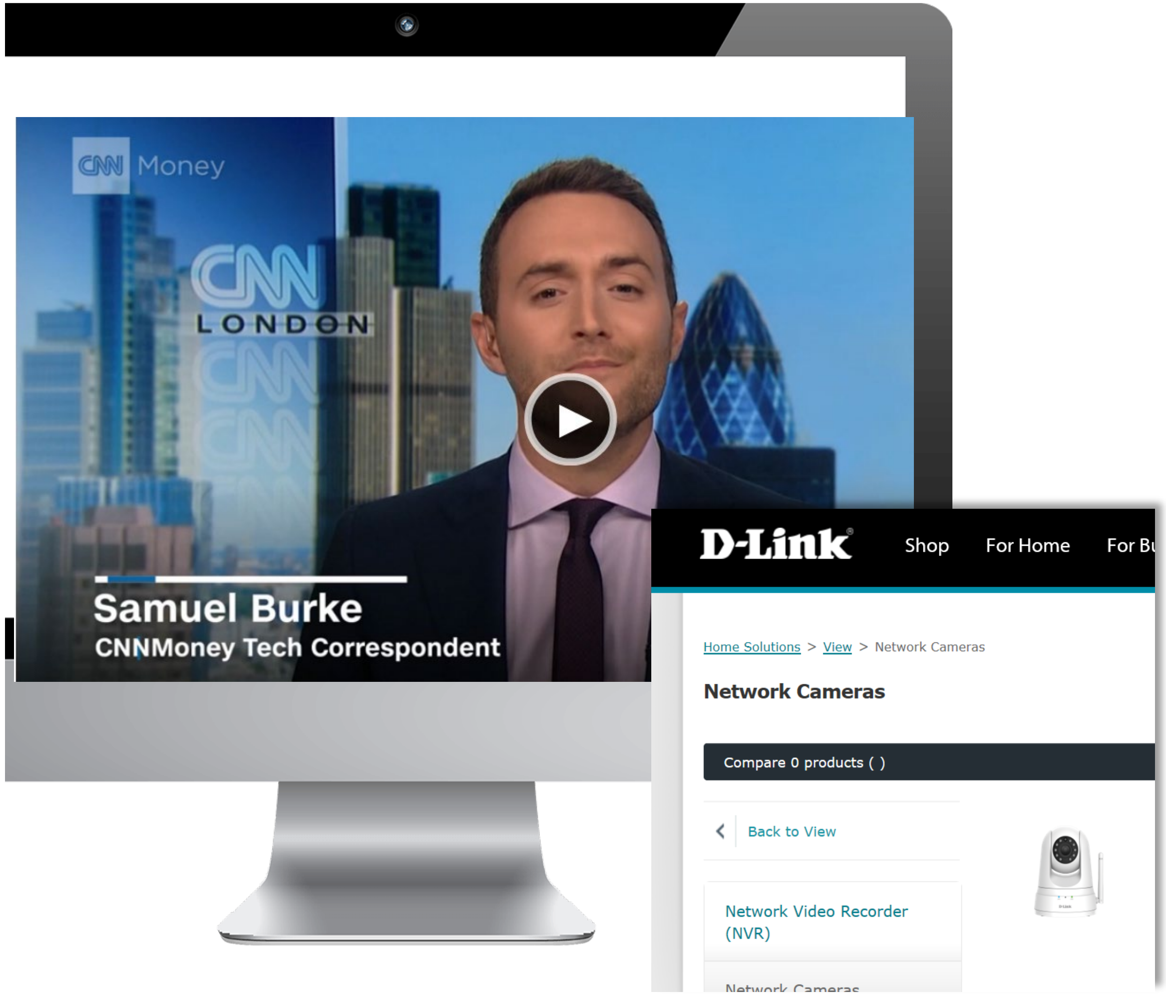
IaaS Compute Cloud (Azure, AWS, etc..)

