Internet of Things: Security, Privacy and Risk Considerations for a Connected World

Speakers:

- Steve Bridges, Senior Vice President, Cyber/E&O Practice, JLT Group
- Ellen Shew Holland, Associate Vice President & Chief Risk Officer, Southern Methodist University
- Darren Teshima, Partner, Orrick, Herrington & Sutcliffe LLP

Learning Objectives

At the end of this session, you will learn:

- **Opportunities and Risks Posed by IoT**
  - Overview of IoT opportunities
  - Key IoT risks faced by companies
  - What companies can do to mitigate risks
- **Key Insurance Coverages**
  - Potentially applicable coverages and how they work
  - Potentially applicable exclusions and defenses to coverage
  - Recent case developments
- **Practical Implications from a Risk Management Perspective**

Overview of IoT

- **Overview of IoT**
  - Digitizing the physical world
  - Transforming interactions between consumers, business & government
  - Rapid adoption

Issues to Consider

Litigation & Brand Risks

- Product Liability/Medical Malpractice
- Cybersecurity
- Privacy
- IP Issues

Identifying Key Risks in IoT

- Identify the “Thing” or “Things”
- Industry norms related to the “Thing”
- What does the “Thing” do?
- What data is related to the “Thing”
- Security of the “Thing”
- “Ecosystem” of the “Thing”
- How Can Others Use the Thing

Mitigating the Risks

- Contract Language
  - Warnings
    - Provide warnings re security and safety risks
    - Disclose duration of security and firmware updates
    - Implement strict password requirements
    - Warn about hazards of unattended use of devices and appliances
- Disclaimers
  - Can be used to mitigate liability
    - User negligence in security measures
    - Unintended or unauthorized use
    - Stopping firmware updates
    - Third-party interference

Mitigating the Risks (cont.)

- Terms of Service
  - Connected devices provide unique opportunity to enter into a contractual relationship with typical consumer
  - Forum for warnings, disclaimers
  - Warranties, limitations of liability
  - Arbitration agreements and class action waivers
  - Technology allows terms of service to be interactive
- Insurance
  - New connected devices also raise questions concerning whether or not traditional insurance policies will cover potentially novel claims
  - Careful review of policies to see if they would cover consequences of a cyber incident / gap analysis
  - Insurance underwriters require documentation of strict security controls

Regulatory Considerations

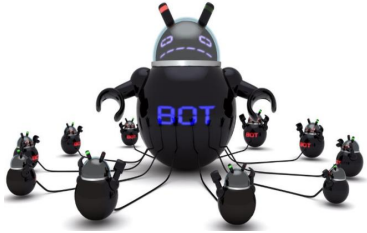
- **Current Legal Framework for IoT**
  - California Online Privacy Protection Act (Cal. Bus. & Prof. § 22575-22579)
  - Information Security (Cal. Civ. Code § 1798.81.5)
    - 20 Center for Internet Security Controls
  - Data Breach Notification Law (Cal. Civ. Code § 1798.82, 1798.29)
  - Computer Intrusions (Cal. Pen. Code § 502)
  - Unfair Competition Law (Cal. Bus. & Prof. Code § 17200 et seq.)
  - IoT Specific Laws (connected cars and TVs, Smart Grid, etc.)
  - FTC: Section 5 under the FTC Act

IoT Lawsuits

- **FTC Enforcement Actions**
  - TRENDNet Home Security (connected video cameras)
  - ASUSTeK Computer, Inc. (home routers and cloud services)
- **Consumer Lawsuits**
  - Smart TVs (Vizio)
  - Connected Toys (VTech, Hello Barbie)
  - Connected Sex Toys
- **FDA Actions**
  - In-Home Monitoring Devices (Abbott St. Jude)

IoT Best Practices

- California AG's Data Breach Report, Feb. **2016**
  - Center for Internet Security's 20 Critical Security Controls
  - Minimum Standard of Care for Reasonable Security



- California AG's Recent Press Release on Botnets Attacks
  - Change default passwords on your household electronics (e.g., webcams, DVRs, routers, printers)

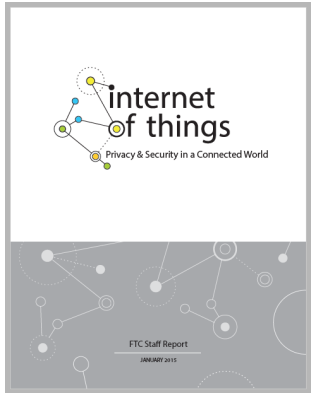
https://www.oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-urges-consumers-protect-their-devices-potential

