The Internet of Things, Big Data, and Storage Security: and New Vectors for Liability

a.k.a. – Old Wine, Contorted New Bottles...
IoT Features

• Ubiquity
• Number of Devices (Sagan$^2$)
• Monoclonality
• 3D Communication Exchange
• Remote Control and Monitoring
• Big Data Generation (think analytics)
IoT Use Cases

• High volume low value devices (consumer and municipal)
  • Example: Home appliance mgt., lighting, wearables
• Low volume, high value devices (industrial, municipal)
  • Example: Medical device mgt., infrastructure mgt
• High Volume, high value devices
  • Example: Automobiles
Some Other IoT Features

• End of device/object function life match end of IoT utility or functionality
• Orphaned? Updated? Upgraded?
• Big Data generated, stored, and used/monetized
• Back end processing and storage of data/information generated by IoT devices/objects
IoT Data: Exabytes, Zettabytes and OMG

• Back end processing and storage of data/information generated by IoT devices/objects
Data Storage Security: The Good Old Days

- Customers were high up in the food chain
- Liability could be managed, limited by contract
- Reliable liability metrics could be applied to assess risks for device/software failure
- End users, consumers not factored into risk assessments
Data Storage Security Today: Exposure to New Vectors of Liability

- Data accessibility - from storage industry products now directly affects all end users (customers, consumers, individuals, industry, and municipalities).
- Liability is open ended, with many flavors.
- No reliable liability metrics could be applied to assess risks for device/software failure

Why?
Data Accessibility Failure and IoT

Consider:
- Management console breach
- Access to data stored is blocked
- Devices and sensors can’t call home, or each other
- IoT ecosystem balance malfunctions or fails

Consider affected communities:
- End users, consumers and individuals
- Hospitals, medical facilities
- Municipal utilities services
- Big Data/Analytics providers who monetize IoT data
Think of the possibilities...
Are Storage Industry Providers Now Subject to HIPAA? Are They Business Associates?

New Business Associate Compliance Requirements
Security Risks

Perceived Downsides To The Internet Of Everything

- Threats To Data Or Physical Security: 42%
- Inability Of Our IT Systems To Keep Up With Change: 38%
- Regulatory Challenges: 32%
- Competition From New Rivals: 28%
- Greater Price Transparency/Lower Profit Margins: 25%
- Job Losses Due To Outsourcing Or Automation: 25%

BI Intelligence
The size, monoculture (uniformity), insecurity, and non-standardized coding and manufacture of connected devices and services provided through them puts millions of users of the “Internet of Things” at risk for serious injury and financial harm on a massive scale.

Consider tens of billions of connected devices by 2020

IoT Liability Concerns – Why?

- **Poor Coding:**
  - Coding for these devices is often a one time event, will become obsolete and ultimately fail to properly work, either through neglect (no upgrades) or through faulty initial design.

- **Minimal Testing:**
  - Testing of these devices is unregulated, unaudited and generally not disclosed (so what *is* the MTBF for an IoT?)

- **No Regulation:**
  - Coding for these devices is unregulated, unaudited, and subject to little if any quality control.

- **Poor/No Security**
  - Security (and security standards) for these devices have yet to be adopted or even developed.

- **Poor/No Event Logging**
  - Most IoT devices have no logging mechanisms to record failure or malfunction events.
IoT Liability Concerns – Where are they?

- **Automobiles**
  - brakes, acceleration, cooling, steering, engine, tire and oil pressure, and navigation systems
- **Aircraft**
  - commercial, private, and drones
- **Medical Devices**
  - external and implanted
- **Household Appliances**
  - Cooking, HVAC, lighting, entertainment
- **Transportation management**
- **Environmental Monitoring**
  - Building, Household management
- **Energy Management**
  - utilities providing power, water, etc.
- **Communications devices**
  - mobile devices
- **Computing devices**
  - Traditional computers and mobile devices
- **Wearables, etc.**
- **Banking and Finance** - other consumer services
- **Robotics and AI**
- **Toys, Games and Entertainment Devices**
IoT Liability Concerns for the Storage Industry

- Arising from Customers (by contract) or users (no contract)
  - Lost profits
  - Negligence (ordinary and gross)
  - Warranty – merchantability and fitness
  - Fraud
  - Strict Liability (to be tested in certain circumstances)
  - Unfair, deceptive trade practice
The FTC Chimes in on IoT Security...

- Companies developing IoT products and services should implement “reasonable security”
  - Query: What is “reasonable security”?  
  - Factors Include: amount and sensitivity of collected and the cost of remedying the security vulnerabilities.
- Companies should (but don’t) implement “security by design”
  - Privacy risk assessment
  - Minimize data collected and retained
  - Test security measures
  - Train employees about good security
  - Implement access control measures
The FTC *does not* mention what measures are to be taken to ensure the physical and personal protection from defective or malfunctioning IoT.
The FTC Chimes in on IoT Security...

- Continue to monitor products throughout the life cycle, and to the extent feasible, patch known vulnerabilities.

What does this mean in the real world?
The Stage is Set for IoT Class Actions and Mass Torts

- Coding for these devices is unregulated, unaudited, and subject to little if any quality control.
- Coding for these devices is often a one time event, will become obsolete and ultimately fail to properly work, either through neglect (no upgrades) or through faulty initial design.
- Coding for these devices is often insecure or not testably secure.
- Effects of environmental changes or updates (if any) are unknown, and untested.
IoT Liability Concerns – Why?

• **Poor Coding:**
  – Coding for these devices is often a one time event, will become obsolete and ultimately fail to properly work, either through neglect (no upgrades) or through faulty initial design

• **Minimal Testing:**
  – Testing of these devices is unregulated, unaudited and generally not disclosed (so what *is* the MTBF for an IoT?)

• **No Regulation:**
  – Coding for these devices is unregulated, unaudited, and subject to little if any quality control

• **Poor/No Security**
  – Security (and security standards) for these devices have yet to be adopted or even developed

• **Poor/No Event Logging (evidence)**
  – Most IoT devices have no logging mechanisms to record failure or malfunction events
IoT Theories of Liability

- **Negligence:**
  - Ordinary and Gross

- **Express and Implied Warranties:**
  - Including merchantability and fitness

- **Fraud:**
  - Misrepresentation

- **Strict Liability**
  - When to apply strict liability theory

- **Privacy**
  - Terms of Service or EULA not clear or does not address
Potential IoT Litigation Hurdles

• Class Action Waivers
  – Many will fail
  – Single events cases will may also have high value

• Mandatory Arbitration:
  – As yet undecided
  – Many will fail

• Why Will Many, if Not Most, Class Waivers and Arb. Clauses Fail?
Potential IoT Victims
Consumers

Children
Potential IoT Victims Consumers
Potential IoT Victims Consumers

And Sex Toy Users
Questions?

Thank You