Data rationalization point

Cloud DB Exposed to the Internet via tightly controlled REST API

Web front end delivering the results of analytics on IoT data collection

# FTC Sues maker of consumer products for failing to build in basic cyber security measures

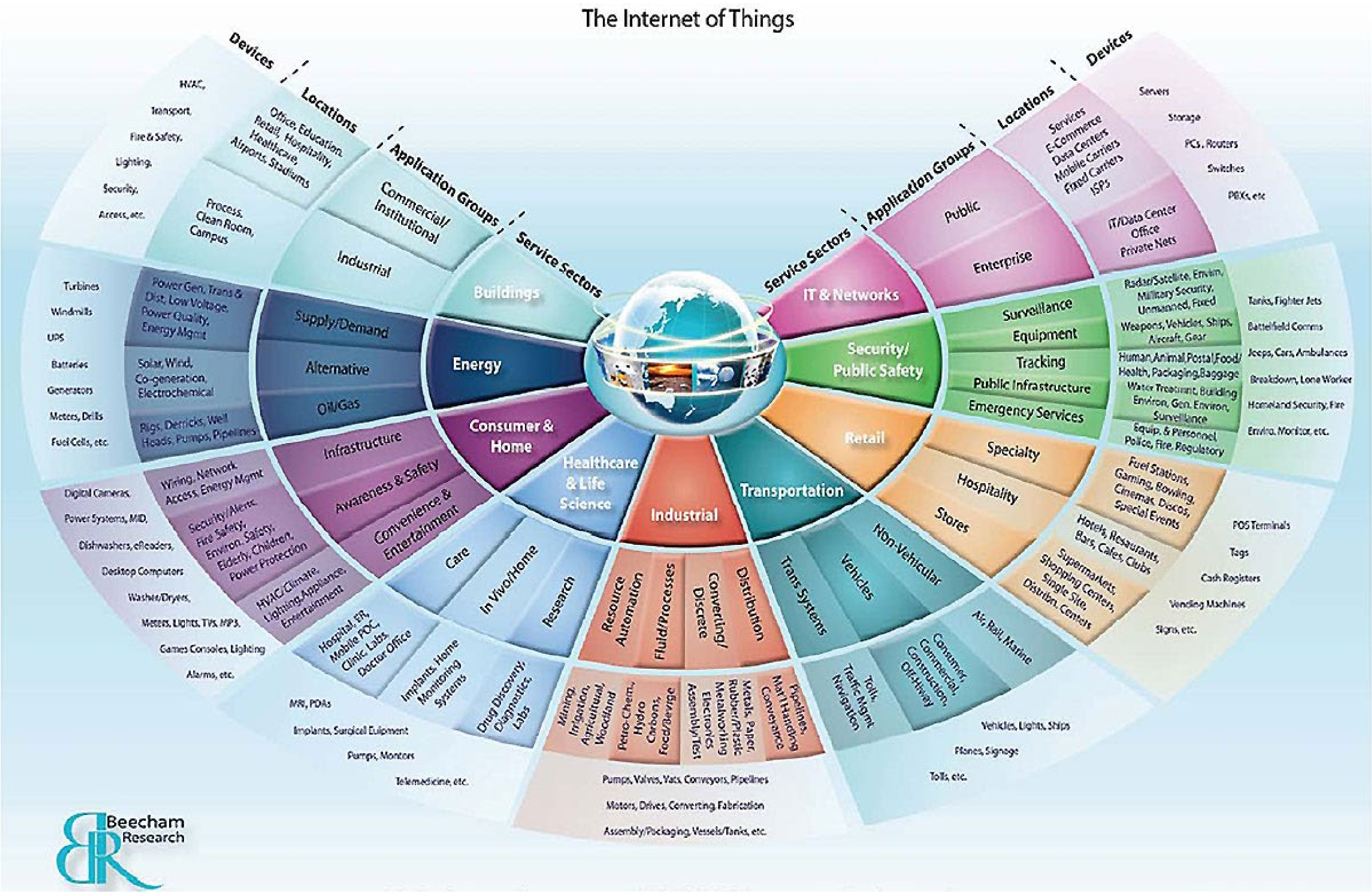


[http://money.cnn.com/2017/01/05/technology/ftc-d-link-lawsuit/index.html?iid=EL](http://money.cnn.com/2017/01/05/technology/ftc-d-link-lawsuit/index.html?iid=EL)

- Part of the highly publicized Dyn Attack
- D-Link is facing litigation costs and penalties, as well as court order mandates for compliance for omitting basic cyber security measures
- FTC is bringing this forward.
- D-Link products are extremely popular world-wide
- Suit filed January 2017. Court dismissed 3 of 6 FTC complaints citing lack of demonstration of disclosure of PII or harm….lawsuit still ongoing.