IoT Best Practices (FTC)

- FTC's Recommended Privacy & Security Practices

("Internet of Things: Privacy & Security in a Connected World", FTC Staff Report, January 2015)

- Building security into devices by design
- Equipping devices with the minimum connectivity necessary to function
- Creating devices that default out-of-the-box to the highest security settings
- Providing necessary security patches throughout devices' life
- Giving consumers data deletion mechanisms to use before device disposal
- Developing and following privacy policies that reasonably limit the collection and retention of consumer data
- Considering data minimization, i.e., limiting the amount of data collected
- Deidentifying personal information collected
- Empowering consumers to personalize their devices' privacy settings



Overview of Cyber Coverages

- **First Party**
  - Data Breach Expenses
  - Network Extortion
  - Digital Asset Loss
  - Business Interruption Loss
- **Third Party**
  - Technology Errors & Omission
  - Security and Privacy Liability
  - Regulatory Liability
  - Multimedia Liability

Overview of Cyber Coverages (cont'd)

- **Characteristic Features**
  - Claims-made coverage
  - Coverage grants are broadly-worded and cover out-of-pocket losses as well as third-party claims
  - Coverage extends beyond "suits"
  - Often include first-party coverage (data restoration and business interruption)
  - Often "modular" in nature, permitting the policyholder to select specialized coverages appropriate to its operations

Key First Party Coverages

- **Data Breach Expenses**
- Covers incident response costs, including:
  - Forensic investigation
  - PR firms and law firms retained to minimize harm and restore public confidence
  - Costs of providing breach notice
  - Identity theft protection services
  - Restoration, recreation, or recollection of Electronic Data

- **Business Interruption Loss**
- Coverage for losses due to an Interruption, including:
  - Extra expenses that would not have been incurred but for interruption
  - Reduction in net income due to interruption plus continuing normal operating expenses

Key First Party Considerations

- Breach of Cloud Provider's System
  - Is your data covered wherever it resides—at a cloud provider; on mobile devices?
  - Check definition of "Your System"

- **Cyber Extortion Coverage for Ransomware**
  - Ransomware often doesn't result in destruction or theft of data, so policy must also cover loss of access to data
  - Policies that provide cyber extortion coverage may cover a ransom payment, if the insurer provides prior consent

- **No Coverage for Loss of Your IP**
  - Loss of IP-value of information or other digital assets not covered

Key Third Party Coverages

- **Security & Privacy Liability**
- Covering liability arising out of breach of duty, neglect, error, or omission resulting in:
  - Failure of Security or Security Breach
    - Loss of access to computer system; hacking attack that results in theft, destruction, or corruption of data; transmission of malicious code to other systems
  - Privacy Injury or Privacy Peril
    - Theft, loss, or unauthorized disclosure of “private information,” “personal information,” or “personally identifiable information”
    - Failure to notify
    - Violation of federal, state, local, or foreign privacy statute or regulation

Key Third Party Coverages (cont'd)

- **Regulatory Coverage**
- Extends to government investigations or proceedings and civil actions
- Civil governmental fines and penalties may be covered
- May include duty to defend and/or duty to pay defense expenses
- Often is subject to a sublimit

- **Professional Services**
- Covers liability arising out of acts, errors, omissions, misstatements in the performance of professional services, which can include:
  - Application service provider services
  - e-Commerce transaction services
  - Electronic exchange and auction services
  - Internet hosting services
  - Internet service provider services

Cyber Coverage Exclusions

- **Key Exclusions**
  - Criminal, dishonest, fraudulent or malicious acts; intentional violation of a privacy policy; or intentional or knowing violation of law
  - Collection of information through electronic spyware or similar means, wire tapping or bugging, etc.
  - Breach of an express warranty or guarantee
  - Violations of antitrust and unfair competition laws; violations of consumer protection laws; false, deceptive, or unfair trade practices; false advertising; patent infringement; misappropriation of trade secrets
  - Assumption of the liability of others under contract, or in some cases any obligation under contract

Thank You

Steve Bridges, Esq.
Senior Vice President
Cyber/E&O Practice
JLT Group

T 312 637 6119

E steve.bridges@jltus.com

Darren Teshima
Partner
Orrick, Herrington & Sutcliffe LLP

T 415 773 4286

E dteshima@orrick.com

Ellen Shaw Holland
Associate Vice President and Chief Risk Officer
Southern Methodist University

T 214 768 2083

E esholland@smu.edu