**Why is this happening?**

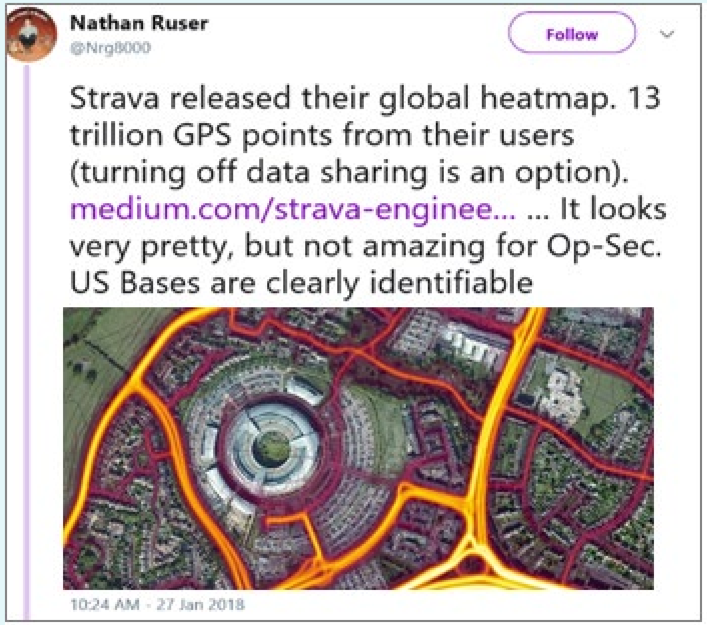
# The IoT was created to gather Big Data……


The Internet of Things
Devices
Locations
Application Groups
Service Sectors
HVAC,
Transport,
Fire & Safety,
Lighting,
Security,
Access, etc.
Office, Education, Retail, Hospitality, Healthcare, Airports, Stadiums
Process, Clean Room, Campus
Commercial/ Institutional
Industrial
Buildings
Turbines
Windmills
UPS
Batteries
Generators
Meters, Drills
Fuel Cells, etc.
Power Gen, Trans & Dist, Low Voltage, Power Quality, Energy Mgmt
Solar, Wind, Co-generation, Electrochemical
Rigs, Derricks, Well Heads, Pumps, Pipelines
Supply/Demand
Alternative
Oil/Gas
Energy
Digital Cameras,
Power Systems, MID,
Dishwashers, eReaders,
Desktop Computers
Washer/Dryers,
Meters, Lights, TVs, MP3,
Games Consoles, Lighting
Alarms, etc.
Wiring, Network Access, Energy Mgmt
Security/Alerts, Fire Safety, Environ. Safety, Elderly, Children, Power Protection
HVAC/Climate, Lighting, Appliance, Entertainment
Infrastructure
Awareness & Safety
Convenience & Entertainment
Consumer & Home
Healthcare & Life Science
Care
In Vivo/Home
Research
Hospital, ER, Mobile POC, Clinic, Labs, Doctor Office
Implants, Home Monitoring Systems
Drug Discovery, Diagnostics, Labs
MRI, PDAs
Implants, Surgical Euipment
Pumps, Monitors
Telemedicine, etc.
Industrial
Resource Automation
Fluid/Processes
Converting/ Discrete
Distribution
Mining, Irrigation, Agricultural, Woodland
Petro-Chem, Hydro Carbons, Food/Bevrge
Metals, Paper, Rubber/Plastic Metalworking Electronics Assembly/Test
Pipelines, Mat'l Handling Conveyance
Pumps, Valves, Vats, Conveyors, Pipelines
Motors, Drives, Converting, Fabrication
Assembly/Packaging, Vessels/Tanks, etc.
Transportation
Trans Systems
Vehicles
Non-Vehicular
Tolls, Traffic Mgmt Navigation
Consumer, Commercial, Construction, Off-Hway
Air, Rail, Marine
Vehicles, Lights, Ships
Planes, Signage
Tolls, etc.
Retail
Specialty
Hospitality
Stores
Fuel Stations, Gaming, Bowling, Cinemas, Discos, Special Events
Hotels, Restaurants, Bars, Cafes, Clubs
Supermarkets, Shopping Centers, Single Site, Distribn. Centers
POS Terminals
Tags
Cash Registers
Vending Machines
Signs, etc.
Security/ Public Safety
Surveillance
Equipment
Tracking
Public Infrastructure
Emergency Services
Radar/Satellite, Envirn, Military Security, Unmanned, Fixed
Weapons, Vehicles, Ships, Aircraft, Gear
Human, Animal, Postal, Food/ Health, Packaging, Baggage
Water Treatment, Building Environ, Gen. Environ, Surveillance
Equip. & Personnel, Police, Fire, Regulatory
Tanks, Fighter Jets
Battlefield Comms
Jeeps, Cars, Ambulances
Breakdown, Lone Worker
Homeland Security, Fire
Enviro. Monitor, etc.
IT & Networks
Public
Enterprise
Services E-Commerce Data Centers Mobile Carriers Fixed Carriers ISPs
IT/Data Center Office Private Nets
Servers
Storage
PCs, Routers
Switches
PBXs, etc
Beecham Research

# What’s at stake? Understand the Impact

Many Companies Are Building Products With Insecure Or Misconfigured Apps, Platforms And Devices

## **Strava’s** Fitness Tracking App Exposes U.S. Military Secrets



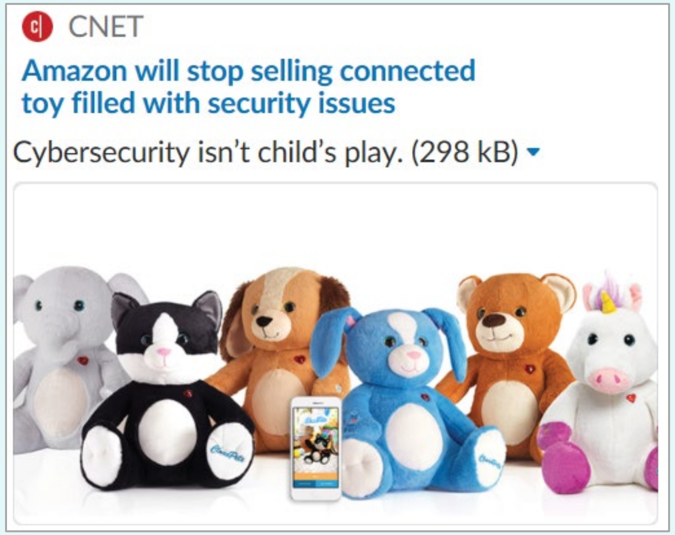
Nathan Ruser
@Nrg8000

Strava released their global heatmap. 13 trillion GPS points from their users (turning off data sharing is an option). medium.com/strava-enginee... ... It looks very pretty, but not amazing for Op-Sec. US Bases are clearly identifiable

10:24 AM - 27 Jan 2018

http://fortune.com/2018/01/29/strava-heat-map-fitbit-fitness-tracking-military/

## **Cloud Pets** Allows Hackers To Spy On Children



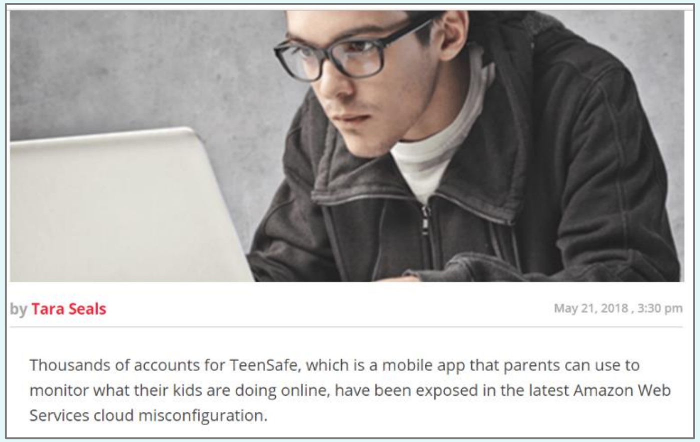
CNET

Amazon will stop selling connected toy filled with security issues

Cybersecurity isn’t child’s play. (298 kB)

https://www.cnet.com/news/amazon-will-stop-selling-connected-toy-cloud-pets-filled-with-security-issues/

## **TeenSafe** Tracking App Exposes Private Records



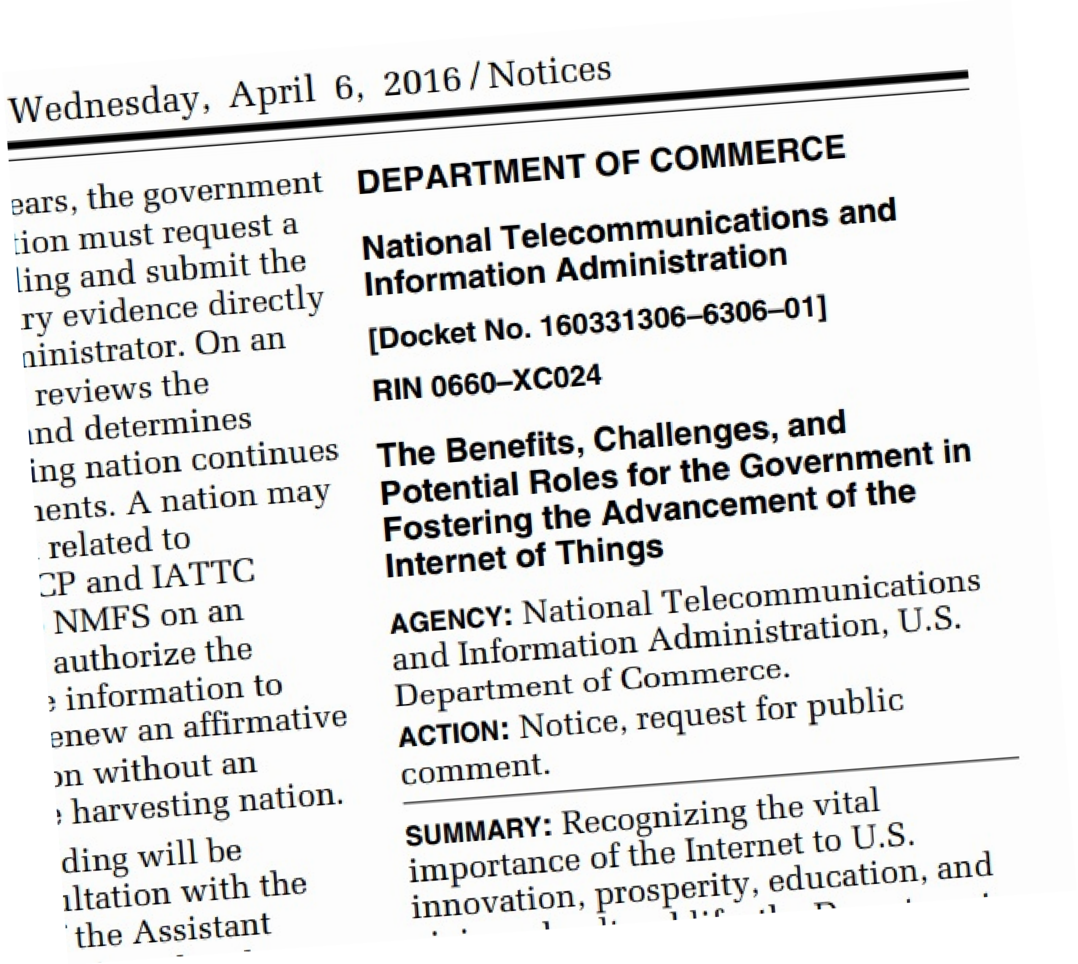
by Tara Seals

May 21, 2018 , 3:30 pm

Thousands of accounts for TeenSafe, which is a mobile app that parents can use to monitor what their kids are doing online, have been exposed in the latest Amazon Web Services cloud misconfiguration.

https://threatpost.com/teensafe-tracking-app-exposes-thousands-of-private-records/132152/

# Is the Internet of Things Really Different?



Wednesday, April 6, 2016 / Notices

ears, the government
tion must request a
ling and submit the
ry evidence directly
ninistrator. On an
reviews the
nd determines
ing nation continues
nents. A nation may
related to
CP and IATTC
NMFS on an
authorize the
information to
enew an affirmative
on without an
harvesting nation.
ding will be
ltation with the
the Assistant

**DEPARTMENT OF COMMERCE**

**National Telecommunications and Information Administration**

**[Docket No. 160331306–6306–01]**

**RIN 0660–XC024**

**The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things**

**AGENCY:** National Telecommunications and Information Administration, U.S. Department of Commerce.

**ACTION:** Notice, request for public comment.

**SUMMARY:** Recognizing the vital importance of the Internet to U.S. innovation, prosperity, education, and

## *Key Concerns:*

- *Privacy – generating a lot of data*
- *Security – Connecting everything*

***"Systems of Systems"***

# The Government Role is Slow to Evolve

## January, 2017 - Challenges from Report:

1. Reserving certain frequencies for communication for emergency responders

2. IPv4, IPv6 problem-running out of addressable space on internet-need to solve for these two problem.

**Conclusion:** It will take gov't a while to catch up with technology

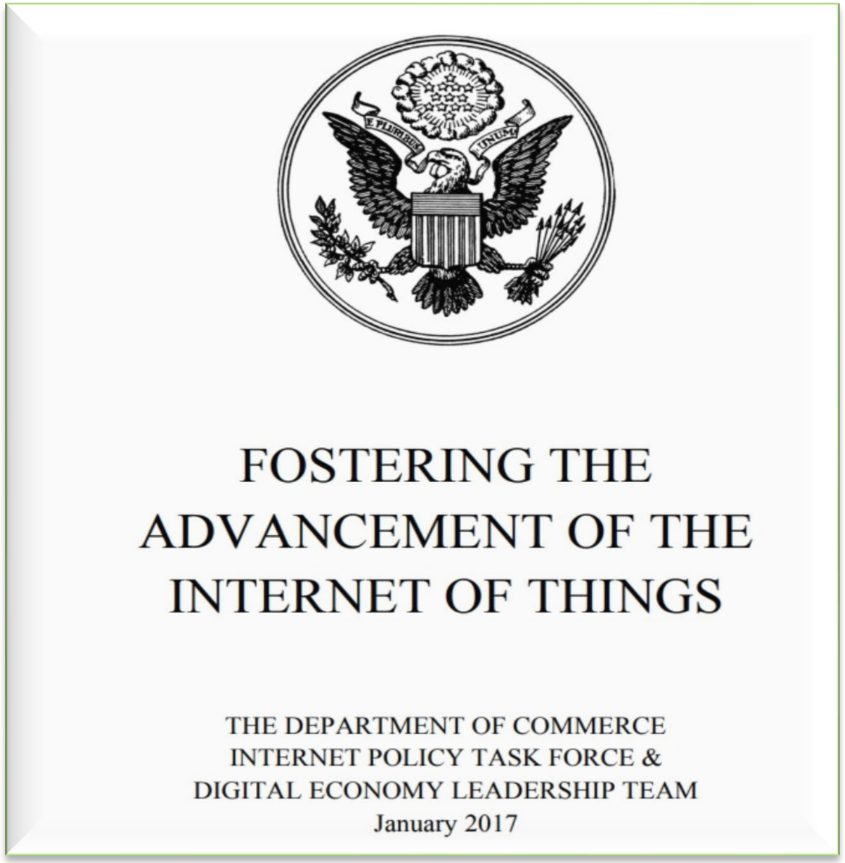
## October 25, 2018 – Presidential Memorandum

[Developing a Sustainable Spectrum Strategy For America's Future]

## Giving America a Boost in 5G:

https://www.ntia.doc.gov/blog/2018/president-s-national-spectrum-strategy-will-give-america-boost-5g

## NTIA Green Paper



FOSTERING THE ADVANCEMENT OF THE INTERNET OF THINGS

THE DEPARTMENT OF COMMERCE
INTERNET POLICY TASK FORCE &
DIGITAL ECONOMY LEADERSHIP TEAM
January 2017

# Industry Groups Talking IoT Security or Privacy

- ***The Federal Trade Commission (FTC)***
  - Consumer Privacy and Security
- ***The Department of Commerce's (DOC)*** National Institute of Standards (NIST)
  - Cyber Security Framework geared toward IoT management as deployed in an Enterprise/Industry 4.0
  - Process centric
  - Deployed state guidance, vs. Manufacturer guidelines
- ***Consumer Product Safety Commission(CPSC)***
  - Consumer safety in products
    - now expanding to connected product hacks that can result in consumer injury
- ***National Highway & Traffic Safety Administration***
  - Issued Voluntary guidance on self driving cars in Sept 2017

# SB-327 – CA bill governing security in IoT

- *This bill, beginning on January 1, 2020, requires a manufacturer of a connected device, … to equip the device with  reasonable security features that are appropriate to:*
  - *The nature and function of the device,*
  - *Appropriate to the information it may collect, contain, or transmit,*
  - *Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure, as specified.*

| | Product Mfg Focused | Integration Focused |
|---|---|---|
| **Device Hardware** | UL<br>OWASP Open Web Application Security Project | industrial internet® CONSORTIUM |
| **Software / Mobile App** | UL<br>OWASP Open Web Application Security Project<br>SAFECode Software Assurance Forum for Excellence in Code Driving Security and Integrity | industrial internet® CONSORTIUM |
| **Communications & Networking** | UL<br>OWASP Open Web Application Security Project<br>AICPA SOC 2 AICPA Service Organization Control Reports Formerly SAS 70 Reports<br>CERTIFIED ISO 27001 INFORMATION SECURITY | industrial internet® CONSORTIUM<br>NIST CYBERSECURITY FRAMEWORK (CSF) IDENTIFY PROTECT DETECT RESPOND RECOVER |
| **Hosting On-Premise or Cloud** | AICPA SOC 2 AICPA Service Organization Control Reports Formerly SAS 70 Reports<br>CERTIFIED ISO 27001 INFORMATION SECURITY | NIST CYBERSECURITY FRAMEWORK (CSF) IDENTIFY PROTECT DETECT RESPOND RECOVER |

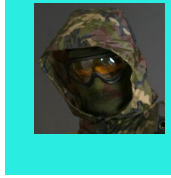
# Trust Framework, Visualized

## THREAT ACTORS

Criminals

Nation States

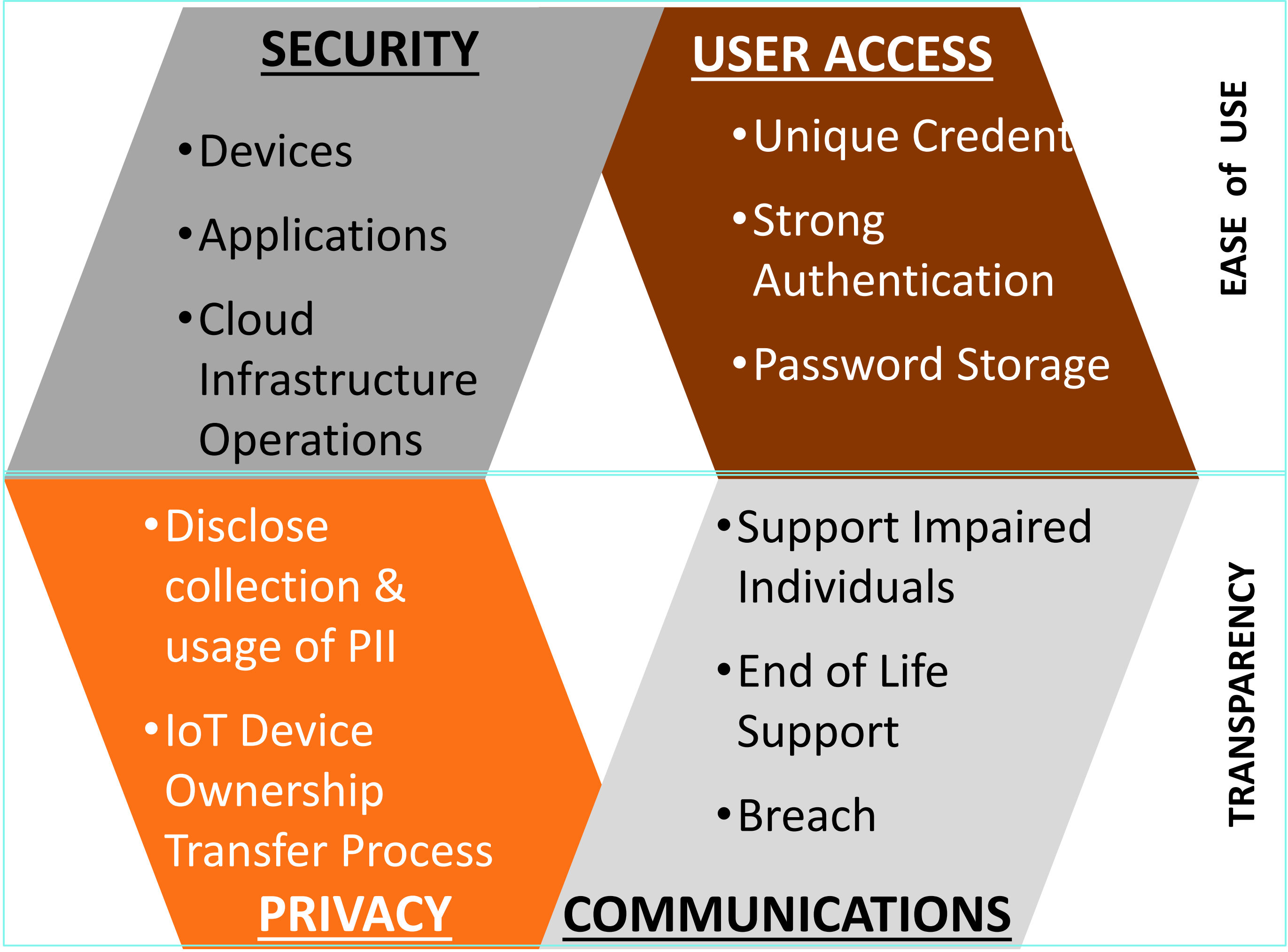
Terrorists/ Hackers



Disruptive Events

## THREAT TACTICS & EVENTS

- Malware
- Phising
- Social Engineering
- Scanning
- SQL Injection
- High Value Target Recon
- Privilege Elevation
- Earth Quake
- Civil Unrest
- War



**SECURITY**

- Devices
- Applications
- Cloud Infrastructure Operations

**USER ACCESS**

- Unique Credent
- Strong Authentication
- Password Storage

- Disclose collection & usage of PII
- IoT Device Ownership Transfer Process

**PRIVACY**

- Support Impaired Individuals
- End of Life Support
- Breach

**COMMUNICATIONS**

StanleyBlack&Decker

# How to Get Started with IoT

- Start by researching your industry, and emerging regulatory trends coming from Government agencies
  - Example, if your in the automotive industry, what is the Department of Transportation thinking about?
- Next pick one of the emerging frameworks focused on IoT and the unique considerations associated with IoT and OT.
- Think about risk, apply controls first in the areas of highest risk for your use case.

RSA Conference2019

Thank You!